High Capacity Analog Channels for Smart Documents

Von der Fakultät Ingenieurwissenschaften der
Universität Duisburg-Essen
zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs (Dr.-Ing.)

genehmigte Dissertation

von

Taswar IQBAL
aus
Pakistan

Referent: Prof. Dr.-Ing. Walter Geisselhardt
Korreferent: Prof. Dr.-Ing. Jana Dittmann

Tag der mündlichen Prüfung: 07.04.2006

Acknowledgments

First of all I would like to thank my supervisor Prof. Dr. -Ing. Walter Geisselhardt for his highly valuable ideas as well as moral and financial support, extended through out this research. His role as a supervisor would be a guideline for me in future. I am very thankful to my co-supervisor Prof. Dr. -Ing Jana Dittmann for her highly valuable comments about this dissertation.

I am very grateful to Prof. Dr. -Ing. Axel Hunger (head of the Institute for Multimedia and Software engineering and Prof. Dr. -Ing. habil. Peter Jung (head of the Institute for Communication Techniques) for giving access to printing and scanning facilities, which were absolutely necessary to accomplish this research.

I would to like express my gratitude to Prof. Dr. -Ing. habil. István Erlich (head of the Institute for Electrical Power Systems) for offering job opportunities at very crucial time during this research as well as for his moral support. Furthermore, his kind cooperation at the sudden death of my little sweet daughter Maheen Fatima shall always be remembered.

I am very grateful to Dr. -Ing. Guido Bruck from the Institute for Communication Techniques for very fruitful discussions we had during this research.

I am also thankful to Mrs. Kerstin Luck, Mrs. Nataśa Terzija, Mr. Joachim Zumbrägel, and Mr. Bernd Holzke at the Institute of Distributed Systems for their cooperation through out this research. I would like to pass my special thanks to Mr. Joachim Zumbrägel and Mr. Bernd Holzke for providing all-time working infrastructure as well as for their technical help extended beyond their responsibilities. I am also very thankful to the secretary Mrs. Elvira Laufenburg and all other members at the institute for Multimedia and Software engineering for their cooperation. Finally, I am highly grateful to Mr. Dietrich Schwartz (a very good person who passed away recently) and other members of the Institute for Communication Techniques for their cooperation.

I am deeply obliged to all my friends for their cooperation and well wishes.

Finally, but most importantly I am very grateful to my family for their patience, understanding and encouragement to accomplish this study.

Abstract

Widely-used valuable hardcopy documents such as passports, visas, driving licenses, educational certificates, entrance-passes for entertainment events etc. are conventionally protected against counterfeiting and data tampering attacks by applying analog security technologies (e.g. KINEGRAMS®, holograms, micro-printing, UV/IR inks etc.). However, easy access to high quality, low price modern desktop publishing technology has left most of these technologies ineffective, giving rise to high quality false documents. The higher price and restricted usage are other drawbacks of the analog document protection techniques. Digital watermarking and high capacity storage media such as IC-chips, optical data stripes etc. are the modern technologies being used in new machine-readable identity verification documents to ensure contents integrity; however, these technologies are either expensive or do not satisfy the application needs and demand to look for more efficient document protection technologies.

In this research three different high capacity analog channels: high density data stripe (HD-DataStripe), data hiding in printed halftone images (watermarking), and superposed constant background grayscale image (CBGI) are investigated for hidden communication along with their applications in smart documents. On way to develop high capacity analog channels, noise encountered from printing and scanning (PS) process is investigated with the objective to recover the digital information encoded at *nearly maximum* channel utilization. By utilizing noise behaviour, countermeasures against the noise are taken accordingly in data recovery process.

HD-DataStripe is a printed *binary image* similar to the conventional 2-D barcodes (e.g. PDF417), but it offers much higher data storage capacity and is intended for machine-readable identity verification documents. The capacity offered by the HD-DataStripe is sufficient to store high quality biometric characteristics rather than extracted templates, in addition to the conventional bearer related data contained in a smart ID-card. It also eliminates the need for central database system (except for backup record) and other expensive storage media, currently being used. While developing novel data-reading technique for HD-DataStripe, to count for the unavoidable geometrical distortions, registration marks pattern is chosen in such a way so that it results in accurate sampling points (*a necessary condition* for reliable data recovery at higher data encoding-rate). For more sophisticated distortions caused by the physical dot gain effects (intersymbol interference), the countermeasures such as application of sampling theorem, adaptive binarization and post-data processing, each one of these providing *only a necessary condition for reliable data recovery*, are given. Finally, combining the various filters corresponding to these countermeasures, a novel Data-Reading technique for HD-DataStripe is given. The novel data-reading technique results in superior performance than the existing techniques, intended for data recovery from printed media.

In another scenario a small-size HD-DataStripe with maximum entropy is used as a copy detection pattern by utilizing information loss encountered at nearly maximum channel capacity. While considering the application of HD-DataStripe in hardcopy documents (contracts, official letters etc.), unlike existing work [Zha04], it allows one-to-one contents matching and does not depend on hash functions and OCR technology, constraints mainly imposed by the low data storage capacity offered by the existing analog media.

For printed halftone images carrying hidden information higher capacity is mainly attributed to data-reading technique for HD-DataStripe that allows data recovery at higher printing resolution, a key requirement for a high quality watermarking technique in spatial domain. Digital halftoning and data encoding techniques are the other factors that contribute to data hiding technique given in this research. While considering security aspects, the new technique allows contents integrity and authenticity verification in the present scenario in which certain amount of errors are unavoidable, restricting the usage of existing techniques given for digital contents.

Finally, a superposed constant background grayscale image, obtained by the repeated application of a specially designed small binary pattern, is used as channel for hidden communication and it allows up to 33 pages of A-4 size foreground text to be encoded in one CBGI. The higher capacity is contributed from data encoding symbols and data reading technique.

Keywords: Smart documents, HD-DataStripe, cryptoglyphs, counterfeiting detection, data-tampering, watermarking**,** entertainment tickets protection, printing scanning process, halftone images, 2-D barcodes, biometrics systems, data encoding in background images.

Table of Contents

Chapter

List of Figures

List of Tables

Chapter 1
Introduction

1.1 Impact of Digital Technology on Analog Security Media

The valuable hardcopy documents such as passports, visas, driving licenses, identity cards, entrance-passes for entertainment events, contracts, business letters, educational certificates, are being used very-widely nowadays. As the end-use of such documents (e.g. driver's license, passport) is to verify a person's identity, who is granted certain rights, this fact prompts their chances of illegal usage by the criminals by launching counterfeiting and forgery attacks. Similarly, the documents (e.g. contracts, official letters, bank checks) are to be protected against forgery attacks by the fraudsters, trying to get more than the granted benefits. Conventionally such documents are secured by applying analog security technologies: optical variable devices (e.g. Holograms, KINEGRAMS®), watermarks, microprinting, special printing inks (e.g. UV, IR and magnetic), chemical coating [Phil00, Phil02, Phil04, Ren98, Ren05]. However, the easy access to modern technologies: photocopiers/scanners, printers and image processing software, have left most of the existing analog security technologies ineffective, resulting in high quality false documents that cannot be identified easily as the counterfeited or forged documents. In [DiC] it is reported that financial loss in the USA due to credit card fraud by using the counterfeited documents is estimated $2 billion per year. The welfare fraud by double dippers is believed to be in excess of $4 billion a year. In addition to the financial loss there are other more serious losses caused by terrorist activities, underage drinking/smoking, firearm buying etc. that are very often aided by the counterfeited or tampered identity verification documents.

1.2 Limitations of New Analog Security Technologies

In order to count the threats posed by the modern digital technologies, nowadays more sophisticated analog security technologies e.g. Kinegrams, which is similar to the holograms technology, but claims higher resistance against the counterfeiting and forgery attacks, are being introduced [Ren98, Ren05]. Irrelevant from their performance, the new technologies have the limitations such as higher prices and restricted usage. The higher price is not appreciated due to the fact that end products are going to be produced in mass quantity (e.g. National IDs) and would require huge amount of money to replace the existing documents. This might not be affordable by many poor nations and would result in a security hole. Similarly, restricted usage constraint leaves relatively low value applications still vulnerable. Furthermore, if this restriction is relaxed then there is possibility that technology is transferred to fraudsters, who may break the authentication (decoding) devices and use this knowledge in other applications [KJJ04]. In addition to being expensive and restricted, there is another limitation associated with the above approach that these technologies need constant innovations, requiring very sophisticated research facilities, in order to maintain the technology gap between the legal authorities and the criminals. This gives the impression that technology gap oriented approach would result in expensive products in future as well.

The above discussion poses challenge for research community to search for more efficient solutions. An example could be a cryptographic technique for digital data security where same technology, shared by the criminals and legal authorities, is adopted to secure digital data. However, the criminals need extremely higher efforts to break the solution and this fact encourages considering digital techniques for analog media.

1.3 Motivation

Nowadays inspired by the benefits of digital authentication techniques as well as high quality printing and scanning technologies, *digital techniques* are being investigated with the aim to secure analog media (i.e. contents integrity verification of hardcopy documents). With this objective digital watermarking and digital signatures have been focused upon. Digital watermarking originally intended for contents integrity verification of digital media (audio, video, still images and text data), hides imperceptibly some authenticity related data in the host-media (to be secured) and the hidden data is decoded back at verification time. The *challenge encountered* when considering application of digital watermarking techniques to secure analog media (e.g. printed portrait in a traveling document), can be envisioned from the fact that a lot of literature [CMB+01, FPR+99, IH95-IH02] dealing with the watermarking of digital contents is available; however, very less work [CKL+97, FDG01, GR98, HVH99, PVT04] dealing with analog contents is reported in literature. There are also techniques patented from MediaSec® and DIGIMARC®. All these techniques have one common drawback that their data hiding capacity is much lower as compared with the capacity for digital contents. Also, these techniques are either semi-blind or non-blind, which means that either the encoded message or original unmarked contents are needed in advance to decode the hidden message and this fact puts the authentication device at risk of being broken. Some other techniques [FuA02, HeO00, Wan01, WLH99, Wu01] result in relatively poor image quality in analog form.

Digital signatures are being applied to ensure the integrity of biographical data (contained on ID cards) in analog form, where digital signatures consisting of small payload is generated from the biographical data and is stored on the card in a barcode or using OCR-readable alphanumeric character stripe added on the identity verification document. Digital signatures have weaknesses arising from OCR technology and message digest generating techniques [KJJ04, Zha04].

In the following common challenges encountered and areas of further improvement for digital techniques when being applied to secure hardcopy documents are reviewed.

1.3.1 Identity Verification Documents

The identity verification documents constitute the core of the hardcopy documents and are the primary target of the counterfeiting and data-tampering efforts. Here the ultimate goals to be achieved are:

1. **Data Integrity:** All the data contained in the document such as bearer photographs, biographical data must be secured against the data-tampering attacks.
2. **Highly Reliable Identity Verification System:** The goal is to develop automatic identity verification system that can recognize with high level of confidence that the person being identified is the one who claims he is and not a threat to the system.

The need for second goal is necessiciated from the fact that conventional human interaction based identity verification methods are prone to errors (intentional/unintentional). In order to achieve the above goals by applying digital techniques, in first case, it is required that all the contents are stored in digital form on the card/document, so that at verification time the printed visual contents (goal-1) can be compared with the digital contents for contents integrity verification. The second objective can be achieved by using biometrics characteristics, which are not prone to identity theft/transfer threats and allow automatic identity verification. However, the constraints from this scenario (goal-2) pose more challenges as very large volume of biometrics data [PVT04] needs to be handled for *high reliability*.

Higher data storage demand is conventionally fulfilled using central database systems; however, this approach has limitations and other alternatives such as on-card data storage technologies are focused upon nowadays. Following this approach in [CBN, DStr] all the contents are stored in digital format on the document, using 2-dimentional barcodes. The data recovered from the scanned barcode is used by the digital techniques for contents integrity verification and automatic identity verification. This approach also has a limitation that the capacity offered by the existing 2-D barcode technology (e.g. PDF417) is not sufficient to satisfy all the requirements of highly reliable biometrics-based identity verification systems. To overcome this limitation other storage media such as optical memory stripe, IC chips etc. are suggested that are obviously much more expensive than barcodes and are also not applicable to many types of hardcopy documents e.g. contracts, entertainment tickets etc. These facts enforce to look for more efficient on-card data storage technologies.

1.3.2 Entertainment Tickets, Bank-Checks

Access-passes for the entertainment events, traveling tickets, bank-checks are relatively more prone to counterfeiting attacks due to the fact that their cost constraint restricts the application of *very* sophisticated technology in these products. Conventionally, the anti-counterfeiting technologies, e.g. magnetic stripe, UV/IR inks, holograms, are used; however, such technologies results in expensive final products [MAC+04] and are not considered highly reliable as well. Furthermore, as these products are not going to be used over and over, so this fact should be taken into account. Some of the technologies e.g. memory chips, for hardcopy documents are not suitable at all due to their prohibited cost and the nature of the document under consideration. Consequently, all these factors necessitate the need to look for more efficient document authentication techniques. In this regard anti-counterfeiting digital techniques (e.g. Copy Detection Patterns [Pic04], Cryptoglyphs [Cryp]) for document authentication could be useful as this technology is less expensive, sufficiently robust against counterfeiting attacks and permits automatic: copy detection [Pic04], and contents integrity authentication [Cryp]. However, CDP cannot address data tampering attack whereas cryptoglyphs offer very small data capacity.

1.3.3 Official Letters, Contracts

Everyday documents e.g. contracts, official letters etc. is another class of hardcopy documents, which are conventionally secured against data-tampering attacks using analog seals and are manually verified. In this case digital signatures technique for contents authenticity verification selects crucial part of the document that is more likely to be forged and the resulting data is encoded after encryption into 2-D barcode symbols that is printed at appropriate location in the document. There is digital technique [Zha04], which generates a digital signature from the full textual contents and this digital signature is printed as a 2-D barcode and used for contents verification. However, this approach has the limitations due to its dependence on hash functions and OCR technology. The OCR technology with full advancements cannot guarantee exact recovery and in ideal scenario results in up to 99% accuracy. Similar to digital watermarking technique, some text watermarking techniques [AlA04, BLM+95, BLM99, LoM98, LoM00] for hardcopy documents are given as well. However, these techniques permit small amount of data to be hidden and cannot authenticate contents integrity on one-to-one basis.

1.4 Objectives of This Research

This research turns the key-weapons (high quality printing and scanning technologies) of the counterfeiters against them, while combating the challenges posed by this technology. It is intended to decrease the need for constant innovations to maintain the technology gap between the legal-authorities and the criminal elements for document protection, resulting in less-expensive anti-counterfeiting and tampering-resistant technologies that can be combined with other sophisticated technologies used by the government authorities to reduce the cost without compromising the ultimate quality of highly sensitive-products. Inspired by these incentives some digital techniques to secure and authenticate the analog media are investigated with the following objectives:

A) As clear from the above discussion that main concern of the existing research focused on smart identification documents is to develop the technology having the following characteristics:

1. Resistant against counterfeiting and data-tampering
2. Permit automatic identity verification using multiple biometric characteristics
3. Cost effectiveness

To achieve all of the above goals, objective is set to develop a High Density DataStripe (HD-DataStripe), which would allow encoding bearer portrait, biographical, multiple-biometrics characteristics. The *HD-DataStripe* is a printed binary image, similar to conventional 2-D barcodes; however, it offers higher data encoding rate. In order to develop HD-DataStripe noise encountered at higher data encoding rate during printing and scanning process is studied more deeply and systematically. Then, a novel data-reading technique is given to recover the data encoded in HD-DataStripe. It is to be pointed out that PS process noise gets severe, as we shall see in chapter 3, as data encoding rate is increased and in this research much higher data encoding rate as compared with the existing research [FuA02, ST, Wan01, WuL04] is investigated.

A secondary objective is to show how HD-DataStripe can be used to address the cryptographic security threats: contents confidentiality, integrity, authenticity, non-repudiation and key management, posed to the biometrics identity verification system. Here, for instance, threats encountered from the repudiation attacks to the biometrics identity verification system can be overcome more effectively using high quality multiple biometrics characteristics than the single biometric template for identity verification, under the assumption that system is secure against the manipulation of biometrics template matching result or any other such threats [JRU05].

B) Investigating further applications of HD-DataStripe, contents integrity verification of hardcopy documents such as contracts, official letters is focused upon only on abstract level with the objective to see the potential gains of using HD-DataStripe in this context. Here it is expected that a small size HD-DataStripe would offer sufficient capacity to encode full contents of the document, eliminating the need for message-digests for digital signatures and limitations of OCR technology.

In another scenario again on abstract level application of HD-DataStripe is focused upon as an anti-counterfeiting (copy detection) and contents-tampering resistant technology for the entertainment tickets, bank-checks applications. It is to be mentioned that the new technology would be more sophisticated than the existing one [Pic04], which enables *only* copy detection. The impact of higher channel capacity offered by HD-DataStripe on security of the anti-counterfeiting application in context of contents confidentiality, integrity, authenticity, non-repudiation and key management is considered as well. Security threat posed to the well-known cryptoglyph [Cryp] against *active counterfeiting attacks* is another objective of the research.

C) A digital watermarking technique working in spatial domain for printed grayscale images is investigated with the aim to have further gain in data hiding capacity and image quality as compared with the existing techniques [FuA02, HeO00, Wan01]. To achieve these goals following points in watermarking technique are addressed: halftone technique, printing resolution, data hiding technique, data-reading technique for printed grayscale image. Inspired by the existing fragile/semi-fragile watermarking techniques dealing with digital contents, here on abstract level it is shown how contents integrity and authenticity can be ensured in present scenario in which innocent noise encountered from PS-process and dust-and-scratches is unavoidable.

D) Inspired by the technique given in [SMS03], which allows to hide data in printed constant background grayscale images, a similar application is investigated in this research with the aim to further increase the data hiding capacity, while maintaining same image quality of the printed document. In the existing technique, using especially designed binary patterns representing to "0", "1" bits, data is encoded in the constant background grayscale image. The goal of this research is to see the possibility to further decrease the size of data encoding patterns and check for the resulting capacity gain. Furthermore, apart from decreasing the size of the data encoding symbols, it is also aim to encode multiple-bits per symbol, which results in more severe noises that need to be handled during data recovery process. Possibility of achieving multiple graylevels with the new data encoding symbol and potential gains as compared with the existing technology DataGlyphs® are considered as well. Inspired by the fact that both cryptoglyph™ technology and proposed technique use invisible secondary images for document authentication, a comparion of the advantages and disadvantages of the crypoglyph technology and proposed technique is given.

1.5 Dissertation Organization

The remaining contents of the dissertation are organized as follows:

In **CHAPTER 2** some background material for the following chapters is given. As this research primarily deals with the PS process so the noise encountered in this context is discussed. The key points such as printing-resolution, screen-frequency, most widely used digital halftoning techniques, are introduced from the perspective of some final applications of PS process. A brief introduction to digital watermarking is also given.

CHAPTER 3 is at the heart of this research and deals with reliable data recovery for HD-DataStripe. It begins with reviewing some existing data reading techniques for printed binary images and points out the limitations of the existing technique in the context of HD-DataStripe. Next, the noises encountered during PS process for HD-DataStripe are studied and countermeasures against geometrical distortions, physical dot gain effects, are given. Then different filters dealing with adaptive-binarization and post data processing techniques are given. Finally, experimental results for HD-DataStripe data recovery using the novel data-reading technique are given.

CHAPTER 4 deals with the core application, Smart Identity Cards, which originally inspired this research. Here the biometrics identity verification systems are reviewed with the aim to know the key requirements and constraints for the development of reliable identity verification documents. Some existing smart identification documents are critically reviewed and then the novel Smart ID Card using HD-DataStripe, is given. In addition to smart ID-cards two other applications of HD-DataStripe technology are considered as well. In one scenario application of HD-DataStripe as a copy detection and counterfeiting resistant technology is considered, whereas in the second case digital-signing technique to authenticate hardcopy documents contracts, official letters is focused upon.

Digital marking for the printed grayscale images, which offers higher data hiding capacity and superior image quality, is given in **CHAPTER 5**. A critical review of existing techniques in context of this research is given and it is followed by the data hiding technique and some other issues not addressed in the existing work.

Inspired by the fact that further improvements can be achieved in the data hiding technique for the constant background grayscale images [SMS03] in **CHAPTER 6** the authenticity of hardcopy documents e.g. official letters is concentrated again. And a new data hiding technique, which employs background image to encode data, is given.

Finally, deduced conclusions from the research and directions for further work are summarized in **CHAPTER 7.**

Chapter 2
Background and Related Work

2.1 Introduction

The main focus of this research is to recover the original information to the best possible extent, which has gone through both the linear as well as the non-linear transformations. The original information under consideration is an image data and the non-linear transformations it encounters during printing and scanning (PS) process are: 1) halftoning process (a lossy digital-to-digital transformation), 2) rendition of the pixels to the paper (*usually* a lossy digital-to-analog transformation), and 3) the digitizing/scanning process (lossy analog-to-digital transformation). The first two operations are associated with the printing process whereas the last one as the name shows is related to scanning process. As we shall see later on, each of the above transformations in its conventional use (i.e. when ultimate goal is to have an high quality printed as well as scanned image) plays a very crucial role. However, the importance of the above transformations increases further when the objective is to recover the original information after PS process and this fact demands to study the above transformations in advance, as it would be necessary to keep in mind the impacts of the above transformations on the image being recovered, while developing the techniques to make the image robust against the PS process (treated in Chapter 3). In the following sections each of the above transformations is discussed.

2.2 Printing Process

We start by describing the printing process in general. The printing process begins with an input image, which is *usually* a collection of pixels (a visually meaningful pattern) having either only binary values or color values (red, green, blue) varying in a specific range, depending upon the quality of image. At first stage using a non-linear digital-to-digital transformation, the larger color gamut of input image is mapped to smaller color gamut of the printing device. This non-linear gamut mapping transformation, known as digital halftoning, exploits the low-pass filtering characteristic of human visual system and imposes a constraint on the mapping process that the difference between the original image and the one resulting from mapping process should be imperceptible by the human visual system. In second stage (digital-to-analog process) the digital image (not necessarily an halftone image) is passed to the printing device, which makes a dot on the surface of analog media (paper in the present context, or any other media), using the corresponding ink for all pixels. The inability of the printing device to print reliably and accurately a very small size dot on paper surface makes this transformation non-linear, resulting in a color gamut difference between the theoretical (digital) and experimental color-gamut values.

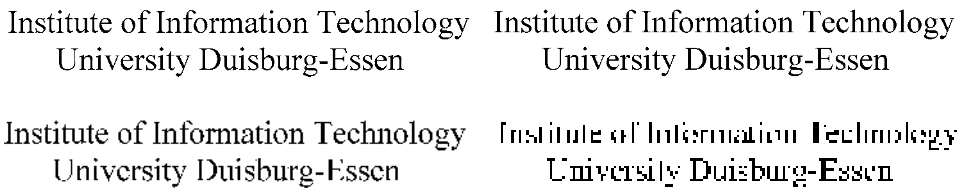
After giving general description of printing process in the following each of the two stages of printing process is discussed from the two perspectives: 1) its impact on the visual quality of the printed document/image (conventional use), 2) its impact on the information (HD-DataStripe) intended to be recovered after PS process. However, the focus will be mainly on the second one, as this is the main concern of this research, whereas the other one is addressed as well (in Chapter 5).

2.3 Distortions Caused by the Dot-Making Process

Although practically this non-linear digital-to-analog transformation occurs later, however, due to its impact on the other (non-linear digital-to-digital transformation) transform, it is discussed before. In the following, the key elements of this transformation and their impact on the well-known printing technologies such as Ink-jet, Laser-jet and Dye-sublimation, are discussed.

2.3.1 Impact of Print Resolution on Printed Image Quality

Print resolution is described as the maximum number of dots that a printer can print in per unit area (usually in per square inch dpi) and has key role on the quality offered by any printing technology. In general any printing device with higher resolution results in better image quality. This is due to the fact that at the higher resolution smaller size dots are used, which are imperceptible by human eyes and consequently result in smooth and contone images. This fact can be observed from Figure 2.1 in which a text image is printed at various resolutions.


Institute of Information Technology
University Duisburg-Essen

Institute of Information Technology
University Duisburg-Essen

Institute of Information Technology
University Duisburg-Essen

Institute of Information Technology
University Duisburg-Essen

Figure 2.1: An illustration of the impact of print resolution (600, 300,150, 75 dpi) on image quality. Note: The quality of the last image would be slightly better in terms of discontinuities, when it is down-sampled by the printer's internal driver.

For grayscale and color images, the higher quality of a printed image is correlated with resolution through the color gamut. The gamut of a printing device is the maximum number of colors that a device can reproduce and for the ink-jet as well as Laser printing technology, it is constrained by the resolution offered by the printing device. For grayscale images printed using binary (black and white) printing devices, the gamut is fully constrained by the resolution and the ability of the printing device to print reliably and accurately a single dot. And for the binary printing devices it is obtained by using halftoning techniques, which are based on the low-pass filtering characteristics of human visual system. According low-pass filtering characteristics of human visual system, human visual system is not able to see a dot size smaller than 30 micron. Consequently, when the small size dots are printed in given area, the human visual system rather than identifying individual dots, perceives the area as a smooth region of a single color, where the color value of the region is the average light reflected by that region. This low-pass filtering characteristic of human visual system is demonstrated in Figure 2.2 in which two images: a constant grayscale stripe and its magnified view, are shown. As it can be seen that under the magnified view the image consists of just a pattern of dots whereas in the second image the same pattern of dots is perceived as a constant strip of gray color and this is attributed to the inability of the human visual system to resolve fine details from a certain distance.

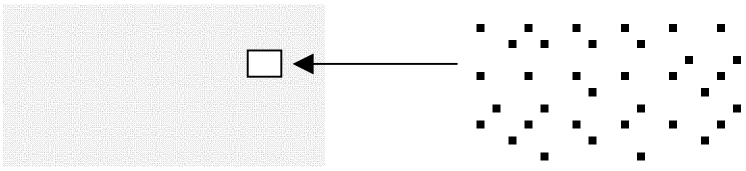


Figure 2.2: A constant grayscale stripe and its magnified view to illustrate the idea of low-pass filtering.

The different graylevels using halftoning technique are achieved by varying the density of black dots in a given small region, called halftone cell and this cell size is very crucial as it controls the maximum number of graylevels that can be produced. A cell of size $x \cdot x$, while using only black ink and without taking into account dot gain effects (to be discussed later on), can produce $x^2 + 1$ graylevels. The cell size, however, cannot be chosen arbitrarily and is constrained by other factors such as screen frequency and maximum resolution offered by the printing device. The screen frequency (lines per inch lpi) is number of times the cell is repeated in a unit area at maximum resolution. It is noteworthy that although higher screen frequency results in more smooth images, but it results in lower gamut, as it is inversely related with the cell size. The relation for the number of graylevels as a function of screen frequency and the device resolution is given by the following equation:

$$\lambda = \left({}^{dpi}\!/_{lpi} \right)^2 + 1 \qquad (2.1)$$

λ number of graylevels,
dpi maximum device resolution,
lpi screen frequency (i.e. number of times halftone cell measuring m by m is repeated).

From equation (2.1) it is evident that those printing technologies in which the color gamut is obtained, using a halftoning technique, the higher printing resolution *usually* results in a higher image quality due to the reason that higher device resolution allows to increase the cell size and the screen frequency. This can be observed easily by printing a grayscale image on two different laser printing devices, offering maximum resolution 300 and 600 dpi, respectively. However, higher resolution is only one factor and alone cannot guarantee higher quality for the grayscale images and it depends upon the ability of the device to print reliably and accurately each and every dot, which is a function of ink transfer or dot making mechanism used in the printing technology and the ink-paper interaction (ink-paper interaction is not considered in this research).

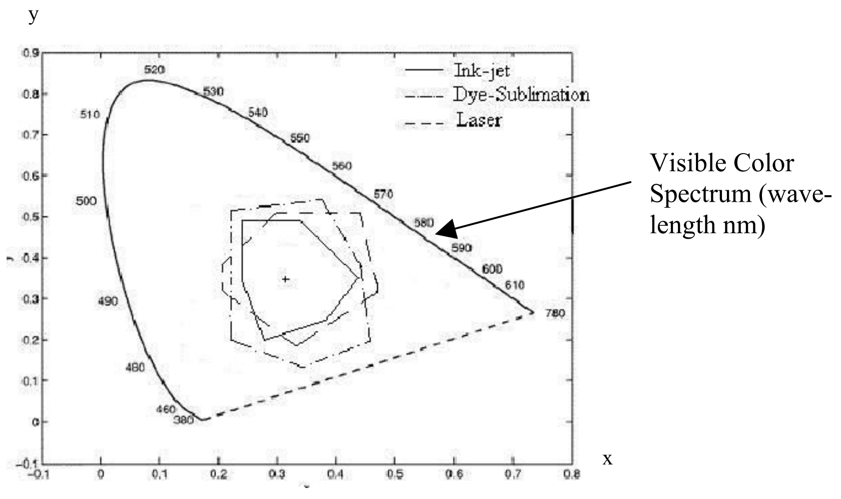
2.3.2 The Ink Transfer Process for Various Technologies

In laser printing technology to make a dot at certain location, laser beam is focused at a very small region (which can be considered as the smallest dot printable by the device) on a drum and as a result that region is charged. Next this charged region attracts the oppositely charged toner. Finally, toner is fixed permanently on the paper surface by applying heat and pressure. In case of color laser printers the above procedure for each color cyan, magenta and yellow, is repeated sequentially. Now as the laser beam can be focused very precisely to form very small size dots and the oppositely charged solid toner is attracted by the charged region, so physical dot can be formed very accurately.

In contrast to Laser print technology, in inkjet printing technology to print a dot at a specific location, a droplet of liquid ink is sprayed on the paper surface by applying pressure at ink reservoir. This mechanism consequently causes the droplet to partially spread on paper surface as well as to be absorbed into the surface, resulting in a dot having physical size bigger than the expected size. And this fact consequently gives rise to dot gain effects (to be addressed mainly in Chapter 3) due to the interaction of the dot with neighboring dots and make it difficult to print isolated dots. To compensate for this increase in dot size due the spreading of liquid ink on paper surface in addition to using coated paper, *probably* the higher resolution (i.e. to decrease dot size) is used in ink-jet technology.

Unlike ink-jet and laser technologies, dye-sublimation technology, which offers the highest color gamut (i.e. 256 graylevels) at 300 dpi, does not use any halftone technique and results in continuous tone (photographic quality) printed images. The main strength of this technology lies in its dot printing mechanism. This technology prints a square-shape dot accurately and reliably at 300 dpi by precisely diffusing up to 1/256 amount of ink at the desired position. A particular graylevel for the printed dot is obtained by precisely controlling the amount of ink diffused into the square-shape dot. However, dye-sublimation technology has the disadvantage that it has higher per copy cost as compared with the ink-jet and laser technologies.

After discussing ink-jet, laser and dye-sublimation technologies, it can be stated that higher resolution and the accuracy of the single isolated dot being printed, are the most important characteristics of a printing device. These characteristics not only result in higher image quality due to higher color gamut, but *are of special interest for the applications* in which image has to be recovered after printing and scanning process. A comparison of color gamuts of Laser-jet, Ink-jet, and Dye-sublimation printers [Atr04] is shown in Figure 2.3, which shows that the Dye-sublimation printing technology offers the highest gamut whereas the Ink-jet and Laser technologies have more or less same gamut size.



Visible Color Spectrum (wave-length nm)

Figure 2.3: A comparison of color gamuts of laser-jet, ink-jet, and dye-sublimation printers (reproduced from [Art04]). Note: No details are given about the units on x and y-axis in [Durr87, ShT97].

It is to be pointed out that in ink-jet technology unlike Laser technology the color gamut is increased by increasing the number of basic inks and other techniques. If the color gamuts of the Laser and ink-jet technologies are compared for single ink (e.g. black) at same resolution, then the gamut for ink-jet technology in general, would be smaller than the other one. And this is due to the presence of more dot gain effects in ink-jet technology. Consequences of this fact will be apparent in the following chapters, while considering information recovery from PS process. Dye-sublimation technology is expected to have promising performance due to its apparent characteristics.

2.3.3 Dot Gain Effects Encountered at Higher Resolutions

Due to the dot gain effects a printed dot gets bigger after printing, as noticed in the previous section while considering ink-jet technology. However, dot gain effects continue to exist in laser technology as well and their main source is circular-shape of the printed dot. It is important to note that dot gain effects are unavoidable, as it can be seen from Figure 2.4, and this is due to the shape of the original (digital) and printed dot. In digital form a pixel is of square shape whereas the printed dot has circular shape. From Figure 2.4 it can be seen that even when there is no or very minor ink spreading on the paper surface for laser technology, still either dot gain or loss is occurred, which causes the printed image to appear either darker or lighter than the original one. It is mentioned in [Kan99] and observed in this work as well that in general ink-jet technology has higher dot gain effects as compared with the laser technology.

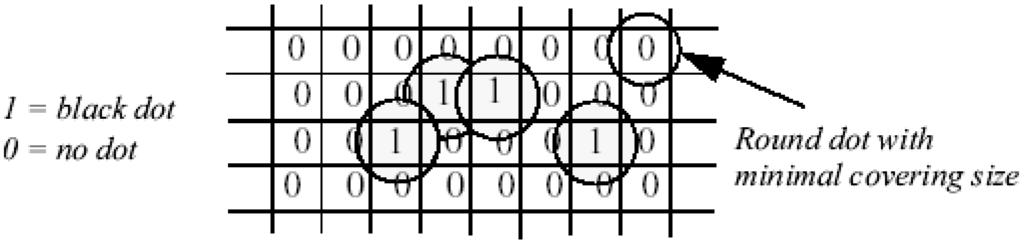


Figure 2.4: An illustration of physical dot gain effects development process [Goo01].

Although, dot gain effects are unavoidable and this is the limitation of the existing ink-jet and laser printing technologies, however, for high quality printers the dot gain behavior is studied very well in advance and based on this behavior, halftoning algorithm is designed [Goo01, Kan99]. In section 2.4 two such images are shown: one without taking into account the dot gain effects (Figure 2.11b) and the other one after compensation for such effects (Figure 2.15). The dot gain effects in inkjet and Laser printing technologies are compensated in halftoning algorithm by varying the density of black dots in the halftone cell. Finally, it is to be pointed out that although dot gain effects can be compensated and in fact these effects have been compensated successfully, as we shall see while discussing digital halftoning techniques. However, dot gain effects pose challenge for the applications, in which it is not acceptable to modify the number of pixels to compensate for the dot gain effects.

2.4 Distortions Caused by the Digital-to-Analog Gamut Mapping

The fact that most of the printing technologies available today use *only few basic colors* (1 for binary/grayscale printing, and 3-4 for color printing), which are mixed together in special ways to form other colors, results in a device having color-gamut (number of colors device can successful produce) that is far less than the color gamut of a good quality digital image. This can be seen from Figure 2.5 in which typical gamuts of various output devices (monitor, printer, etc.) offering *subjective* comparison are shown. To overcome this limitation of the printing devices, color gamut or simply calling gamut of the digital image is mapped to the gamut of the printing device. This mapping is encouraged by the fact that human visual system cannot distinguish among all the colors used in a high quality digital image and the number of colors, which are recognizable by the human visual system, are less than the original gamut of the digital image. This phenomenon is used in almost all the existing printing technologies to keep their cost low and the technique used for gamut mapping is called digital halftoning.

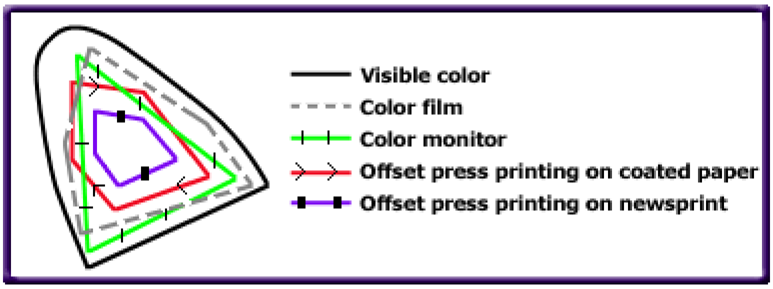
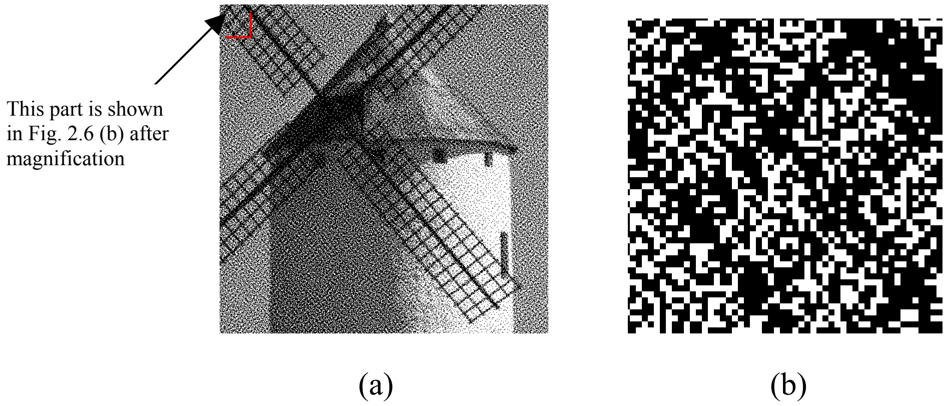

Visible color
Color film
Color monitor
Offset press printing on coated paper
Offset press printing on newsprint

Figure 2.5: A subjective comparison of color gamuts for various image output devices.

2.4.1 Digital Halftoning

Digital halftoning is the process to represent a continuous-tone image by an image consisting of only basic printing colors in such a way that from a certain distance both images (original and halftone) are *perceived* as of similar quality. The halftoning process is based on the fact that human visual system is not able to recognize individually very small size dots due to its low-pass filtering characteristics. By varying the ratio of primary colors in a small area all the colors that are recognizable by our visual system can be produced/simulated. Although, under the magnifying glass the printed image or single color plate looks as a collection of dots of primary color, however, at a normal viewing distance image is perceived as continuous-tone image. This fact is illustrated in Figure 2.6(a-b) where an image a grayscale is printed using a halftoning process and in the Figure 2.6(b) magnified version of Figure 2.6(a) is printed. In digital halftoning process, a specific graylevel is achieved by varying the number of black pixels in a halftoning cell. A halftoning cell of size 3 by 3 with 10 levels of gray is shown in Figure 2.7.



This part is shown in Fig. 2.6 (b) after magnification

(a) (b)

Figure 2.6: a) A halftoned image, b) magnified view of a small part of image shown in part (a). (Note halftone image shown in part a is not of constant single graylevel, as such images are not yet generated).

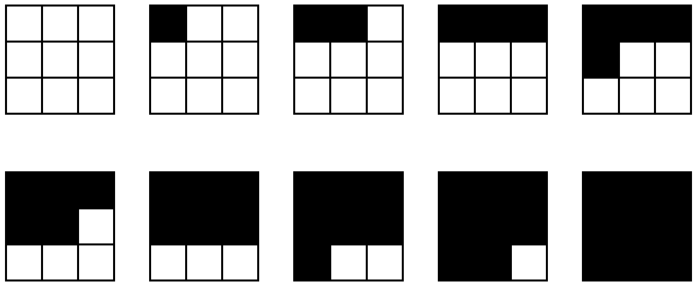


Figure 2.7: An illustration of 10 graylevels for a 3 by 3 halftone cell.

As mentioned earlier that the size of a halftone cell is restricted by the halftone screen frequency (recall equation 2.1). It is desirable to have both higher screen frequency as well as graylevels, which would result in higher quality image. However, due to the limited resolution (imaging elements) in the practical printing devices, a compromise has to be made in the selection of screen frequency. It is suggested that a value, 150 lpi, for screen frequency is sufficient to print high quality grayscale images. So the printing device with 1200 dpi would provide 65 graylevels for 150 lpi screen frequency.

A lot of work has been done on digital halftoning and an extensive bibliography can be found in [Goo01, Kan99]. However, still more work needs to be done in the areas such as:

1. Computational efficiency against higher image quality: All the existing halftoning algorithms, which result in higher quality, are computationally expensive.

2. Efficient methods for performance evaluation: Good methods for providing objective quality comparison criteria to compare the performance of various halftoning techniques are still needed.
3. The term ‘good’ for digital halftoning still remains to be defined.

These are only a few areas to be pointed out. The work on digital halftoning can be classified into the following categories: 1) Ordered dithering halftoning, 2) Error diffusion halftoning, 3) Hybrid halftoning, and 4) Iterative halftoning. As digital halftoning is not the main focus of this research due to this reason these techniques are not discussed in detail and only basic idea behind these techniques is given, however, for interested readers references are provided for further information.

2.4.2 Ordered Dithering Halftoning

In such halftoning technique a predefined matrix of fixed size is used repeatedly to binarize the grayscale image. It has the advantage that it is computationally very efficient, however it does not result in very high quality halftoned images, as we shall see. Ordered dithering is further classified into cluster dot ordered dithering and dispersed dot ordered dithering.

In clustered dot dithering, also known as amplitude modulation (AM) halftoning, the size of a single halftone dot is increased to get different halftone levels. The AM halftone dot forming process for a 3 by 3 size halftone cell is illustrated in Figure 2.8. in which different graylevels for AM halftoning are shown. A typical AM halftone matrix for a grayscale image varying in the range 0-1 with step-size 1/255, is shown Figure 2.9 (a). This matrix results in 17 graylevels and the multiplying factor 1/17 keeps the halftone matrix in the rage 0-1. The numbers 0 and 1 represent full black and white graylevels, respectively. In this matrix dithering pattern formed is rotated at 45 degree so that artifacts resulting from the periodic application of the dithering matrix are least noticeable by human eye. An halftoned image resulting from the application of the above dithering matrix is shown in Figure 2.9(b). As it can be noticed from the Figure 2.9 that AM halftoning is not able to produce high quality images due to its inability to produce details in the original image. However, AM halftoning technique has the advantage that it is robust against dot gain noise and has been mainly used in the devices, which are not able to produce single isolated dots. It is also mentionable that AM halftoning technique is the oldest halftoning technique and has been used in photographic printing and binary displaying devices. Within the family of clustered dot ordered dithering many different techniques and variations are given in Chapter 13 [Kan99].

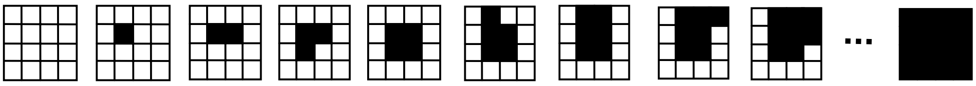
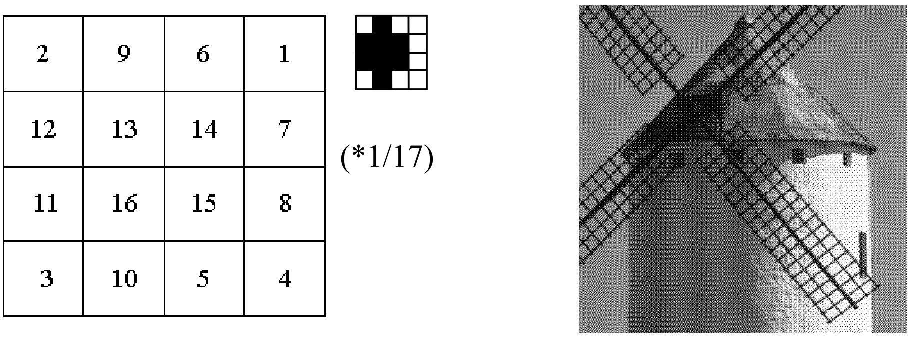


Figure 2.8: An illustration of AM halftoning in which size of a single dot is increased to obtain different graylevels.



2	9	6	1
12	13	14	7
11	16	15	8
3	10	5	4

(a)

(b)

Figure 2.9: An illustration of clustered dithering halftone technique, (a) 17 level clustered dithering cell, (b) resulting halftone image. Next to top-right corner of Figure (2.9a) is shown its pixel representation for 0.5 graylevel.

2.4.3 Dispersed-Dot-Ordered Dithering

Unlike clustered-dot-ordered dithering in dispersed-dot-ordered dithering, which is also known as Frequency Modulation (FM) halftoning technique, microdots within the halftoning cell (dithering matrix) are *dispersed* and different halftone levels are obtained by varying the density of microdots within the cell. The role of multiplying factor 1/17 is same as explained in clustered dot halftoning. Some graylevels for a halftone cell using FM technique are shown in Figure 2.10. A typical FM matrix (cell) and a halftone image resulting from the application of this matrix are shown in Figure 2.11. As it can be seen from Figure 2.11(b) that images resulting from FM halftoning are of higher quality due to its capability to produce details in the image. However, this technique has a disadvantage that it is not robust against dot gain effects and results in halftone images, which appear darker than the original images. To compensate for the dot gain effects in FM halftoning, randomly selected microdots within the halftone cell *are turned white.* More detailed information along with a list of references on FM halftoning can be found in chapter 14 [Kan99].

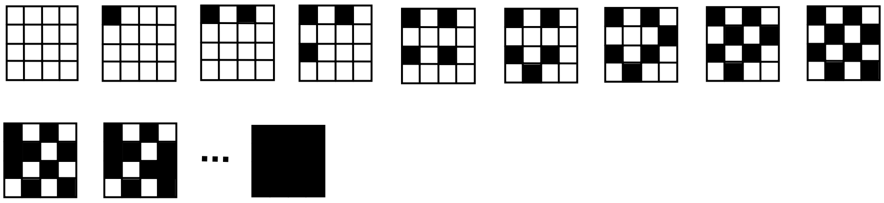
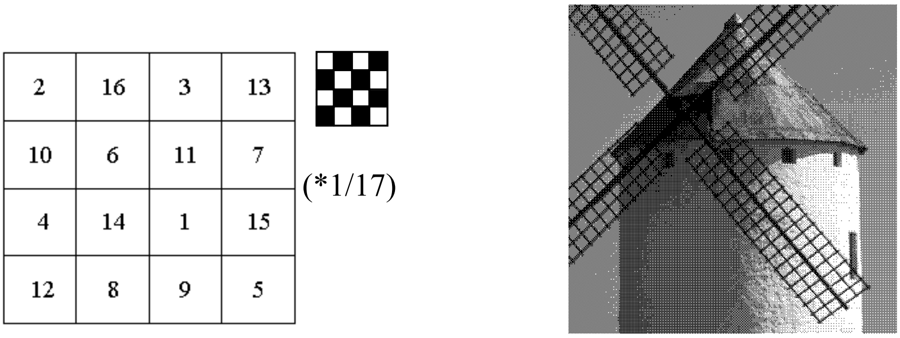


Figure 2.10: An illustration of FM halftoning in which to obtain different graylevels pixels within a cell are placed in dispersed order.



2	16	3	13
10	6	11	7
4	14	1	15
12	8	9	5

(*1/17)

(a) (b)

Figure 2.11: Illustration of Dispersed-Dot-Ordered Dithering, (a) 17 level Dispersed Dithering cell, (b) resulting halftone image. Next to top-right corner of Figure (2.11a) is shown its pixel representation for 0.5 graylevel.

It is to be pointed out that in some techniques, called hybrid halftoning, both AM and FM techniques are combined to get benefit of the advantages of AM and FM techniques [Goo01]. In hybrid technique, a filter is applied on the original grayscale image and based on the output of this filter either AM or FM technique is employed for halftoning purpose. In relatively smooth regions AM technique is applied, whereas in the regions pattern changes quickly or regions having detailed information FM technique is applied. However, it is to be pointed out that even after the joint application AM and FM techniques, the resulting halftoning images are of not very good quality [Figure 2.7(b) Goo01] as compared with other techniques such as the Error Diffusion and Iterative halftoning techniques.

2.4.4 Error Diffusion Halftoning

The error diffusion (ED) halftoning technique, pioneered by Floyd and Steinberg in 1975, results in better image quality as compared with other techniques discussed so far [Goo01]. According to ED technique whole grayscale image *g*, assumed to be scaled between 0 (white) and 1 (black), is processed in a raster order. A pixel at a given location is binarized using a fixed threshold level (0.5) and the error, which is the difference between the original pixel value (grayscale value) and its resulting binary value, is diffused to a fixed-size neighborhood region whose elements yet have to be processed. The error diffusion is accomplished by a *filter* (a key-element of the ED halftoning), which distributes a % of the error to each of the pixels in the desired neighboring region. A generic ED algorithm is shown Figure 2.12.

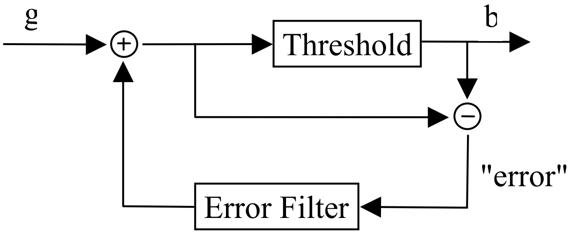


Figure 2.12: Error Diffusion Algorithm [Kan99].

The well-known filter given by Floyd and Steinberg is shown Figure 2.13a in which *X* is a location corresponding to the grayscale pixel under consideration for which error value after binarization is to be diffused. The error is diffused to the immediate neighboring pixels (right, below, lower-right and lower-left corners) and the amount of error passed to each of the neighboring pixels is determined by filter weights (7/16, 3/16, 5/16 and 1/16). It is noticeable that the filter weights add up to one so that error is not amplified. The weights are not selected randomly, but taking into the account the effects of resulting halftone image quality and are selected in a way that 0.5 grayscale stripe results in checkerboard pattern; however, this property (i.e. checkerboard pattern) is not suitable for data hiding application as it gives rise to pepper-and-salt noise (as we shall see in Chapter-5). Furthermore, the filter weights and size play a crucial role in the quality of the ED halftone images. An image resulting from the application of ED halftoning is shown in Figure 2.13b. As it can be observed from the figure that ED technique results in more pleasing images as compared with the halftoning techniques discussed earlier and this is due to the capability ED technique to produce more fine details of the original image. However, the noise in some areas is observed as well. Many variations in the family of ED technique have been proposed. In some ED techniques error is diffused in the forward, downward as well as backward direction, whereas in others different sizes and weights for ED filter are considered. A quality comparison of halftone images for ED filters with different weights and sizes is made in [Goo01, Kan99]; however, none of these techniques completely eliminates the noise. A good biography on ED halftoning can be found in Chapter 16 [Kan99].

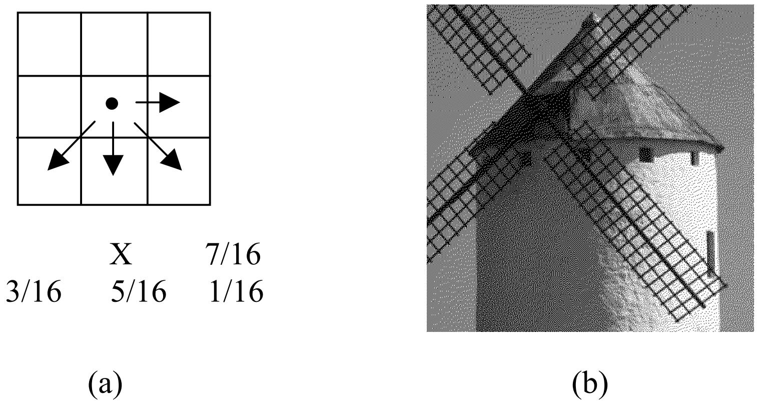


Figure 2.13: Error Diffusion halftone technique, (a) ED filter for 16 levels grayscale image, (b) resulting halftone image.

2.4.5 Iterative Halftoning

In an iterative halftoning technique also known as search based halftoning, unlike previously considered techniques, which work on either pixel-by-pixel basis (ordered dithering halftoning) or on a small region (ED halftoning), the whole image is considered at once. The grayscale image is first binarized using some appropriate thresholding method. Next the error between the binarized image and the original grayscale image is minimized iteratively using some suitable error measure, while the binarized image is kept modifying during each iteration. And this iteration process continuous, until a predefined error criteria is met. Since the human eye act as a low pass filter, usually the error between the low-pass filtered versions of the original and the halftoned image is checked; however, many other methods apart from comparison between the low-pass filtered images have been considered as well. The iterative halftoning techniques, are computationally more expensive as compared with the ordered dithering and ED halftoning, but are getting more and more popularity due to their higher quality and fast increase in computing power. Again, some good references can be found in Chapter 17 [Kan99]. A novel iterative halftoning technique [Goo01] discussed below, is of special interest to us due to its higher image quality and is used in this work while developing watermarking technique for the printed grayscale images.

The algorithm is now summarized in Figure 2.14. First, the original image *g*, is filtered with filter *f*. Then the position of the largest density value in f_g is found and a dot is placed at the same position in *b*, which is completely white to begin with. Then *b* is filtered with filter *h* and the difference $f_g - h_b$ is made. The position of the largest density value in $f_g - h_b$ is found again and the next dot is placed at this position and so on until a certain number of dots are placed in *b*. The number of dots to be placed is decided by the sum of the density values in *g*. Something worth mentioning here is that in constant images all pixels hold the same value and the program will return the first (or the last) pixel it meets as the position of the maximum. This can cause the resulting image to be highly structured when halftoning a constant image. By adding small quantities of random noise to the grayscale image, this effect can be avoided.

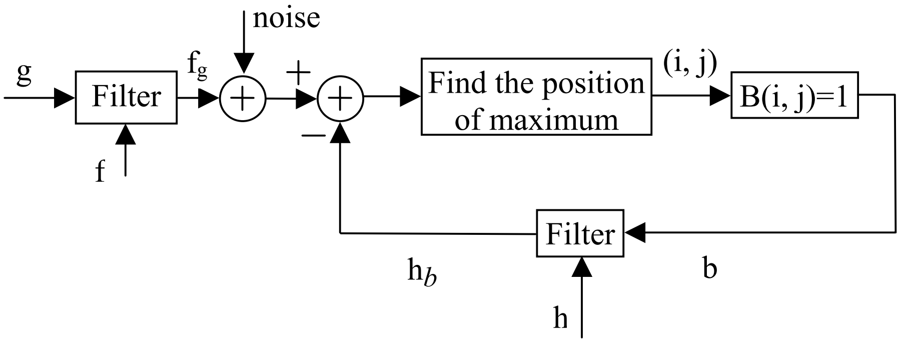


Figure 2.14: The Iterative halftone algorithm [Goo01].

It is to be pointed out that two *differen*t filters are used to filter the original grayscale image and binary image. However, two filters do not differ significantly and the filter used in binary image has different parameter values only. In addition to this, the filter applied on the binary image uses different size when it is used to place dots in very light and dark regions. Whereas for the graylevels having values varying between 10-90% the same filter size is used. Details about the filters can be found in [Goo01]. A halftone image resulting after the application of above iterative halftoning technique is shown in Figure 2.15.

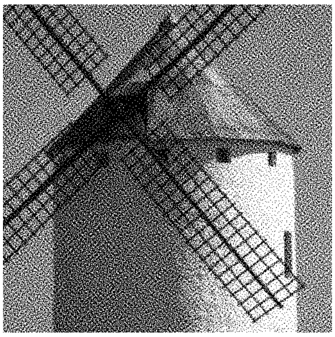


Figure 2.15: Illustration of the Iterative halftoning image quality. The halftone image is provided by the author (Dr. Sasan Gooran).

2.5 Scanning Process

The scanning process is an analog-to-digital conversion process. In this process input analog signal (e.g., hardcopy documents, photographs) is converted into digital form by the optical sensors. To obtain a digital sample at a specific location that location is illuminated and the reflected light is focused by a lens on an optical sensor, which generates an electrical signal proportional to the intensity of the light detected by the sensor. Between the lens and optical sensors typically three different filters are placed, which split the light into red, green and blue components before the light is detected by the sensors. The above scenario (shown schematically in Figure 2.16) is implemented in a single device, known as scanner.

The response of an optical sensor at any location in a scanner can be described formally [ShT97] as follows:

$$t_i^s = \int_{-\infty}^{\infty} f_i(\lambda)\, d(\lambda)\, r(\lambda)\, l_s(\lambda)\, d\lambda + \varepsilon_i \qquad i = 1,2,...,K \quad (2.2)$$

where K is the number of scanner color recording channels, $\{f_i(\lambda)\}_{i=1}^{K}$, are the spectral transmittances of the color filters, $d(\lambda)$ is the sensitivity of the detector used in measurements, $l_s(\lambda)$ is the spectral radiance of the illuminate, $r(\lambda)$ is spectral reflectance of the area being scanned, ε_i is the measurement noise, and t_i^s denote the value obtained from the ith channel.

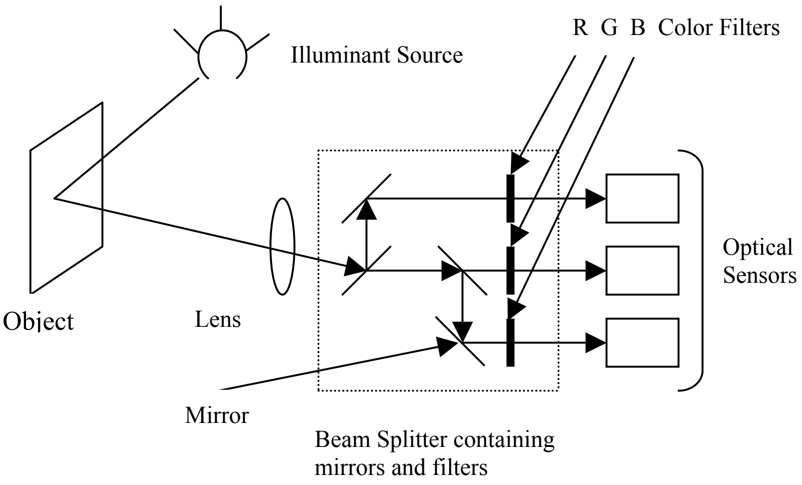


Figure 2.16: Schematic diagram of a scanner.

The quality of a scanning device depends on the following components:

1. Optical Sensors: This is perhaps the most crucial component of any scanning device. There are three different types of sensors: 1) Photomultiplier Tube (PMT), 2) Charged Coupling Devices (CCD), 3) Contact Image Sensor (CIS), in use nowadays.

The PMT a vacuum tube that converts light energy into electrical signal and *amplify* it, is used in high quality drum scanners because they are more sensitive to light as compared with CCD sensors. The CCD a miniature photometer that merely detect light intensity and represents the intensity with analog voltage unlike PMT, which not only precisely converts the detected light into analog signal, but amplify/multiply it as well, are widely used in desktop scanners. Finally, CIS is newer technology, which integrates scanning functions into fewer components, allowing scanners to be more compact in size due the smaller sensor size as compared with CCD. These sensors are used in low cost scanners and result in poor color and image quality as compared with CCD.

2. **Illumination Source** A high quality illuminating source must have the following characteristics: 1) full spectrum of light, 2) stable and long lasting, 3) lower power consumption rate, 4) lower temperature, 5) short initiation time. The fluorescent bulbs, used in the earlier scanning devices and still in use in lower-end devices, have two major drawbacks that they do not produce consistent white light over long period and have higher temperature, which affects the operation of other optical sensors. The "cold-cathode" bulbs, used in the existing high quality units, do not use light filament and result in lower-temperature devices. These light sources improve the performance due to the fact that at lower-temperature optical sensors perform better and otherwise optical *devices* need to be isolated, which increase the cost and size of the device. The Xenon bulbs are the latest and highest quality light sources with the properties that they are stable, long lasting, full light spectrum and have short initiation time. However, Xenon bulbs have one drawback that their power consumption rate is higher as compared with "cold-cathode" bulbs.

3. **Lens, Beam Splitters and Color Filters**: These optical components are used to focus, redirect and split the light beam reflected from the object being scanned and play crucial role in the quality of scanned image. In a high-quality scanner high-quality glass lenses are used, which are color-corrected and coated for minimum diffusion, whereas low quality devices use plastic lenses. To split light beam into portions, in low quality devices thin glass mirrors at angular position are used, whereas in high quality devices two right angle prisms connected together are used. The color filters have the characteristics of selective transmittance, capable of passing a certain part of the electromagnetic spectrum while being opaque to the other portions.

4. **Scanner Resolution:** It is the number of samples a scanner is able to take in a unit area (pixels/dots per square inch) and it depends on the two factors: 1) the number of optical sensors in a scanner head, and 2) step size of the stepper motor. A device offering 600 dpi resolution uses 600 optical sensors in linear sensor array (scanner head) and a step size one inch. There are two types of resolutions, optical resolution (actual resolution) and interpolated resolution. Optical resolution depends on the number of

sensors used in the sensors array and the step size of the stepper motor, whereas interpolated resolution is obtained using special interpolation techniques on the optically obtained samples and provides much higher resolution. It is noteworthy that the higher resolution allows capturing more details in the scanned image. However, the resolution offered by the newer scanners is much higher than the requirement for the most of the existing scanner applications such as photographs, text documents etc. In other words to scan an image/document at full scanner resolution (e.g. 4800 dpi) does not increase the quality of the image whether the image is scanned for reproduction or to put on a computer screen. A general rule for optimal scan resolution is given below:

$$SR = (DR \times DW) / OW, \tag{2.3}$$

Where SR = ideal scanning resolution, in dpi

DR = resolution of final display device, in dpi

DW = width at which the image will be printed or displayed, in inches

OW = width of the original being scanned, in inches

There are new applications such as those focused in this research, which require that the image is scanned at a higher resolution and such applications have importance not from visual quality point of view but rather for machine vision purpose.

5. Dynamic Range: It is the range of tones that a scanner can record and depends on the purity of the illuminating source, *optical glass* colored filters, *optical* lens and system noise. This range in ideal case varies between 0.0 (pure white) to 4.0 (pure black), however, for the existing flatbed desktop scanners dynamic range value is 2.4, which is sufficient for many applications, and indicates that the device is not able to distinguish at very light and very dark color tones. In the best quality flatbed scanners dynamic range increases up to 2.8-3.2, by using extra bit-depth and improved optics and such devices are used in standard color prepress. Finally, ultimate dynamic range is offered by the drum scanners, which provide dynamic range between 3.0 and 3.8, and are very costly and provide over-kill quality for most of the applications.

2.6 Distortions Encountered in Print and Scan Process

When paper is used as high-density storage media this means that exact data is to be recovered from all the distortions encountered during PS process and this fact demands to study the *joint effects* of PS process. The major PS process distortions include: 1) Rotation, 2) Data expansion/shrinkage 3) Pixel value distortion. In the following first two distortions will be discussed whereas the third one has been briefly introduced in section 1.3.3 and the more details are left to Chapter 3.

2.6.1 Image Skewing

It is a small amount of unavoidable rotation an image/document encounters during the PS process and it is attributed to both the printing as well as scanning processes. This amount of rotation is usually not very significant and in conventional applications it is unnoticed. The skewing effects are unavoidable even in high quality *printing process* and this fact can easily be verified by printing a test image of fixed size using advanced printing facilities available at photographs printing labs. From the printed test image it can be seen that the image is printed 3% bigger than its original size and the purpose of this increase in size is to compensate for the skewing effects. While considering joint effects of PS process, it is observed in this research and reported in [FuA02] as well that regardless the fact that how precisely a document to be scanned is put on the scanner bed, certain amount of rotation is unavoidable.

Next it comes whether such small amount of rotation is significant or not. The answer is that it depends on the application. As mentioned above, although certain amount of rotation is occurred during photographic printing process, however, such effects are easily compensated (at the expense of slightly higher cost attributed to wastage due to high quality paper and inks) in such applications by printing the photographs with 3% extra size and then cutting the extra size. Consequently, there are no aftereffects in this application. However, in other applications (pattern recognition, OCR, using paper as a high density storage media) where ultimate goal is to recover with minimum error the original information from digitized image, in this case even slight rotation is very significant and requires quite serious measures to count for such distortions.

Another important factor while consider skewing effects is quality of the underlying application. For instance, slight rotation doesn't cause any problem in data recovery process if the encoded/printed data is not of very high density (e.g. data printed at 75 dpi and scanned 300 dpi). Practical example can be that when data is encoded in conventional low-density barcodes such small amount of the rotational distortion is not significant as registration marks added around the barcode can easily be used to compensate for such distortion. However, when the objective to recover the hidden data from high quality printed image (e.g. HD-DataStripe), where registration marks can only be added around the image then even slight rotation is significant and increases the error rate in the recovered data quite significantly. And this is due to the reason that at higher density noise is so strong that even small rotation gets significant.

2.6.2 Document Expansion/Shrinkage

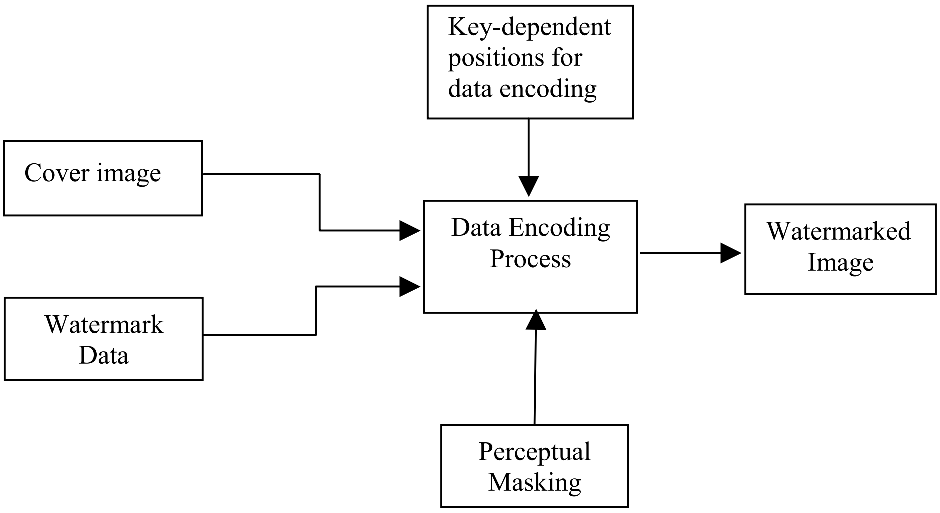
Another important distortion encountered during PS process, or only during printing process, is the document shrinkage. And this fact has already been observed by the printing industry that certain amount of the document shrinkage occurs during the printing process. In this research it is also verified that printed document suffers from the shrinkage effects. As mentioned above in the discussion on unavoidable rotation that slight modification in the printed document at higher resolution (high density barcode) has significant effects. Now for shrinkage effects, imagine the scenario that a data stripe is printed at 300 dpi, however, when it is scanned at 300 ppi resolution, there is only 298 pixels per inch. So what could be done, as any interpolation technique cannot be used as the exact data recovery is targeted. On the other hand if the document is sampled using the sampling interval at equal distance, obtained by dividing the new length (obtained after scanning) by the original length it would still not be effective and it would still not allow to recover the original information accurately.

2.7 Digital Watermarking

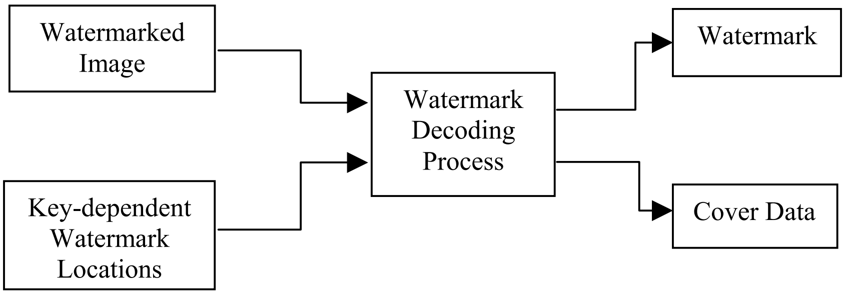
Inspired by the fact that fundamental principles for watermarking techniques for hardcopy documents (to be discussed in Chapters 5 and 6) are borrowed from digital watermarking concepts, here a brief introduction to the topic is given. Digital watermarking *conventionally* allows authenticating the ownership of valuable digital contents: still images, audio and video signals by assigning copyrights. In digital watermarking a watermark (short message usually consisting of company name, logo etc.) is encoded imperceptibly in the underlying contents to be assigned copyrights/ownership. For ownership authentication the watermark is decoded from the contents and given as a proof of ownership. A general watermarking technique is shown in Figure 2.17. Data encoding process takes two signals: cover data (contents to be copyrighted) and the watermark, as a input, selects the positions for data encoding using appropriate technique and embeds the data at selected positions according to the criteria employed by the perceptual masking technique. It is to be mentioned that watermark size is determined by system's data encoding capacity, which is constrained by the perceptual masking and robustness against the alterations the application is going to encounter. The order of positions might be key-dependent, if desired, for authorized decoding of watermark. The watermark decoding process begins with watermarked contents by selecting those positions, which have been used by the watermark encoding process, and reads the watermark at selected positions.

An effective watermarking technique must successfully deal with the triple requirement of imperceptibility, robustness and capacity [PZ96, VPIP01]. *Imperceptibility* requires that the marked and the original contents should be perceptually indistinguishable. *Ro-*

bustness refers to the successful decoding of watermark from marked contents, which have gone through alterations. *Capacity* is amount of data that can be encoded as a watermark. Furthermore, there are two more properties: security and uninformed decoding, which are also highly desirable. Security constraint refers to unauthorized decoding of the watermark and requires that the watermark not to be decoded by unauthorized people. Neither, it can be copied from one contents and used to other contents. The uninformed decoding requires that the knowledge of original contents should not be needed for watermark decoding. All these requirements are inter-correlated in a complex manner and are application dependent as well.



Block diagram of general data encoding process.



Block diagram of watermark decoding process.

Figure 2.17: Block diagram of the watermark encoding and decoding process.

The work on digital watermarking can be classified according to encoding and decoding process. While considering encoding process all data encoding techniques either work in spatial or in transform domain. In spatial domain a single pixel or a group of pixels is modified to encode single watermark bit. The data encoded in spatial domain is very sensitive to translation, rotation, cropping and data compression attacks and this leads to consider data encoding in transform domain. In transform domain cover data is transformed using any of the transforms (DCT, FFT, WT) and again single or group of components is modified to encode single bit. The level of modification (e.g. least significant bit in spatial domain and low-frequency components in transform domain are imperceptible) is governed by perceptual masking technique, which exploits the limitations of human perceptual systems (visual and acoustics) to introduce modifications. In [PoW98] a model based watermarking encoding technique is given, which takes into account human visual system (HVS) model to encode watermark in transform domain. Like encoding process, watermark decoding process can be classified into two categories: informed (blind) and uninformed (non-blind) decoding. In informed decoding original cover data is required and watermark is decoded by taking the correlation between the marked and original contents. In uninformed watermark decoding the original image is assumed unavailable and usually the statistical properties of the watermarked image are utilized. A detailed discussion on different watermarking techniques can be found in [CMB+01], whereas in [MoS98] the problem is addressed from information theoretic point of view.

Digital watermarking techniques can be classified as: robust and fragile. In robust watermarking objective is that the watermark payload is robust against the conventional image processing operations (e.g. lossy data compression, cropping, scaling etc.) and should not be removed without significantly degrading the quality of watermarked contents. The *fragile watermarking* techniques on the other hand deal with contents integrity and authenticity. Fragile watermarking techniques have two important characteristics: robustness against conventional image processing operations or innocent distortions and sensitivity to malicious contents tampering attacks. It is to be mentioned that in context of this research, which focuses on watermarking technique robust against PS-process, innocent distortions consist of noises encountered from halftoning process, PS-process and dust-and-scratches. Some fragile watermarking techniques, which are relevant to this research are reviewed in the following.

In [Kim05] H. Y. Kim has given contents integrity and authenticity verification technique for binary/halftone images. To ensure contents integrity host image is divided into regions *A* and *B*, each region containing different number of fixed-size (e.g. 3 x 3 pixels) non-overlapping blocks. Next value of central pixel of all the blocks in region *B* is turned to zero and message authentication code (MAC) or digital signatures (DS) of resulting host image consisting of regions *A* and *B* is computed and embedded into region *B*. The size of the region *B* has been determined by the size of MAC (128 bits) or DS (1024 bits for RSA) to be embedded. Furthermore, blocks constituting region *B* are selected with the constraint that the central pixels modification results in least visual distortion *(transparency constraint*), and a pseudorandomly selected sequence of blocks has been used. For contents integrity verification, embedded MAC/DS is extracted and compared with the one computed using same procedure as before and if both are matched then contents integrity is ensured. Both secret-and public-key versions can be used for contents integrity and authenticity verification. It is to be pointed out that technique can detect contents tampering attack up to single pixel, but cannot either localize the modified parts or distinguish between innocent and malicious content changes. The technique [WoM01] from Memon et al. for grayscale images not only detects but also locates up to single pixel contents changes and works with both symmetric and public-keys. Here host image is divided into blocks and message digest of each block combined with watermark block using XOR (exclusive-or) operation is embedded in LSB (forced to zero before computing message digest and embedding the watermark) of corresponding block pixels in encrypted form. There are also *invertible fragile* watermarking techniques [DSF02] that are targeted for applications in which the *original* (unmarked contents) from the watermarked image are to be obtained. Here contents of data embedding region are compressed to spare space for DS embedding. Next, DS concatenated by compressed data are embedded in the data embedding region. To get original contents back, the compressed contents related to data embedding region are separated from the watermark, decrypted and substituted back in embedding region (at the positions known by the public-key). One drawback of the above mentioned techniques is that they are not robust against conventional image processing operations and to address this point semi-fragile techniques are given.

A semi-fragile watermarking technique [Ditt01] uses visual features of the contents for contents integrity verification. Here the visual features of the contents are extracted and encoded in a feature vector that is embedded into the image using a robust watermarking technique. In feature selection and extraction process, capacity constraint imposed by the robust watermarking technique is taken into account. For performance evaluation both types of noises: innocent (luminance reduction, contrast reduction, scaling, additive noise, sharpening, softening, JPEG and MPEG compression) and malicious (different types/sizes of objects are added/removed as contents modification attacks) are considered. Key point concerning to us is the possibility to extend the underlying principle to hardcopy scenario (for binary images) for contents tampering detection and localization. This would require modifying the existing visual feature extraction techniques for binary images by taking suitable measures and then *watermarked* binary image (not watermark) recovered from PS-process can be used accordingly to detect and differentiate between the innocent and malicious changes as well as locating maliciously modified regions.

There is another category of semi-fragile watermarking techniques known as hologram watermarks, which use computer generated holograms for contents integrity verification [DFV01, DSF02, FMF+02, SSC05]. According to [DSF01], computer generated holograms can be considered as another way of conternts feature extrcation. Hologram watermarks are robust against cropping attack, allowing contents integrity authentication from small part of the watermarked contents. In addition to this, they have the following drawbacks: reconstructed hologram watermark is similar but not exactly same as the encoded one and this fact makes it suitable only for visual contents integrity authentication but not for biometrics-based automatic authentication, which requires exact data recovery for template matching. This problem is addressed in [FMF+02] using error correction coding, which increases data size that has other consequences (violation of capacity constraint). The hologram watermarks for images and biometrics data have high capacity demand that is not easy to meet for hardcopy documents and how this capacity demand is met in [FMF+02] is unclear to the author.

Common weakness of the above techniques except hologram watermarks is that they are applicable to digital contents but cannot be applied directly to hardcopy documents where certain amount of errors/distortion is unavoidable due to PS-process. Furthermore, they demand for higher capacity (watermark payload) except [Ditt01].

The above discussion on watermarking is applicable to any kind of digital contents: still images, video and audio, and a lot of literature [International Conference on Information Hiding, SPIE Conference on Security Steganography and Watermarking of Multimedia Contents, SPIE Conference on Optical Security and Counterfeit Deterrence Techniques, IEEE Transaction/Conference on Image Processing, are some of well-known sources] dealing with digital contents is available. In contrast to digital contents there has been reported very-less work, which deals with analog contents. The usage of digital watermarking technology in different applications since its emergence is shown in Figure 2.18. The literature dealing with hardcopy documents (image and text data) is reviewed in Chapters 5 and 6 where these applications are investigated.

An overview of the latest developments in analog security technologies can be found [Ami02, LN05, Phil00, Phil02, Phil04, PNW+04, Shi04, ShW04, Ren05, TcH04]. Briefly speaking, this literature deal mainly with first-line authentication by using advanced technologies to combat the counterfeiting and data-tampering attacks.

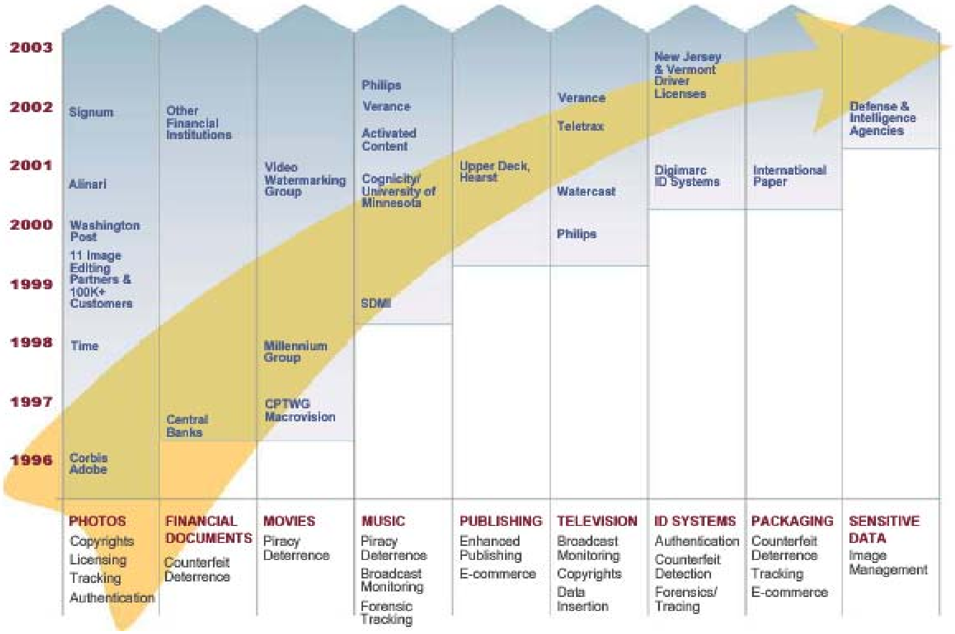


Figure 2.18: Evolution of digital watermarking technology since 1996 [DIGIMARC®]

Chapter 3
The Novel Data-Reading Technique for High Quality Printed Binary Images

3.1 Introduction

Despite their widespread existing use in many different application areas, recently *printed binary images* have attracted special attention among the research community for new applications [FuA02, HeO00, Wan01, WLH99, WuL04]. This trend is triggered from the advancements in computational power, printing, scanning and photocopying facilities, which are nowadays easily accessible to a very large community and have posed potential threat to many existing applications prone to forgery and counterfeiting. The new application domain, which is the main focus of the following chapters, is in the field of authenticity verification of hardcopy documents e.g. ID cards, traveling documents (visas, passports), conventional printed text documents, entertainment tickets etc. Some binary images for different novel applications are shown in Figure 3.1. In this chapter information recovery, while using paper as a storage media or communication channel, is focused upon and a Data-Reading Technique for the *novel HD-DataStripe* is given.

Before proceeding further, here some terms, which one will encounter quite often are formally described within the context of this research with the aim to avoid any confusion. In this research an image is considered as an *high quality printed binary image* if it is printed at 300 dpi or higher (pp. 10, sec. 2.3.1), which means that the size of the binary symbol (printed dot) is less than or equal to 84.67 microns. An HD-DataStripe shown in Figure 3.1f is a high quality printed binary image like the conventional 2-D barcodes (e.g. PDF417) with randomly arranged binary symbols and a registration mark pattern added around it. In HD-DataStripe *gain in capacity* is achieved by increasing the density of binary symbols (information carrying symbols). An information carrying symbol while considering paper as a communication channel (storage media), depending on the number of inks used in the printing technology, can take different values (i.e. can encode more than one bit per symbol); however, in present research only binary symbols (i.e. one bit per symbol) are considered. Furthermore, the binary symbols are interpreted differently in different contexts as explained in the following. A binary symbol is referred as a pixel in the context of original digital information and it is the smallest unit, which is intended to be recovered after PS process, i.e. binary symbol (pixel) is transmitted through channel (PS process). When this digital binary symbol is transferred to the paper, it is referred as a printed dot or simply a dot. Although, in reality a white dot does not exist due to white surface of the paper; however, for the sake of description it is assumed other way round and is referred as printed white dot or simply a white dot. Finally, when a printed binary symbol (dot) is scanned at higher resolution using over sampling criteria for information recovery, then it is referred as a binary-pattern, square-block or sub-matrix (to be referred onwards as submatrix for simplicity) and all these terms are used interchangeably in data recovery process. According to the above formulation, the data capacity per unit area, for instance, would be the number of pixels, dots and squares, in the context of digital (original information), analog and scanned contents, respectively.

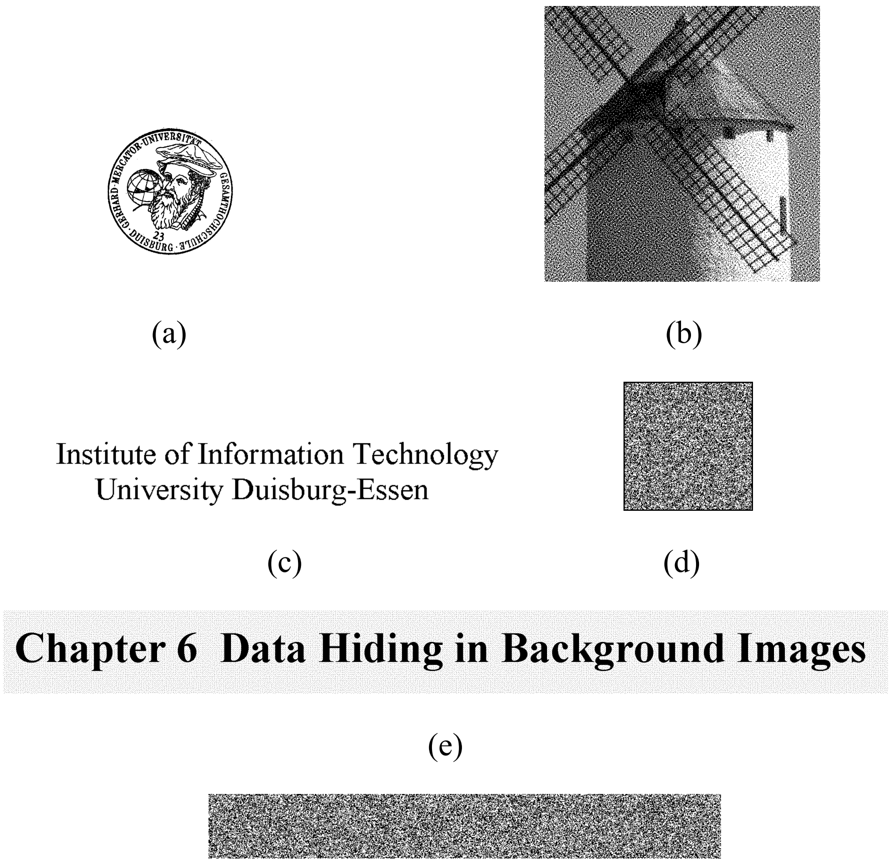

GERHARD MERCATOR UNIVERSITÄT GESAMTHOCHSCHULE DUISBURG 23
(a)
(b)
Institute of Information Technology
University Duisburg-Essen
(c)
(d)
Chapter 6 Data Hiding in Background Images
(e)
(f)

Figure 3.1: Some novel applications of the printed binary image: a) document authenticity verification seal with hidden data, b) an image with hidden data for ID cards application, c) a piece of text with hidden data for authenticity verification, d) a copy detection pattern for brand protection, e) a constant grayscale background image with hidden data offering sufficient capacity to encode many pages of full text in an A-4 size background image, and f) HD-DataStripe for Smart ID applications with sufficient capacity to store card holder photograph, biometrics data, biographical data etc.

To recover binary data after printing and scanning (PS) process, generally speaking any existing data-reading techniques [FuA02, Wan01, WuL04] begins by adding the registration marks around the digital binary image. These registration marks are intended to combat the geometrical distortions that are encountered during PS process and to obtain sampling points. Then the printed image is scanned as a grayscale image at a resolution that is at least two times more than the printed dot resolution, where the over sampling is intended to preserve the printed dots. The scanned grayscale image is binarized using *global* threshold level. Finally, the sampling points array is generated from the identified registration marks and the binarized image is sampled using the sampling points array to recover the *original* digital binary data. The key elements of any information recovery process are: 1) data capacity per unit area, 2) sampling points, and 3) binarization technique.

In [Wan01] registration mark pattern consists of 8 marks, which are located at the corners and at the middle of each of the four sides around the image. From the identified marks, sampling points array is generated, where each element of array contains (x, y) coordinates of a sampling point. To binarize the scanned grayscale image a single threshold level, which is the minimum point in the histogram of the *sampled* grayscale image, is applied. The histogram of *sampled* grayscale image is used to minimize the possible effects of noise from PS process on threshold level. To evaluate the performance of the data-reading technique binary image of size 256 x 256 pixels is printed at 75, 150 and 300 dpi and 0, 121 and 15927, errors out of 65536 are reported, respectively. It is mentioned that poor performance at 300 dpi is attributed to noise (dot gain effects) encountered from PS process at higher printing resolution and this imposes a limit on the amount of data that can be encoded. The data reading technique given by [FuA02] uses only 4 marks located at the corners as a registration mark pattern. Using the coordinates of the identified marks, the scanned grayscale image is partitioned into number of sub-blocks (squares), which is equal to number of pixels in the original image. To recover the original binary information sum of luminance values within the sub-block under consideration is thresholded. This technique is used to recover data from a binary image printed at 150 dpi. In another technique [Wu01, WuL04] intended to recover printed signatures, registration marks are placed more closely. The 50 and 25 pixels separate the sequence of marks along horizontal and vertical sides, respectively. For binarization purpose mean of the minimum and maximum luminance values of scanned grayscale image is used as threshold level. In this technique data recovery at 72 dpi is considered. In all of above-mentioned techniques, the data is recovered successfully when the encoded data does not suffer strongly from the noises (see Sec. 3.4) from PS process. Furthermore, the maximum resolution 150 dpi at which successful data recovery is reported, offers 22.5 Kbits (K=10^3) per square inch data capacity.

When using existing techniques to recover data encoded at 300 dpi, the errors are mainly due to the following points: (1) sampling points are not very accurate as such points are estimated using only couple of registration marks (2) to recover a single data value, binarized image is sampled at just one point. For instance, if there are just few white pixels (Figure 3.7) (or vice-versa) due to the poor binarization process or due to the strong dot gain (loss) effects within the square under consideration, then this is very likely that these pixels may not be at sampling point, resulting in wrong sampled value. On the other hand, in [FuA02] all pixels within the square are taken into account in the sampling process; however, strong dot gain effects force the sum of the values within square to be much lower and consequently the square will be marked as erroneously using global threshold level.

While developing novel data-reading technique for high quality printed binary images, originally all the ideas are given in this research. However, later on it was found that some of the ideas such as the application of over sampling and registration marks to certain extent have been used in [FuA02, Wan01, WuL01]. Key contributions of this research to recover binary data after PS process are summarized below and discussed in detail in the following sections.

3.2 Key Points of the Novel Data-Reading Technique

In order to combat the *unavoidable physical dot gain effects* encountered at higher printing resolutions (e.g. HD-Data Stripe), in this research dot gain effects are classified into two categories: 1) severe dot gain effects, and 2) relatively less severe (RLS) dot gain effects. This classification is based on the operational range of the printing device: linear, nonlinear operational mode (Sec. 3.4 pp. 42). The effects of both types of dot gain effects on the printed and scanned image are investigated and by keeping in mind the countermeasures to combat such effects are taken. Next, the RLS dot gain effects due to their special characteristics are focused upon and a binarization technique, called "Adaptive Binarization Technique", to handle such effects is given. Unlike the existing binarization techniques, which employ one single threshold level, the proposed technique takes into account the local variation in luminance value caused by the DGEs.

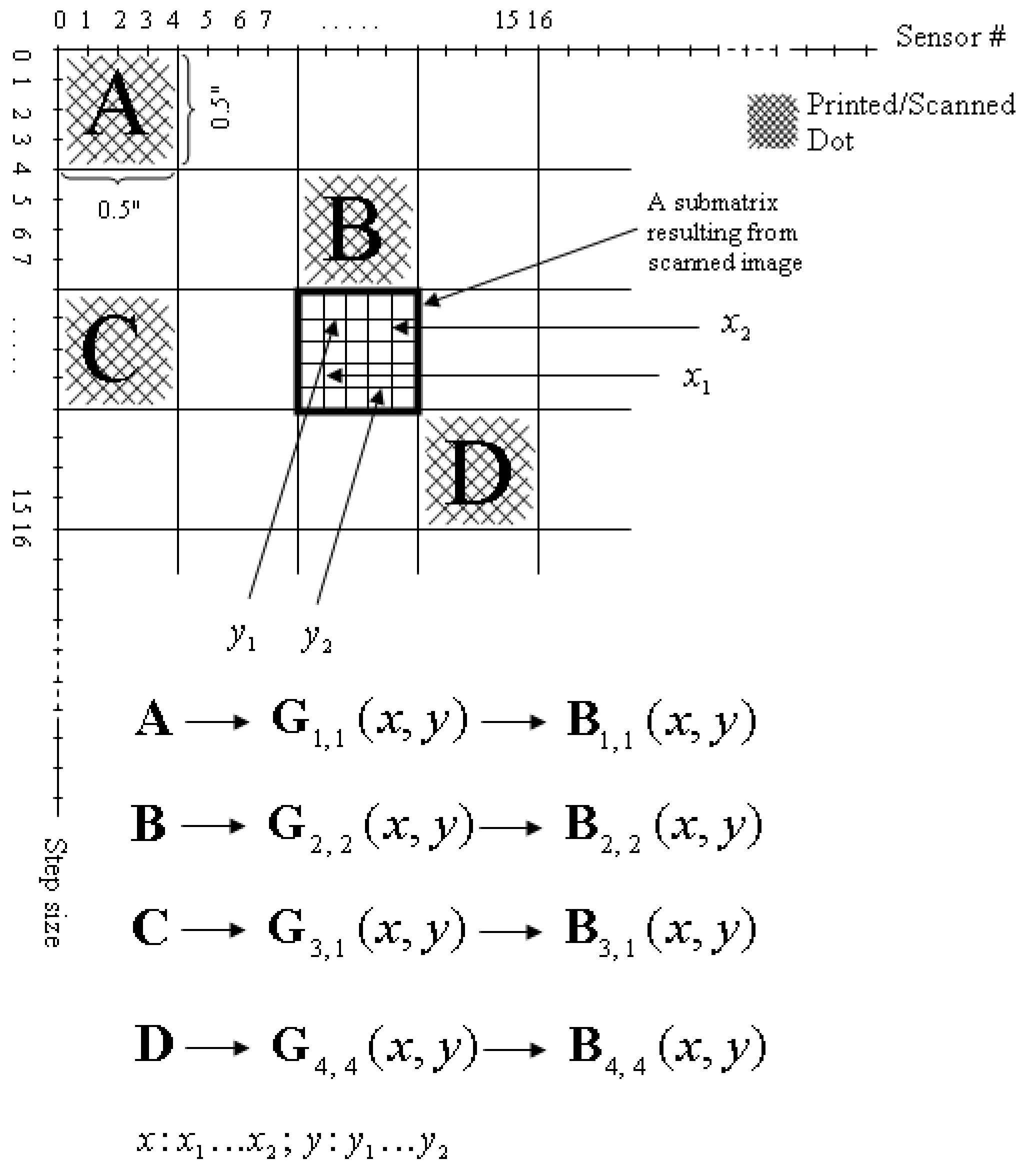
As the performance of the data-reading technique, targeted to recover data at higher data encoding rate, is very sensitive to the way in which registration marks pattern is designed and processed, the registration marks pattern in this research is designed in such a way that *no estimation* is needed to combat the nonlinear image shrinkage distortion encountered during PS process and this consequently results in more accurate sampling points array.

Finally, the most significant contribution of this work is that *the post data processing filters* are developed to process the binarized image. Each of these filters characterizes a binary-pattern (square block or sub matrix sec. 3.3) of a certain type based on the behaviour of pixels within that particular pattern and by taking into account the correlation (behaviour) of this pattern with its immediate neighbouring patterns. A particular pattern is processed according to the priority assigned to it. In other words in this research to recover the original binary data, the scanned image is sampled using Active Sampling technique (i.e. it applies post data processing filters in conjunction with adaptive binearization technique) in contrast to the existing techniques working in passive mode.

While considering the performance of proposed data-reading technique, for experimental purpose 7 printers and 2 scanners are investigated using both simulated and real-data. The robustness of technique against the common distortions encountered in practical applications such as: skewing distortion and wear-and-tear effects are considered as well. In case of wear-and-tear effects, the robustness of data-reading technique against contrast reduction, luminance reduction, dust-and-scratches noise, additive uniform noise and additive Gaussian noise is investigated. Each of the above points will be discussed in detail in the following sections.

3.3 Brief Mathematical Description

Before going into the details of the novel data-reading technique, it would be beneficial to describe clearly some mathematical terms, which are referred quite frequently in this chapter and can be helpful to understand the problem as well. Let us represent the scanned grayscale image and its corresponding binarized image by the matrices, $\boldsymbol{G}$ and $\boldsymbol{B}$, respectively. Each of the images $\boldsymbol{G}$ and $\boldsymbol{B}$, using the identified registration marks, is partitioned into $N = \lambda_1 \cdot \lambda_2$ submatrices (square blocks). Where N is the total number of pixels in the original digital binary image having λ_1 and λ_2 pixels in the horizontal and vertical dimensions, respectively. Each square block (with both sides having probably equal length) corresponds to a *certain printed dot* and is formed by scanning the image, using at least two times more than the printing resolution. The resultant partitioned matrices are represented by $\boldsymbol{G}_{i,j}(x,y)$ and $\boldsymbol{B}_{i,j}(x,y)$, where subscripts $i, j,$ denote a specific submatrix at ith row and jth column, and coordinates (x, y), denote the location of a particular pixel within the submatrix. The above description can be visualized more clearly with the help of sketch shown in Figure 3.2.



$$\mathbf{A} \longrightarrow \mathbf{G}_{1,1}(x, y) \longrightarrow \mathbf{B}_{1,1}(x, y)$$

$$\mathbf{B} \longrightarrow \mathbf{G}_{2,2}(x, y) \longrightarrow \mathbf{B}_{2,2}(x, y)$$

$$\mathbf{C} \longrightarrow \mathbf{G}_{3,1}(x, y) \longrightarrow \mathbf{B}_{3,1}(x, y)$$

$$\mathbf{D} \longrightarrow \mathbf{G}_{4,4}(x, y) \longrightarrow \mathbf{B}_{4,4}(x, y)$$

$$x : x_1 \ldots x_2 ;\ y : y_1 \ldots y_2$$

Figure 3.2: Illustration of matrices ***G***, ***B*** and sub matrices using PS process. Note: The size of printed and scanned dot is shown as 0.5", which requires 4 sensors and motor step-size (0.5/4)", at 4 times higher over sampling; however, this is only for demonstration purpose, as in reality there is very large number of sensors and very small motor step-size per inch.

For example, the expression, $\sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} G_{2,8}(x, y)$, computes the sum of all the grayscale values for *the pixels* ranging from $x = x_1$ *to* x_2, *and* $y = y_1$ *to* y_2, corresponding to the sub-matrix at the location 2nd row and 8th column (a pixel at location (2, 8) in the original digital image).

x_1, represents the first column of the submatrix under consideration,

x_2, represents the last column of the submatrix under consideration,

y_1, represents the first row of the submatrix under consideration,

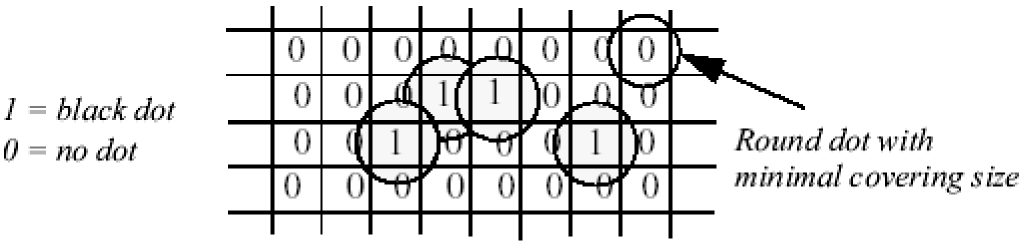
y_2, represents the last row of the submatrix under consideration,

$$x_m = \left\lfloor \frac{x_1 + x_2}{2} \right\rfloor, \qquad y_m = \left\lfloor \frac{y_1 + y_2}{2} \right\rfloor,$$

are the integer mean values, representing the central coordinates of a particular submatrix.

3.4 Countermeasures Against Physical Dot Gain Effects

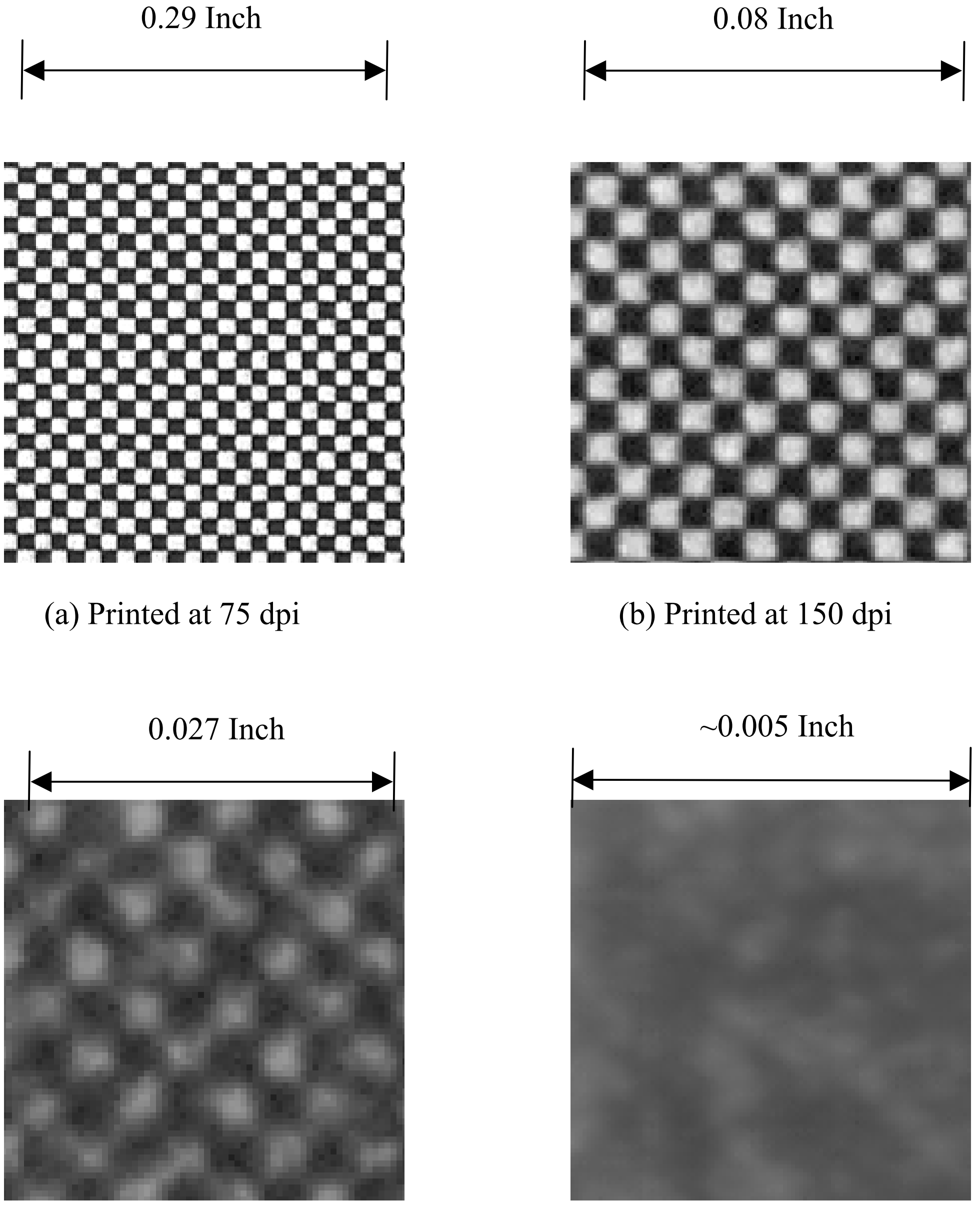
Formally speaking, while considering paper as a communication channel, physical dot gain effects *(more precisely PS process noise)* is the channel noise that limits the amount of data that can successfully (with very small bit error rate) be transmitted through the channel and is inversely proportional to the channel capacity (bits per square inch). Physical Dot Gain Effects are mainly caused by the circular shape Figure 3.3 and enlargement of the size of the printed dots. Its strength depends upon the underlying printing technology, ink, and paper quality. In [Goo01, Wan01] it is mentioned that at higher printing resolutions (e.g. 300 dpi or more) these effects are unavoidable, regardless the quality of the paper, printer, ink being used.



0	0	0	0	0	0	0	0
0	0	0	1	1	0	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

Figure 3.3 An illustration of physical dot gain effects development process [Goo01].

As a consequence of these effects, when a white dot surrounded by all or majority of the black dots is printed at a very high resolution, then the printed dot either turns completely into the black or partially black and white, depending on the quality of the printing device. The resulting dot gain effects corresponding to fully and partially black dots are referred as the severe dot gain effects and RLS dot gain effects in this research and are shown in Figure 3.4. Figure 3.4 shows the magnified view of printed and scanned binary image consisting of checkerboard patterns printed at various resolutions: 75, 150, 300 and 600 dpi to illustrate dot gain effects development process. The dot gain effects shown in Figure 3.4 demonstrate only one type of effects; however, there are other types of dot gain effects, which are discussed in sec. 3.7. Similar, to dot gain effects there are dot loss effects, according to which size of the printed black dot gets smaller and such dots might be expected from old printing devices or empty toner.

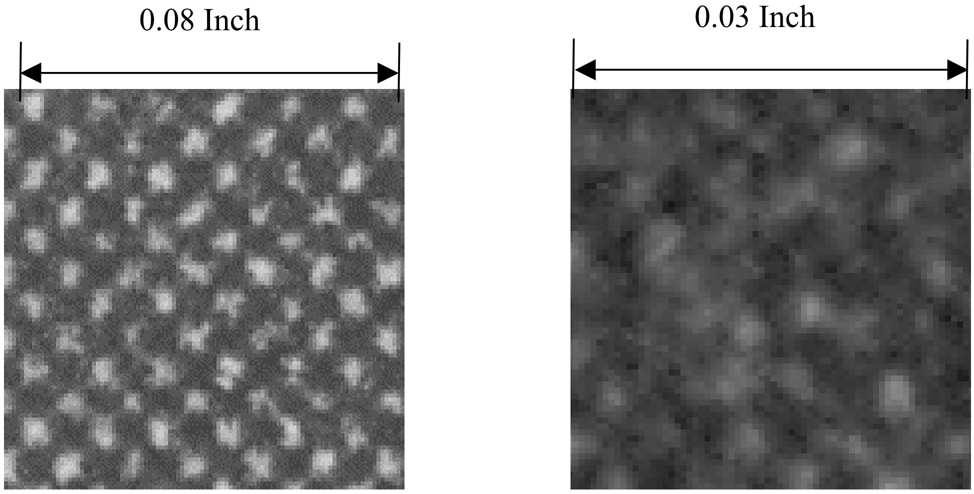


(a) Printed at 75 dpi

(b) Printed at 150 dpi

(c) Printed at 300 dpi

(d) Printed at 600 dpi



(e) Printed at 150 dpi (Inkjet)

(f) Printed at 300 dpi (Inkjet)

Figure 3.4(a-f): A *magnified view* of some printed and scanned images to illustrate dot gain effects: a) image printed at 75 dpi and scanned at 600 ppi, b) image printed at 150 dpi and scanned at 1200 ppi, c) image printed at 300 dpi and scanned at 2400 ppi (relatively-less severe DGE scenario), d) image printed at 600 dpi (full printer resolution) and scanned at 4800 ppi (severe DGE scenario). Note: images (a-d) and (e-f) are printed using the HP LaserJet 4600 and inkjet printers, respectively.

It can be seen from Figure 3.4 (d and f) that at full resolutions quite often printed white dots turn into completely black dots, which is an indication of existence of severe dot gain effects. This fact restricts full channel utilization that means to use paper as communication channel at full resolution. In existing work [Wan01] where a data-reading technique is given to recover data after PS process, it is mentioned that the physical dot gain effects encountered at higher resolutions, impose a bound on the volume of data that can be encoded in a printed binary image, which can be recovered correctly after PS. This last statement is very crucial for our purpose as the *primary* objective of this research is to develop a data-reading technique that can successfully recover data *encoded at higher printing resolutions* after PS process.

It is noteworthy to mention that the impact of dot gain effects is not same on all type of images and it depends on the application in which image is going to be used. From this perspective, printed images can be classified into two categories: 1) images targeted for high quality visual perception, and 2) the original digital image is targeted to be recovered back after PS. For first type of images dot gain effects have been studied very well and are compensated by varying the ratio of dots of basic half toning colors and this is done by the printer drivers, using some suitable half toning technique [Goo01]. For such images higher printer resolution usually results in higher image quality (visual perception) (sec. 2.3). On the other hand for images (e.g. Figure 3.1b, a watermarked halftone image) targeted to be recovered back after PS process, dot gain effects is an issue yet to be handled as the existing halftone-oriented measures are not applicable here due to the fact that pixel flipping is not permitted. Usual measure against dot gain effects for second type of images (text, graphics, HD-DataStripe) is to increase the signal energy [FuA02, HeO00, Wan01, Wu01, WuL04], which means the size of the data encoding binary symbol (dot) is to be increased. However, this approach has a drawback that it results in poor image quality (e.g. printed text or graphics see Figure 2.1), as individual dots are visible and lower data encoding capacity per unit area (e.g. PDF417 barcodes with few hundred bytes per square inch data capacity).

In this research a printing device is characterized by the linear and non-linear region of operation: the first region lasts until 150 dpi where there are no dot gain effects (Figure 3.4b), whereas the nonlinear region starts from above 150 dpi and goes up to full resolution and only this region suffers from dot gain effects.

The following countermeasures against Physical Dot Gain Effects are basically originated from the postulate:

Postulate: In nonlinear operating region a good-quality printing device is expected to print each and every dot *quite reliably* at half of its resolution. The reliability means that signal is distorted *less than* x% (e.g. $x = 90$) and the remaining *(100-x)%* signal information can be utilized by the sophisticated pattern recognition technique for signal detection. Furthermore, noise (distortion) and print resolution (signal energy) are directly proportional and are exponentially related:

$$N = c \cdot \exp(R) \tag{3.0}$$

Here, N is signal noise, R is print-resolution (signal energy) and c constant of proportionality. In this research eq. (3.0) is intended to show that N approaches to its limiting form (100%) more quickly than R reaches to full resolution and above relation gives only an indication of the behavior. It is to be mentioned that N and R in eq. (3.0) have to be normalized so that at $R=600$ dpi (full resolution), it results in 100% noise, similarly, for minimum values of R and N; however, this is not the target of this research.

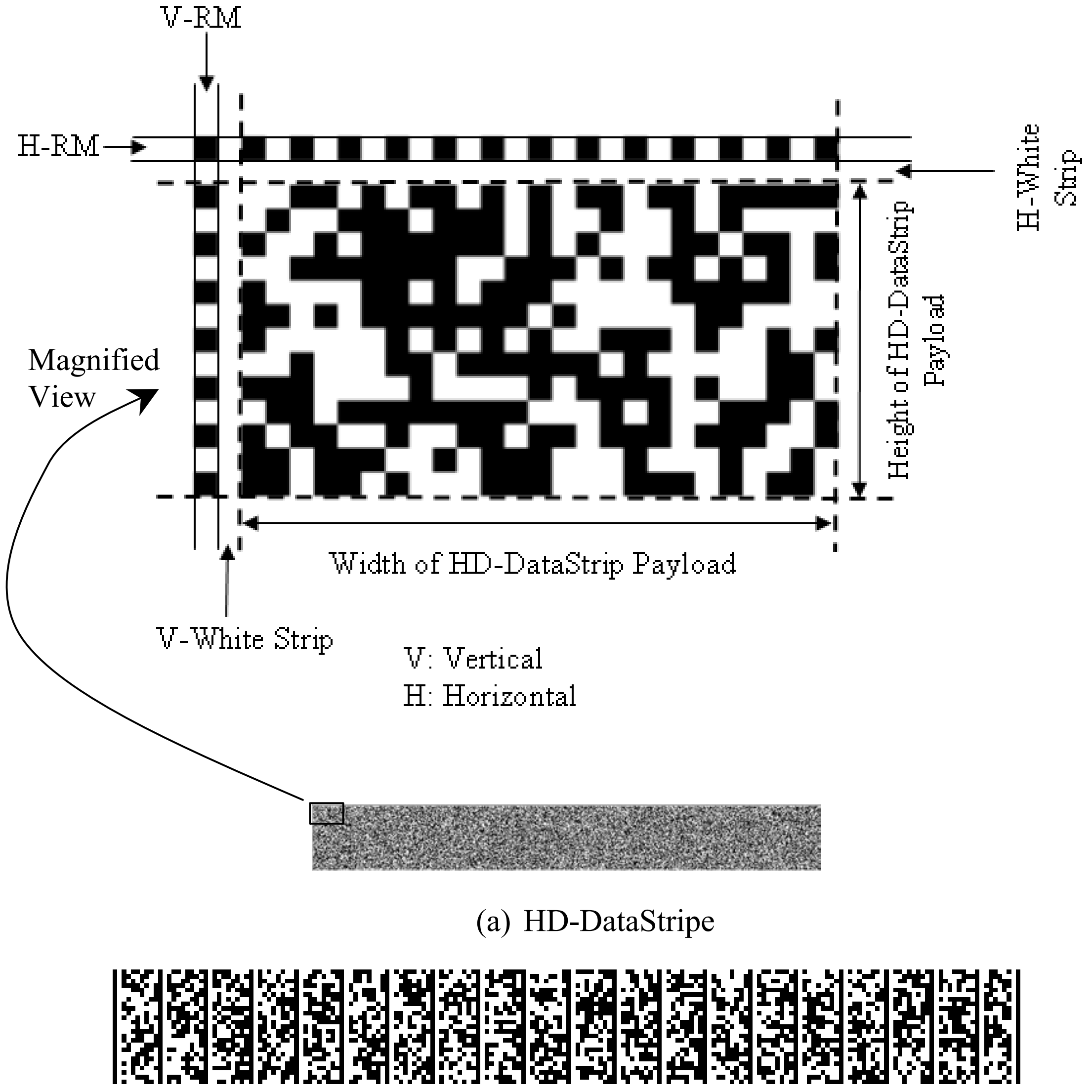
After the observation that severe dot gain effects (Figure 3.4 d and f) results in *complete* information loss, which is not permitted in the application scenario under consideration, it is decided to investigate relatively less severe (RLS) dot gain effects for the information-loss sensitive applications (Figure 3.1). This is encouraged by the fact that for RLS dot gain effects (Figure 3.4c), also information loss does occur; however, information carrying signal is not distorted beyond recovery and there still exists slight regularity in the signal, which can be utilized by adaptive binarization and post data processing filters to recover the original signal back and this is the objective of this research.

3.5 Proposed Registration Marks

Registration marks (RMs) is a specific pattern of binary pixels that is added around the digital binary image (e.g. HD-DataStripe), targeted to be recovered after PS process. The RMs are used: 1) to count for the geometrical distortions, 2) to find the sampling points. While considering geometrical distortions (e.g. rotation), RMs are used to estimate the amount of rotation a printed and scanned image encounters during PS process and then the scanned image is re-aligned accordingly. Furthermore, RMs is also used to estimate the sampling points (regions) at which the image is sampled to recover the original digital data. It is to be mentioned that in the context of this research the 2nd role of RM-pattern is much more crucial.

As the objective of this research is to recover data from a high quality printed and scanned image; where high quality means that image is printed at higher resolution, offering much higher data encoding rate per unit area. On the other hand resolution of the printed image and its dot size are inversely proportional and this fact results in small size dots (constituting the registration mark pattern) that are more difficult to recognize accurately. In this work while selecting the pattern for the registration marks, it is kept in mind that the estimation of sample points (regions) must be avoided as much as possible in order to keep the error contribution from the inaccurate sampling points at minimum level.

The RM-pattern proposed in this work consists of an alternating sequence of black and white pixels (in the context of original digital contents), which is added around the *image* (information carrying area of HD-DataStripe shown in Figure 3.5) and is separated from the image by one pixel wide horizontal and vertical stripes of white pixels. The one pixel separation between the RM-pattern and the information-carrying area of HD-DataStripe is intended to assist in the RM recognition process. This means that it protects the RM-pattern from the possible physical dot gain effects caused by the neighboring dots during printing process. In Figure 3.5 (a) a magnified view of a small part of HD-DataStripe image is shown to illustrate the RM-pattern. It is to be noticed that RM-pattern is almost imperceptible and consume very less space, resulting in further capacity gain due to the absence of separating bars that are used in conventional 2-D barcodes (PDF417) shown in Figure 3.5(b). Next, using the identified RM-pattern scanned image is partitioned into *N square blocks* (a square corresponds to a printed dot that is scanned at resolution more than the printing resolution) rather than sampling points and these square blocks are used for *Block Pattern Characterization* based on the *binary* as well as the *grayscale pattern* of the square block.



(a) HD-DataStripe

(b) Conventional PDF417 Barcode (magnified)

Figure 3.5: a) Magnified view of a small part of the HD-DataStripe to illustrate the registration marks used in the novel HD-Data Stripe, b) The registration marks (vertical black lines followed by separating vertical white lines) used in PDF417 barcode.

In order to identify the RM-pattern, the identification process for one element of RM-pattern proceeds as follows. First, the intended mark is isolated from its neighborhood by using its (luminance value) difference from the neighboring region. Then within the selected region a point corresponding to the minimum luminance value is found and is assumed as a central point. Next, the four boundaries of the mark are located by using the change in luminance value. To locate any two opposite boundaries, the process starts with the initial central point and moves a fixed distance by one pixel step-size in the direction in which luminance value decreases the least, whereas the fixed size stripe of pixels is considered to check the luminance value. This process is repeated until the opposite boundaries are separated by the desired distance. Then the exact central point is computed as the middle point of the square that is formed by these boundaries. Similarly, all marks in the RM-pattern are identified. Finally, the scanned image is partitioned by using the vertical boundaries of marks located on horizontal RM-pattern and horizontal boundaries of marks located on vertical RM pattern.

An important point concerning the above RM-pattern might be the higher computational time, which is true. While considering the processing time of RM-pattern, initially it is found quite high due to the pixel by pixel operations required to locate each of the registration marks. In other words using exhaustive search (i.e. each pixel in certain area around the scanned image is considered), starting from the top-left corner, each isolated pattern is located in certain area around the scanned image and then these identified patterns are processed to identify the whole RM-pattern. This approach obviously results in higher computational time. Next the higher computational effort is improved by utilizing regularity in RM-pattern and requires *only one mark* to be identified by the exhaustive search method, whereas to identify the next mark the immediate neigboring mark is searched at fixed step away from the central point of the already identified mark. Then a fixed region is selected to look for possible central point (corresponding to minimum luminance value) of this mark and this possible central point is used to find the exact central point as well as to locate its boundaries as discussed before. The utilization of regularity in RM-pattern results in very high computational gain in RM-pattern processing and reduces the computational time from several minutes to few seconds (Figure 3.20). It is to be mentioned that the computational time would be negligible while implemented in C language, unlike the existing MATLAB code that is computationally not very efficient.

3.6 Binarization Process

The binarization process converts the scanned grayscale image into a binary image by comparing each element of the grayscale image with a fixed threshold level and the thresholding operation results in a binary value “1” if grayscale value is above the threshold level and “0” otherwise. In binarization process, conventionally, one global threshold level is used, which could be a *minimum value* of a histogram of sampled grayscale, *average* of the minimum and maximum luminance values in a scanned image etc. The global threshold level is appropriate to binarize the images printed at a resolution up to 150 dpi and beyond that it cannot cope with the dot gain effects. In other words regions suffering from the dot gain effects are binarized erroneously. This fact degrades the performance of the data recovery process and can be seen from the existing work in which successful data recovery is reported up to 150 dpi. To combat the dot gain effects encountered for application scenario under consideration more sophisticated binarization techniques are needed that can cope with the distortions from PS process encountered at higher printing resolution (300 dpi) or data encoding rate. By keeping in view the adaptive binarization technique is given in this research. It is to be pointed out that in adaptive binarization technique the impact of dot gain effects is not fully addressed and for the remaining one post data processing filters are given.

3.6.1 Proposed Adaptive Binarization Technique

Driven by the fact that the binarization techniques using one single (global) threshold level are not suitable for images suffering from dot gain effects, the proposed technique employs 3 different techniques each one handling a specific category of dot gain effects. In other words dot gain effects are categorized into 3 categories and each category is handled by its corresponding binarization technique, which is especially designed for it. First, binarization technique handles those regions, which either do not suffer at all or suffer relatively less from dot gain effects. Whereas second and third techniques, which depend mainly on the local properties of the regions suffering from dot gain effects, are targeted to deal with the RLS dot gain effects (discussed in sec. 3.4) posed by the scenarios: 1) a white dot is surrounded by all or majority of black dots, and 2) a black dot is surrounded by all or majority of white dots, respectively. Each of these techniques is described in the following.

Initially the scanned grayscale image is binarized using a single threshold level as follows:

$$B(x,y)=\left\{\begin{matrix}1 & if\ G(x,y)\geq T_1 \\ 0 & otherwise\end{matrix}\right\}, \qquad (3.1)$$

where $x=1,2,..,\chi_1$, $y=1,2,..,\chi_2$ χ_1, χ_2 denoting horizontal and vertical dimensions of matrix $\mathbf{G}$, and T_1 is a threshold level having value 128 (50% of luminance value). The parameters used in this section and afterwards are given in appendix-C.

Next, the adaptive binarization technique works as follows:

If $\sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} B_{i,j}(x,y) \le T_2,$ (3.2)

holds, where the role of eq. (3.2) and its parameter value are discussed in the following, then the following statistics for submatrics *i, j* shown in Figure 3.6 are computed,

$$\overline{X}_{diff_1} = \left(\sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} G_{i,j}(x,y)\right)\Big/(x_2 . y_2) - \left(\sum_{x=x_1}^{x_2}\sum_{y=y_2-\alpha}^{y_2} G_{i-1,j}(x,y)\right)\Big/(\alpha . x_2)$$

$$\overline{X}_{diff_2} = \left(\sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} G_{i,j}(x,y)\right)\Big/(x_2 . y_2) - \left(\sum_{x=x_2-\alpha}^{x_2}\sum_{y=y_1}^{y_2} G_{i,j-1}(x,y)\right)\Big/(\alpha . y_2)$$

$$\overline{X}_{diff_3} = \left(\sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} G_{i,j}(x,y)\right)\Big/(x_2 . y_2) - \left(\sum_{x=x_1}^{x_1+\alpha}\sum_{y=y_1}^{y_2} G_{i,j+1}(x,y)\right)\Big/(\alpha \cdot y_2)$$

$$\overline{X}_{diff_4} = \left(\sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} G_{i,j}(x,y)\right)\Big/(x_2 \cdot y_2) - \left(\sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_1+\alpha} G_{i+1,j}(x,y)\right)\Big/(\alpha \cdot x_2)$$

where α is a fixed constant that controls the portion of the neighboring square, to be taken into account and its value for horizontal and vertical neighboring squares, respectively, is given by:

$$\alpha = \alpha_H = \alpha_V \qquad \alpha_H = \left\lceil \frac{x_1 + x_2}{2} \right\rceil, \qquad \alpha_V = \left\lceil \frac{y_1 + y_2}{2} \right\rceil.$$

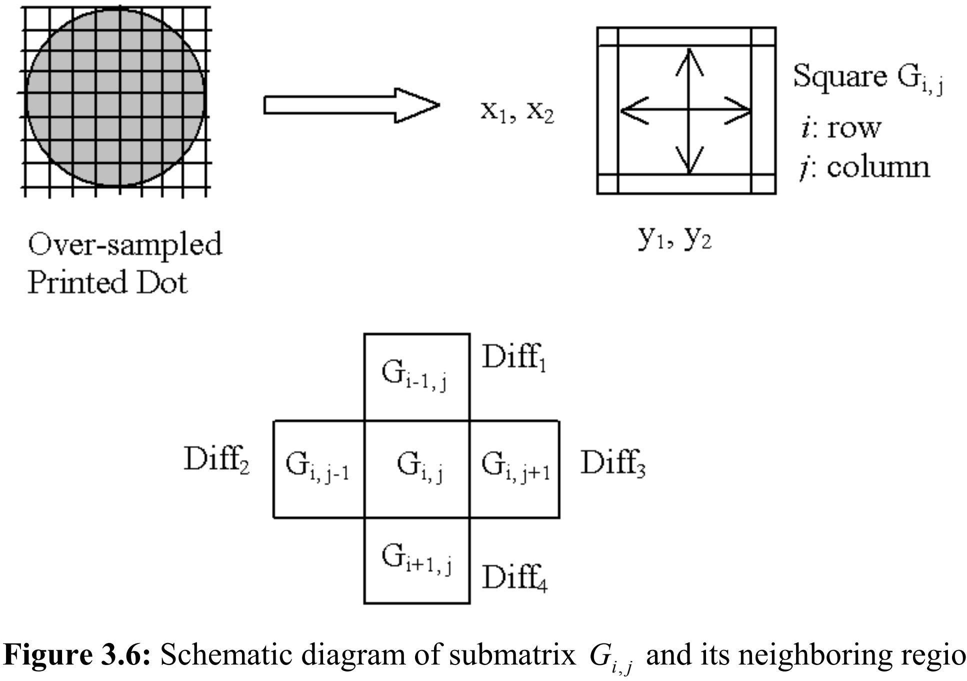


Figure 3.6: Schematic diagram of submatrix $G_{i,j}$ and its neighboring region participating in adaptive binaization process.

Finally, if any of the following conditions given by eqs. (3.3-3.6) is satisfied, then the square $B_{i,j}$ under consideration is marked as white.

$$\overline{X}_{diff_1} \geq T_3\,,\ \overline{X}_{diff_2} \geq T_3\,,\ \overline{X}_{diff_4} \geq T_3\,,\ \overline{X}_{\max_1} \geq T_4\,,\ \overline{X}_{\max_2} \geq T_4\,,\ \overline{X}_{i,j} \geq (1/2)\cdot \overline{X}_{i,j+1} \tag{3.3}$$

where $\overline{X}_{\max_1}$ and $\overline{X}_{\max_2}$ are the two largest elements of $X = [\overline{X}_{diff_1}, \overline{X}_{diff_2}, \overline{X}_{diff_4}]$. Similarly, other conditions can be formulated.

$$\overline{X}_{diff_1} \geq T_3\,,\ \overline{X}_{diff_3} \geq T_3\,,\ \overline{X}_{diff_4} \geq T_3\,,\ \overline{X}_{\max_1} \geq T_4\,,\ \overline{X}_{\max_2} \geq T_4 \text{ and } \overline{X}_{i,j} \geq (1/2)\cdot \overline{X}_{i,j-1} \tag{3.4}$$

$$\overline{X}_{diff_2} \geq T_3\,,\ \overline{X}_{diff_3} \geq T_3\,,\ \overline{X}_{diff_4} \geq T_3\,,\ \overline{X}_{\max_1} \geq T_4\,,\ \overline{X}_{\max_2} \geq T_4 \text{ and } \overline{X}_{i,j} \geq (1/2)\cdot \overline{X}_{i-1,j} \tag{3.5}$$

$$\overline{X}_{diff_1} \geq T_3\,,\ \overline{X}_{diff_2} \geq T_3\,,\ \overline{X}_{diff_3} \geq T_3\,,\ \overline{X}_{\max_1} \geq T_4\,,\ \overline{X}_{\max_2} \geq T_4 \text{ and } \overline{X}_{i,j} \geq (1/2)\cdot \overline{X}_{i+1,j} \tag{3.6}$$

T_3, T_4 are fixed constants *usually* taking value 5 and 15, respectively.

The purpose of eq. (3.2) is to reduce the computational time. If this constraint is relaxed then each square block will be considered as a possible victim of the RLS dot gain effects and consequently operations defined by eq. (3.3-3.6) will be performed on each square, which would result in much higher computational time. In other words even those squares, which do not suffer from dot gain effects at all, will unnecessarily be processed, resulting in higher computational time. The value of T_2 controls the strength of the dot gain effects to be considered and using $T_2 = 12$, allows the adaptive binarization technique to consider RLS dot gain effects as well. It is to be noticed that adaptive binarization technique given by eq. (3.3-3.6) does not depend on the binarized image, which is obtained using the single threshold level. Consequently, the role of T_1 in the context of adaptive binarization is not very crucial. It is also worth mentioning that the last constraint used in each of eq. (3.3-3.6) is intended to take into account more severe dot gain effects, which might be encountered in printing devices with slightly poor quality.

Finally, while considering 3rd category of RLS dot loss effects, a scenario in which isolated black dots (a black dot surrounded mainly by white dots) suffer from dot loss effects due to the inability of the device to print every isolated black dot precisely. This *dot loss* can be attributed to the fact that the aim of the conventional devices (unlike security printing devices) being used in offices is to give pleasing printed images (text, graphics etc.) for good visual perception and such devices are not intended to print each and every dot very accurately, a requirement from applications being considered in this research. Aging effects of the device as well as the *very low* ink or toner level might be the other possible causes of such effects. In this case the adaptive binarization process is given below.

If

$$\sum_{x=x_1+1}^{x_2-1} \sum_{y=y_1+1}^{y_2-1} G_{i,j}(x,y) \Big/ \left((x_2-2).(y_2-2)\right) \leq T_5 \qquad (3.7)$$

holds, then, check the following conditions,

$$\overline{X}_{i,j} \leq (2/3)\cdot \overline{X}_{i,j+1}, \qquad \overline{X}_{i,j} \leq (2/3)\cdot \overline{X}_{i,j-1} \qquad (3.8)$$

$$\overline{X}_{i,j} \leq (2/3)\cdot \overline{X}_{i+1,j}, \qquad \overline{X}_{i,j} \leq (2/3)\cdot \overline{X}_{i-1,j} \qquad (3.9)$$

and the square is marked as black if either of the conditions given by eqs. (3.8-3.9) is satisfied.

As before eq. (3.7) is intended to control the computational time and $T_5 = 120$, allows to consider the scenario with relatively less *dot loss effects* as well. Furthermore, this reduces the task of the filters to be discussed in the following sections. It is to be noticed again that eqs. (3.8-3.9) are independent of T_1. Although, the operations of eqs. (3.8-3.9) can be integrated; however, it would increase the computational time.

3.7 Post Data Processing Filters

The adaptive binarization technique given in previous section is *not targeted* to handle all possible scenarios (types of the patterns) resulting from the RLS dot gain effects as well as those patterns suffering from very minor dot effects. For this purpose post data processing filters are given, which characterize almost all types of patterns encountered in PS process for the application scenario under consideration. Broadly speaking, in characterization process post data processing filters take into account the behavior of binary pixels within the square $B_{i,j}$ under consideration as well as the behavior (correlation) with the neighboring region (given by $B_{i\pm1,j\pm1}$, $i \neq j$). Furthermore, priorities are assigned to different types of post data processing filters in order to minimize the impact of wrongly recognized neighborhood and for this purpose squares (patterns) suffering from *less* dot gain effects are assigned higher priorities. It is noteworthy that it is mentioned in [Wan99] that post data processing of the scanned grayscale image should be considered; however, it is not considered in existing work and rather than this original digital data is recovered by blindly sampling the binarized image. Due to the application of adaptive binarization as well as post data processing filters, the sampling process used in the novel data-reading technique is referred as active sampling in contrast to the passive sampling used in existing work. Each of the post data processing filters is discussed in the following sections.

Filter-1: This filter deals with the characterization of patterns in which the printed dots corresponding to the submatrices under consideration suffer least from dot gain effects during printing process. Such printed dots are least victim of dot gain effects mainly due to the nature of the pattern formed by the dot under consideration and its immediate neighborhood. This means that the dot under consideration and its neighboring dots are of same type: either all black or all white and this scenario consequently results in minimum dot gain effects. The constraint on the neighborhood is usually satisfied but it is not strictly required to be fulfilled and any dot with or without minimum dot gain effects is supposed to be characterized by this filter. This filter can be described formally as follows.

The statistic denoted as, X , related to the submatrix being characterized is computed as follows:

$$X = \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i,j}(x, y) \qquad (3.10)$$

and the submatrix under consideration is marked as:

$$submatrix = \begin{Bmatrix} white & if\ X = \omega \\ black & X = 0 \end{Bmatrix},$$

where $\omega = no.\ \ of\ \ elements\ in\ the\ submatrix$.

Those squares, which are marked by this way, are assigned the second highest priority after adaptive binarization due to the fact that the squares belonging to this category have the lowest probability of error. It is observed that the large number of squares (binary patterns) belong to this category and are least victims of dot gain effects.

Filter-2: Unlike Filter-1 that considers the squares with minor dot gain effects, Filter-2 deals with those squares, which strongly (with respect to RLS dot gain effects) suffer from strong dot gain effects. Furthermore, Filter-2 complements the function of the filters given for adaptive binarization process (ABP) and consequently considers same type of patterns (i.e. white square surrounded by black ones and vice versa) as in ABP. However, in the present scenario slightly less severe dot gain effects are encountered and this is indicated by the presence of *just few white pixels* or vice versa in the targeted square. The reason to handle such square patterns separately arises from the fact that although the binarization process indicates the existence of a white pattern or vice-versa; however, due to the slight error in the sampling points, usually such pixels are not found at the sampling point and this fact causes error in the sampled value. While characterizing such squares the behavior of neighboring squares is also taken into account. This filter can be described formally as follows.

The statistics denoted as X_1, X_2, about the submatrix $B_{i,j}$ being characterized and its desired neighborhood, respectively, are computed as follows:

$$X_1 = \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i,j}(x,y) \tag{3.11}$$

$$X_2 = \left[\sum_{x=x_1}^{x_2} \sum_{y=y_2-\alpha}^{y_2} B_{i-1,j}(x,y) + \sum_{x=x_2-\alpha}^{x_2} \sum_{y=y_1}^{y_2} B_{i,j-1}(x,y) + \sum_{x=x_1}^{x_1+\alpha} \sum_{y=y_1}^{y_2} B_{i,j+1}(x,y) + \right.$$
$$\left. \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_1+\alpha} B_{i+1,j}(x,y) \right] \tag{3.12}$$

It is to be pointed out that although right side of eq. (3.10) and (3.11) are similar, in fact they apply to different patterns of binarized area, e.g. minor and strong dot gain effects. Finally, the sub-matrix is marked as white if

$X_1 \geq \omega_1$ and $X_2 \leq \omega_2$,

where $\omega_1 = no.\ of\ desired\ elements\ in\ the\ submatrix,$

$\omega_2 = no.\ of\ noisy\ pixels,\ allowed\ in\ the\ neighbourhood,$

and α controls the size of the neighborhood area to be taken into account. The values of the parameters of this filter are given in appendix-C

The constraint on the neighborhood region is given by eq. (3.12). The binary patterns characterized by eqs. (3.11-3.12), arise from the dot gain effects and global threshold level employed in the initial binarization process. Some of the patterns belonging to this category are shown in Figure 3.7.

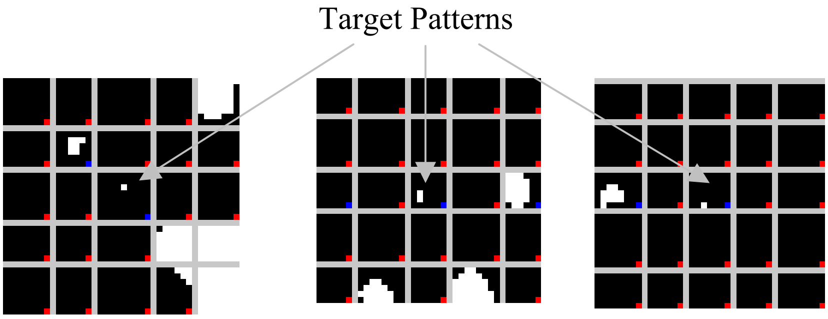


Figure 3.7: Some typical patterns belonging to Filter-2.

By looking at Figure 3.7 it seems to be that by moving the threshold level in binarization process such effects can be decreased; however, this is not the case and when the global threshold level is slightly increased or decreased, the error moves in the opposite direction, this means that the scenario (black dots surrounded by all white ones or the scenario to be discussed in Filter-6) might be detected erroneously.

Filter-3: This filter deals with the square patterns similar to those considered by Filter-1; however, the square patterns considered in present scenario encounter more dot gain effects than before due the existence of the dots (squares) of opposite category in the neighborhood. There is no restriction imposed on the neighborhood region and it is assumed that any square (except those considered in Filter-2) suffering from minor to medium dot gain effects can be handled by this filter. It comes to mind that the operation of Filter-1 can be integrated in Filter-3; however, this is not possible due to the fact that this would erroneously detect the square patterns to be characterized by Filter-5 (to be discussed afterwards). Furthermore, due to the dependence of the characterization process of the following filters on the neighborhood, it is *desirable to correctly mark* (detect) as many squares as possible in advance in order to minimize the errors caused by the neighboring area in the detection process. This is another reason to avoid integration in order to eliminate error contribution by this filter. This filter can be formally described as follows.

The only statistic that needs to be computed in order to characterize the behavior of the filter is denoted as X , is computed as follows:

$$X = \sum_{x=x_1+\alpha}^{x_2-\alpha} \sum_{y=y_1+\alpha}^{y_2-\alpha} B_{i,j}((x,y)|(x \neq y)) \tag{3.13}$$

where $(x_1 < \alpha < x_2)\ and\ (y_1 < \alpha < y_2)$

and the submatrix is marked as,

$$submatrix = \begin{Bmatrix} white & if\ \ X = \omega \\ black & X = 0 \end{Bmatrix},$$

where $\omega = (x_2 - x_1 - \alpha) \cdot (y_2 - y_1 - \alpha) - 4$

It is noteworthy that in characterization of those submatrices (squares), which contain both type of pixels, are not considered due to the more complex nature of the binary pattern and such patterns are treated separately in the following filters. Some patterns (squares) belonging to the Filter-3 are shown in Figure 3.8. As it can be seen from the Figure 3.8 that such patterns do suffer from dot gain effects and need to be handled very carefully, as global thresholding technique and single point sampling cannot promise the correct recovery of such patterns.

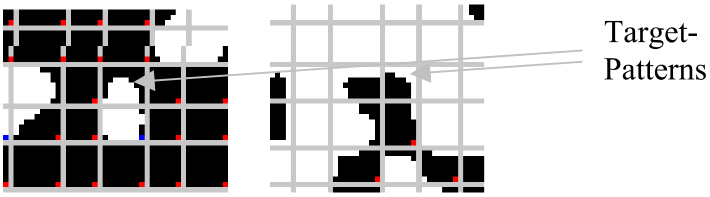


Figure 3.8: Some typical patterns belonging to the Filter-3.

Filter-4: The unpredictable nature of the dot gain effects makes it difficult to state precisely the pattern of the square $B_{i,j}$ under consideration and the immediate neighborhood square patterns that are characterized by this filter. However, usually the square patterns characterized by this filter are of same type as considered in Filter-3; except that here squares suffer more from dot gain effects than before. The mixed (black as well as white) nature of the pixels in central area of the squares under consideration restricts the application of Filter-3 in this scenario. Once again single pixel-based statistics cannot guarantee reliable data recovery due to the more dot gain effects. Furthermore, the patterns characterized by this filter might be of the type used in the following filter-5 as well, when there are small-to-medium dot gain effects.

To characterize those squares in which the histogram computed at the central area is found partially black and white such squares are further classified into different categories and one of the new types of squares can be characterized as follows: The histogram is computed by considering: 1) specific central area and 2) all pixels within the square. Next, the square under consideration is marked as white if the number of black pixels in the whole square is more than the number of white pixels, but *the number of black pixels* in the central area is *less* than the number of white pixels. Similarly, the square is marked as black, if the number of white pixels in the whole square is more than the number of black pixels, but the number of white pixels in the central area is less than the number of black pixels. The above behavior can be described formally as follows.

The two statistics denoted as X_1, X_2, related to the submatrix being characterized are given by the following relations:

$$X_1 = \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i,j}(x,y) \tag{3.14}$$

$$X_2 = \sum_{x=x_1+\alpha}^{x_2-\alpha} \sum_{y=y_1+\alpha}^{y_2-\alpha} B_{i,j}(x,y) \tag{3.15}$$

Where the *value of* α is greater than *that used in eq.* (3.13).

Finally, the submatrix is marked using the following criteria,

$$submatrix = \begin{cases} white & if\ X_1 < \lfloor (0.5)\cdot\omega_1 \rfloor\ and\ X_2 > \lfloor (0.5)\cdot\omega_2 \rfloor \\ black & X_1 > \lfloor (0.5)\cdot\omega_1 \rfloor\ and\ X_2 < \lfloor (0.5)\cdot\omega_2 \rfloor \end{cases} \tag{3.16.1}$$

And if none of the conditions given in eq. (3.16.1) is satisfied, then the following criterion is applied.

$$submatrix = \begin{cases} white & if\ X_1 > \lfloor (0.5)\cdot\omega_1 \rfloor\ and\ X_2 > \lfloor (0.5)\cdot\omega_2 \rfloor \\ black & X_1 < \lfloor (0.5)\cdot\omega_1 \rfloor\ and\ X_2 < \lfloor (0.5)\cdot\omega_2 \rfloor \end{cases} \tag{3.16.2}$$

Where $\omega_1 = x_2 \cdot y_2$,

$$\omega_2 = (x_2 - 2\cdot\alpha)\cdot(y_2 - 2\cdot\alpha).$$

The square is marked as white if number of white pixels is more than the black pixels in both histograms. Similarly, if the number of white pixels is less than the black pixels in both histograms, then the square is marked as black, as in eq. (3.16.2). It is to be noted that lower priority is assigned to the scenario described by (3.16.2) as compared with the other scenario (3.16.1). Some of the patterns belonging to this category are shown in Figure 3.9. The impact of dot gain effects on the patterns can be observed from the figure.

While developing the above criteria of characterization, it is assumed that if the overall number of pixels of type-A is more than half whereas at the central area the number of type-A pixels is less than half, then it is logical to mark such square as of Type-B, as the priority must be given to central area statistics. Experimental results show that filter described by eqs. (3.14-3.16) can successfully characterize such patterns and this consequently validates the assumptions made in this section.

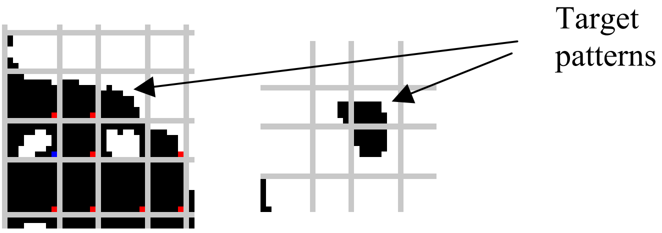


Figure 3.9: Some typical patterns belonging to Filter-4.

In the following two very important filters are proposed to characterize two different types of squares in which the statistics computed at the specific central area do not provide any meaningful information due to the higher dot gain effects. Furthermore, the correlation (dependence) of such squares with the neighboring squares is much higher and more sensitive, making it difficult to characterize such squares. Due to the nature of their correlation such squares are processed at the end, which means that they are assigned the lowest priority among all the filters proposed. It is noteworthy that such squares are not only more difficult to characterize but also affect the performance of the data-reading technique greatly.

Filter-5: This filter deals with one specific type of square patterns defined as targeted white square surrounded by black squares from three sides and vice versa. The nature of such patterns usually results in strong dot gain effects and restricts the application of any other filter considered so far. In the present scenario binary pixel pattern at the central area alone does not provide any meaningful information; however, the behavior of immediate neighborhood region is very helpful and plays crucial role in characterization process. As mentioned earlier while discussing Filter-3 that the targeted patterns can also be characterized by Filter-3 when there are less severe dot gain effects than the present scenario. This filter is characterized by defining a certain binary pattern within the square under consideration and in its neighborhood region as well and is formally described in the following.

It starts by computing the statistic, X_1

$$X_1 = \sum_{x=\sigma_1} \sum_{y=y_1+\sigma_2}^{y_2-\sigma_2} B_{i,j}(x,y) \tag{3.17}$$

σ_1, σ_2 are integer constants. The values of all the parameters of filter are given in appendix-C. Now, if $1 \le X_1 < T_0$ and $T_1 = 0$, here T_0 and T_1 are given by

$$T_0 = \sum_{x=\sigma_1+1} \sum_{y=y_1+\sigma_2}^{y_2-\sigma_2} B_{i,j}(x,y), \qquad T_1 = \sum_{x=\sigma_1+4} \sum_{y=y_1+\sigma_2}^{y_2-\sigma_2} B_{i,j}(x,y)$$

Furthermore,

$$\sum_{x=x_1+3}^{x_2-2} \sum_{y=y_1+2}^{y_2-3} B_{i-1,j}(x,y) + \sum_{x=x_1+3}^{x_2-2} \sum_{y=y_1+3}^{y_2-2} B_{i+1,j}(x,y) + \sum_{x=x_1+2}^{x_2-2} \sum_{y=y_1+2}^{y_2-2} B_{i,j+1}(x,y) = 0\,. \tag{3.18}$$

It is to be noted that in eq. (3.18) dot gain/loss effects has to be taken into account. When all the above conditions are satisfied, only then the submatrix can be considered *as possible candidate* and characterization process proceeds as follows:

$$X_2 = \sum_{x=\sigma_1}^{\alpha} \sum_{y=\sigma_1}^{y_2-\sigma_1} B_{i,j}(x,y) \tag{3.19}$$

where value of α is computed from the following relation,

$$\arg\max_{\alpha \in X} \left\{ \sum_{X} \sum_{y=\sigma_1}^{y_2-\sigma_1} B_{i,j}(x,y) = 0, \quad X \in [\sigma_1, ..., \sigma_1 + 4] \right\}, \tag{3.20}$$

In eq. (3.20) maximum argument of X satisfying the condition given by summation is assigned to α.

Now, if $X_2 \ge T_2$ (T_2 is an integer constant) then compute X_3, X_4, X_5 as follows

$$X_3 = \sum_{x=\alpha} \sum_{y=y_1}^{y_2} B_{i,j}(x,y) + \sum_{x=\alpha} \sum_{y=y_m}^{y_2} B_{i-1,j}(x,y) + \sum_{x=\alpha} \sum_{y=y_1}^{y_m} B_{i+1,j}(x,y), \tag{3.21}$$

$$X_4 = \sum_{x=\alpha-1} \sum_{y=y_1}^{y_2} B_{i,j}(x,y) + \sum_{x=\alpha-1} \sum_{y=y_m}^{y_2} B_{i-1,j}(x,y) + \sum_{x=\alpha-1} \sum_{y=y_1}^{y_m} B_{i+1,j}(x,y) \tag{3.22}$$

Similarly, X_5 can be obtained from (3.21) or (3.22) by substituting $x = \alpha - 2$, and it is given by

$$X_5 = \sum_{x=\alpha-2} \sum_{y=y1}^{y_2} B_{i,j}(x,y) + \sum_{x=\alpha-2} \sum_{y=y_m}^{y_2} B_{i-1,j}(x,y) + \sum_{x=\alpha-2} \sum_{y=y_1}^{y_m} B_{i+1,j}(x,y) \qquad (3.23)$$

where $x_m = \left\lfloor \dfrac{x_1 + x_2}{2} \right\rfloor, \qquad y_m = \left\lfloor \dfrac{y_1 + y_2}{2} \right\rfloor$

Using eqs. (3.21-3.23) another statistic X_6 is computed as

$$X_6 = \begin{Bmatrix} (X_3 + X_4) & X_3 \geq T_3 \\ (X_4 + X_5) & X_3 < T_3 \end{Bmatrix} \quad ; \; T_3 \text{ is a known integer constant.}$$

Finally, X_7 is computed as

$$X_7 = \sum_{x=\alpha-1}^{\alpha} \sum_{y=y_m}^{y_2} B_{i-1,j}(x,y) + \sum_{x=\alpha-1}^{\alpha} \sum_{y=y_1}^{y_m} B_{i+1,j}(x,y) \qquad (3.24)$$

Now if the following conditions are satisfied

$X_6 \leq T_4$, and $X_7 \leq T_5$, where T_4, T_5 are known constants given in appendix-C.

Then the submatrix under consideration is marked as white. While characterizing the binary pattern using eqs. (3.17-3.24), it is to be noticed that the submatrix under consideration is characterized by taking into account the behavior of the neighboring squares as well. And the constraint imposed on the neighborhood is given by eq. (3.18). Furthermore, eqs. (3.19-3.24) are also dependent on the neighboring submatrices unlike eq. (3.17) and most of the filters described earlier. This interdependence imposes the additional constraints on the characterization process, especially for the submatrix under consideration. Some typical patterns from the class of patterns under consideration are shown in Figure 3.10.

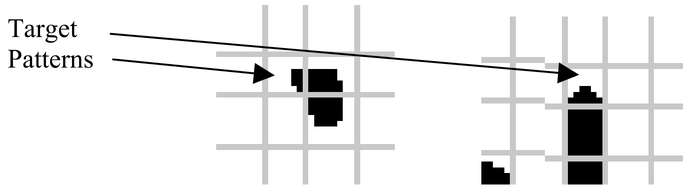


Figure 3.10: Some typical patterns belonging to the Filter-5.

It is also mentionable that binary pattern characterized by eqs. (3.17-3.24) is one particular case, corresponding to the scenario in which white dot having top, bottom and right neighboring dots as black ones and the left neighbor as the white one. There is no constraint on the top-left, top-right, bottom-left and bottom-right immediate neighbors. There are three more cases for the white dot (white dot surrounded by the three neighboring black dots) suffering from similar dot gain effects. The equations for these scenarios can be written similarly as eq. (3.17-3.24) and the parameters remain same. Also there are four cases corresponding to reverse scenario (black dot is surrounded by three white dots and one black one), which is the result of dot loss effects. *Almost same* procedure is to be followed as described by (3.17-3.24) and one such scenario is considered in Appendix-A eqs. (A1-A8).

Filter-6: The patterns characterized by this filter suffer strongly from the dot gain effects and this is attributed to the nature of the pattern formed by the targeted and immediate neighboring squares. A typical pattern belonging to this category usually consists of a black target square and at least three white squares including one at the corner *and vice versa*. Due to the strong nature of the correlation between the target and neighborhood squares as well as strong dot gain effects such patterns are treated at the end (i.e. assigned the lowest priority). This very important filter characterizes a square by computing two statistics as well as taking into account the behavior of the neighboring squares and can be described formally as fellows.

Two statistics denoted as X_1, X_2, related to the submatrix being characterized and X_3, related to its required neighborhood, are computed as follows:

$$X_1 = \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i,j}(x,y) \tag{3.25}$$

$$X_2 = \sum_{x=x_1+\alpha}^{x_2-\alpha} \sum_{y=y_1+\alpha}^{y_2-\alpha} B_{i,j}(x,y) \tag{3.26}$$

Where α *value is same as in eq.* (3.15),

$$X_{31} = \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i-1,j}(x,y) + \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i-1,j+1}(x,y) + \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i,j+1}(x,y) \tag{3.27.1}$$

$$X_{32} = \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i-1,j}(x,y) + \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i-1,j-1}(x,y) + \sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i,j-1}(x,y) \tag{3.27.2}$$

$$X_{33} = \sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} B_{i,j-1}(x,y) + \sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} B_{i+1,j}(x,y) + \sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} B_{i+1,j-1}(x,y) \tag{3.27.3}$$

$$X_{34} = \sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} B_{i+1,j}(x,y) + \sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} B_{i+1,j+1}(x,y) + \sum_{x=x_1}^{x_2}\sum_{y=y_1}^{y_2} B_{i,j+1}(x,y) \tag{3.27.4}$$

The submatrix is marked as white if

$X_1 \geq \varepsilon_1$, $X_2 \geq \varepsilon_2$, and at least one of the statistics computed from eqs. (3.27.1-3.27.4) is zero.

$\varepsilon_1 = no.\ \ of\ \ desired\ elements\ in\ the\ submatrix$
$\varepsilon_2 = no.\ \ of\ \ desired\ elements\ in\ region\ defined\ by\ eq.(3.26).$

Some of the squares belonging to Filter-6 are shown in Figure 3.11.

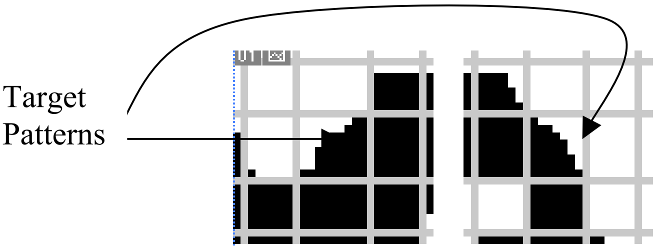


Figure 3.11 Some typical patterns belonging to the Filter-6.

Finally, the constraint on the neighborhood region given by eq. 3.27 is relaxed and the square is marked as follows:

$$submatrix = \begin{Bmatrix} white & if\ X_2 > 0.5 \cdot \varepsilon_3 \\ black & X_2 < 0.5 \cdot \varepsilon_3 \end{Bmatrix} \tag{3.28}$$

Where ε_3, is total number of elements in X_2. It is to be mentioned that eq. (3.28) handles those square which are not handled by using eqs. (3.25-3.27).

Filter-7: Exception Pattern Handling

Finally, an interesting, but important filter is described which checks each of the squares (submatrix) *recognized already* using any of the filters described earlier against the exceptional behavior. In other words, the exceptional handling filter checks the pattern being characterized by taking into account its behavior with the neighborhood pattern as well whether such pattern can occur (means that does this pattern follow any logic). This filter can be described formally as follows.

It computes the statistic denoted by X_1 as,

$$X_1 = \sum_{x=x_1+\alpha}^{x_2-\alpha} \sum_{y=y_1+\alpha}^{y_2-\alpha} B_{i,j}(x,y) \tag{3.29}$$

Where α *value is same as in eq.*(3.15).

Now, if

$$X_1 \geq \varepsilon_1, \tag{3.30.1}$$

$$\sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_2} B_{i-1,j}(x,y) = \omega_1, \tag{3.30.2}$$

and

$$\sum_{x=x_1}^{x_2} \sum_{y=y_1}^{y_1+\beta} B_{i,j}(x,y) = 0 \tag{3.30.3}$$

Where $\varepsilon_1 =$ *no. of desired elements in region defined by eq.*(3.29),

$\omega_1 =$ *no. of desired elements in the corresponding submatrix*.

Now, eqs. (3.30.1-3.30.3) constitute a contradictory set of equations as practically it cannot happen and if such behavior is encountered then it must be due to the noise and countermeasures can be taken to overcome this noise. None of the desired patterns shown in Figure 3.12 can be a white dot due to the fact that in the immediate neighborhood there is another white dot and two connecting white dots cannot be separated by such a small distance (as shown in the Figure 3.12). For instance in the left most pattern desired pattern separates two white dots and the target pattern cannot be white one due to the fact that 3 connected white dots are strong enough to resist the dot gain effects. So by using such measures the patterns can be characterized correctly. However, this scenario is not implemented in the data-reading technique due to the fact that it requires more sophisticated pattern processing operations, which is expected to be computationally more expensive than the ones discussed before. Also the number of patterns belonging to this category is not found too many and so is ignored. It is also mentionable that the general behavior of the exception-handling filter is not described by eqs. (3.29-3.30), it is only a special case. General behavior is not considered due to reasons mentioned above. Some patterns belonging to this category are shown in Figure 3.12.

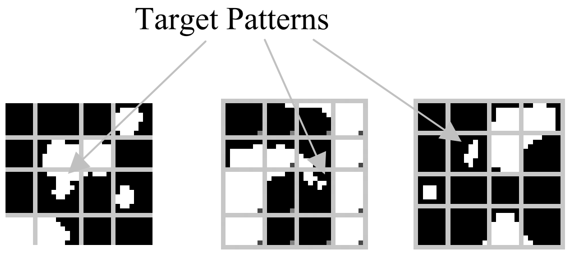


Figure 3.12: Some patterns belonging to the exception handling characterization process.

3.8 Experimental Results

For experimental purpose test images (HD-DataStripe) measuring 104 by 804 pixels with 80 K bits user payload, consisting of randomly generated binary data, are printed at 300 dpi using HP4600 printer. The images are selected by keeping an application in view in which HD-DataStripe is used. The size of the HD-DataStripe is in the Pakistan national ID card. The printed HD-DataStripe is scanned at 8 times more the printing resolution using HP5550c scanner. Each experiment is repeated 3 times for 7 different test images, where test 1-6 and test 7 correspond to simulated and real-data, respectively and the number of errors detected in recovered data are given in Figure 3.13, where the detailed results are given in Table-B1 (appendix-B).

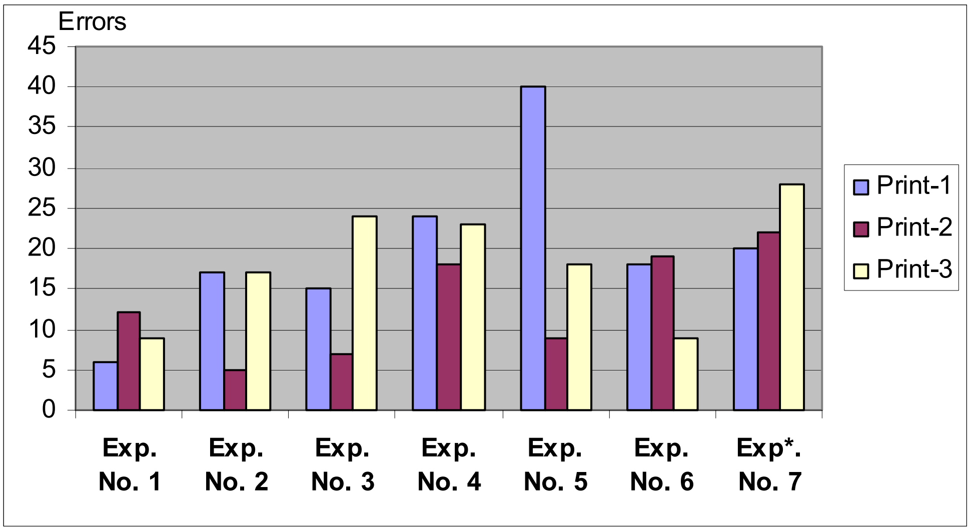


Figure 3.13: Errors encountered in recovered data for HD-DataStripe using novel data-reading technique (* HD-DataStripe with real-data).

It can be seen from the results that all the times data is recovered very accurately. The small number of errors (5-40) is caused by the unavoidable stains on the paper and scanner surface and severe dot gain effects. However, such errors can be compensated easily using error correction coding (ECC) with very small overhead.

In order to see the effects of real-data on the recovered data, HD-DataStripe with user payload consisting of real-data (facial image, digitized signatures, biographical data, and a portion of the digitized fingerprint) is considered. Each of these data types is compressed using the appropriate data compression technique, and the resulting payload is encoded using ECC technique with the aim to see the impact of all the operations encountered in the practical scenario on the HD-DataStripe. Detailed discussion on real-data and the operations performed on it, is postpone till chapter 4 where application of HD-DataStripe in smart ID documents is considered. The resulting HD-DataStripe is again printed 3 times and no performance difference is observed as it can be seen from Figure3.13 (experiment no. 7). It is mentionable that the same set of test images (1-7) is also used in the following experiments.

3.8.1 Impact of Printing Devices on Recovered Data

Now the performance of the data-reading technique is evaluated by considering more printing and scanning devices and for this purpose 7 printers and 2 scanners are investigated. The selection of these devices is governed by the available printing and scanning facilities at the institute as well as the constraints imposed by the data-reading technique, which requires at least 2 times more printing resolution than the data is intended to be encoded (i.e. HP-DataStripe is printed) and 8 times more scanning resolution. These constraints consequently demand for 600 dpi and 2400 ppi printing and scanning devices respectively. Next, 7 test images (HD-DataStripes) used in the previous experiments are printed on each of the printers using the default settings and scanned using HP8250 scanner with same settings (given in appendix-C) as the one used before. The results are shown in Figure 3.14 as average number of errors detected in the recovered data for different printing devices. Same parameters set is used for data-reading technique for all the devices.

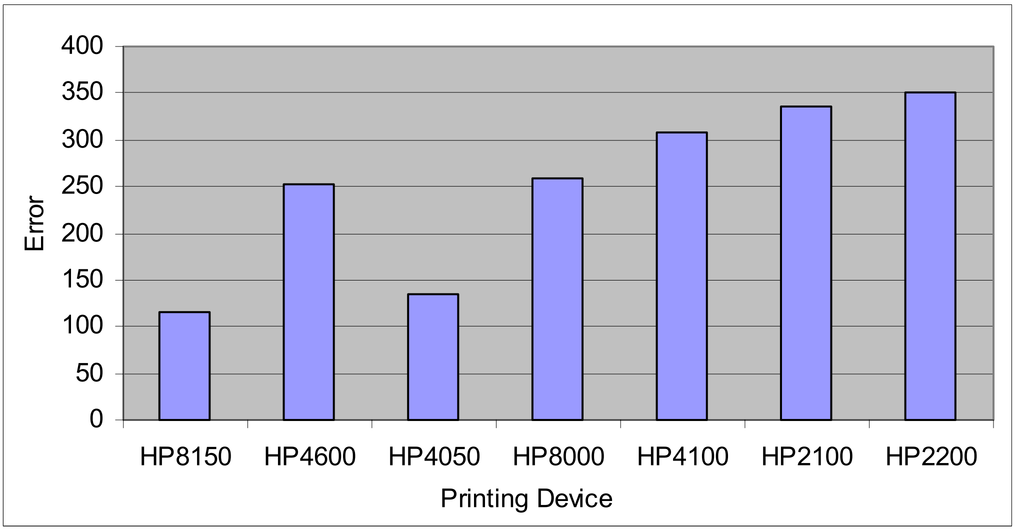


Figure 3.14: Mean number of errors encountered in recovered data for various printing devices.

By looking at the results it can be seen that average number of errors is now higher as compared with the results shown in Figure 3.13, which is due to the following reasons: 1) aging effects, and 2) data-reading technique parameters. Experiments for the results shown in Figure 3.13 were conducted about two years ago and at that time the device was almost new, offering very less dot gain effects. Whereas, in recent experiments it is observed that now this device (HP4600) offers much higher *severe* dot gain effects than before, which is an indication of the aging effects and these effects contribute significantly to the number of errors encountered in recovered data. Second factor contributing to the error is the set of parameters that were used earlier and it is found that some of the parameters (to be discussed shortly) need to be adjusted according to the scenario under consideration. In other words parameters used when a device suffers from minor dot gain effects needs to be modified when the same device suffers from aging effects and these aging effects can be seen by the mean luminance value which decreases with an increase in dot gain effects. Similarly, some parameters might need adjustment for different printers. It is to be mentioned that usually new devices do not require the parameters to be changed.

With the objective to find any further gain in performance, next optimized performance of each of the 7 printing devices mentioned above is investigated. This includes some parameters modification for the adaptive binarization filter, 2nd order polynomial fitting to draw horizontal template lines and scanner effects. The results for optimized performance are shown in Figure 3.15 from which it can be seen that in four cases there has been improvement. For comparison purpose unoptimized performance is shown as well. It is to be mentioned that the improvement is less evident due to the average value and this can be seen that from the detailed results given in the Table-B3 (appendix-B).

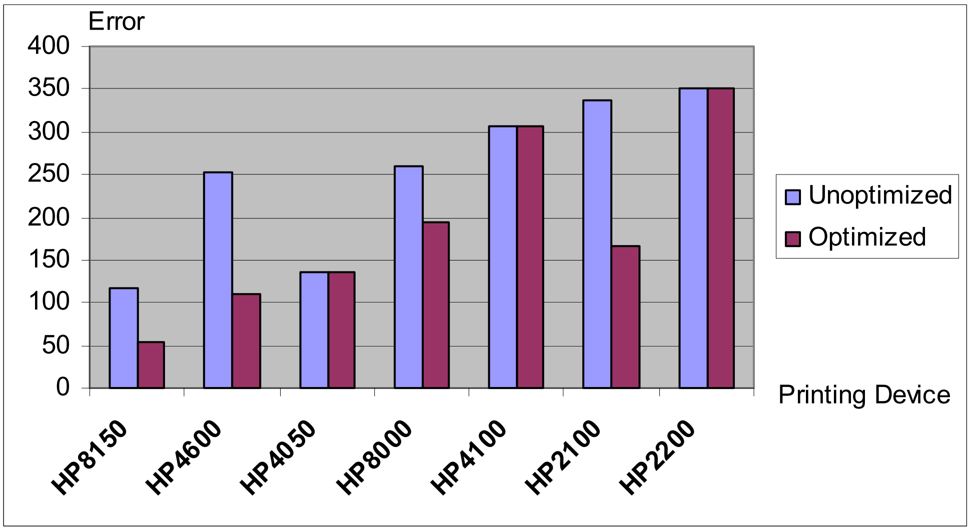


Figure 3.15: Mean number of errors encountered in recovered data for various printing devices using: 1) optimized set of parameters, 2) unoptimized set of parameters.

For HP8150 printer it is found that using a second order polynomial, results in some improvement. It is mentionable that this printer is the newest (but still more than one year old) among all the devices considered in this research. To approximate 2nd order polynomial, which requires three different points to infer its parameters, two at the corners and one at the center, are used. Furthermore, each of these points is taken as the average value of 10 identified neighboring registration marks. To eliminate the error contribution from slight inaccuracy in the identified marks to propagate in the following, each time (for each pair of vertical registration marks) polynomial parameters are inferred using the two identified registration marks for which horizontal template line is to be drawn. As RM-pattern is added only around the image, this pose challenge to approximate 2nd order polynomial, as the center point is not available. For the present scenario, difference between the first and the second point, is always added to first point to get location of middle point. A more sophisticated approach to find the middle point for polynomial approximation is discussed in appendix-C (p. 162). In polynomial approximation, intention is to have accuracy 0.000833-0.000417 of an inch at middle region. This means that any given registration mark at center would be surrounded by the template having only 1-2 pixels (at 2400 ppi) error.

For HP4600 printer 1st order polynomial (i.e. linear approximation) is found sufficient and the value of parameters T_1, T_3, T_4 (given in appendix-C) for adaptive binarization needs to be modified. In this case T_1 (mean luminance value increased by fixed constant 10 discussed in appendix-C) results in improved performance. Above criteria works for the previous experimental results as well. The mean luminance value is calculated from the image consisting of random data, while considering only its information carrying region. The optimized performance is obtained with HP5550c scanner. It is also required to modify the parameters T_3, T_4 in adaptive binarization filter for two different scanners. All these parameters are given in appendix-C.

HP2100 and HP8000 both suffer from *dot loss effects*, a scenario in which impact of light regions extends to neighboring dark regions unlike dot gain effects. In this case to find further gain in performance, value of T_1 in adaptive binarization filter as well as 2nd order polynomial approximation for horizontal template, need to be modified. It is observed that optimized performance is obtained by using T_1 given by the mean luminance value plus a constant value 20-30, which is *2-3 times higher* as compared with dot gain scenario. An objective measure to differentiate between dot loss/gain scenario could not be developed, however, it is mentionable that mean and standard deviation statistics do not provide sufficient information in this context. The middle point for 2nd order polynomial approximation, while considering HP2100, is achieved by subtracting a fixed value two from average of first and third points. Whereas for HP8000 2nd order polynomial approximation is found more challenging as the techniques used for HP2100 and HP8150 to find the middle point *sometimes do not result* in optimized performance. The optimized performance is obtained by subjectively evaluating the accuracy of horizontal template drawn by the 2nd order polynomial, while slightly varying (0, ±1) the value of the middle point (average value of first and third points). A potential objective technique (not yet implemented) for choosing the middle point for 2nd order polynomial considering general scenario is discussed in appendix-C. In case of HP8000 printer it is observed that its performance remains same or slightly improves when toner level approaches towards end. This can be seen from the results given in Table-B9 for an experiment conducted when empty toner message is generated from this device.

For other printing devices HP2200, HP4050 and HP4100 no further improvement is obtained by using any of the measures discussed above. The parameters of the data-reading technique for all the cases discussed so far are given in the appendix-C.

To see the performance of the existing binarization techniques [Wan01, Fu02, Wu01] in present scenario, data recovery is investigated using the RM-pattern given in this work for the existing binarization techniques. The results are given in Table-B10 (appendix-B), which show that the existing binarization techniques cannot be applied in the present scenario. It is to be mentioned that results given in Table-B10 do not present the complete picture of the behavior of existing techniques in present scenario due to the fact that one of the important factors in the performance of the data-reading techniques is RM-pattern and these results are obtained using new RM-pattern rather than using the RM-patterns given in the existing work, which would further degrade the performance. This is evident from the underlying design and processing mechanism of the existing RM-patterns.

3.8.2 Impact of Underlying Contents on Recovered Data

The detailed results given in Table-B3 (appendix-B) show that the error for real-data (Test 7) in contrast to the simulated data is slightly higher and this behavior might raise questions about the strength of simulated data. However, this is not the case and it is noticed that slightly higher error is attributed to the priority assigned to the filters. By changing the priority of Filter-6, such behavior is eliminated and it can be seen from the results given in Table-B8 (appendix-B). Previously, Filter-5 and Filter-6 have been assigned the higher priority over Filter-4. This means that at first stage patterns belong to Filter-5 and Filter-6 are *marked as the candidate patterns* prior to applying Filter-4 and once patterns belonging to Filter-4 have been marked then the other two filters are applied. In other words candidate patterns are ignored by Filter-4. The reason for some of the patterns to be ignored is the fact that Filter-5 and Filter-6 depend more strongly on neighboring behavior and to minimize the error contribution from wrongly marked neighborhood patterns such patterns are first loosely marked. Once the Filter-4 has been applied then candidate patterns are marked permanently. Now, it can be seen from the results given Table-B8 (appendix-B) that with the modified priority, according to which Filter-6 is not applied repeatedly, results in similar behavior for the real and simulated data and slightly improves the average performance as well. It is mentionable that due to the time constraint only Table-B3 is updated and the other results to be given in the following sections are not updated.

Using another approach the small performance difference between real and simulated data is overcome by changing the properties of the real-data before printing. This can be accomplished by: 1) scrambling operation (discussed in chapter-6), and 2) adding pseudorandom noise. In latter scenario considered in this research, pseudorandom noise having similar properties, as that of the simulated data, is added to the real-data by applying the binary exclusive-or operation and the resulting signal is used as (HD-DataStripe). To get the real-data back, the pseudorandom noise is generated with the same key that is used before and the pseudorandom noise is subtracted from the data recovered from HD-DataStripe after PS process by applying binary exclusive-or operation again. By this way performance of real and simulated data are found similar and it is verified experimentally. An HD-DataStripe with real-data, modified as discussed above, when printed using HP 2100 and HP 2200 printers results in 118 and 283 errors, respectively, as compared to 274 and 510 (Table B-3) errors encountered before. This error decreases to 117 and *241* as compared with 118 and 410 (Table-B8) errors, respectively, by avoiding the repeated application of Filter-6 discussed before.

3.8.3 Impact of Scanning Devices on Recovered Data

To see the impact of scanning device two different scanners HP5550c and HP8200 are considered. HP8250 is more sophisticated and offers higher resolution. Furthermore, this device has higher dynamic range for the sensors and this is observed from the fact that it detects stronger distortions caused by dot gain effects better than the HP5550c. For the performance comparison same test images considered above printed using HP8150, HP4600, HP8000 and HP4100 are considered. For data recovery process parameters for data-reading technique used in optimized scenario are used and performance (average number of errors) is shown in Figure 3.16. The detailed results are given in Table-B4 (appendix-B).

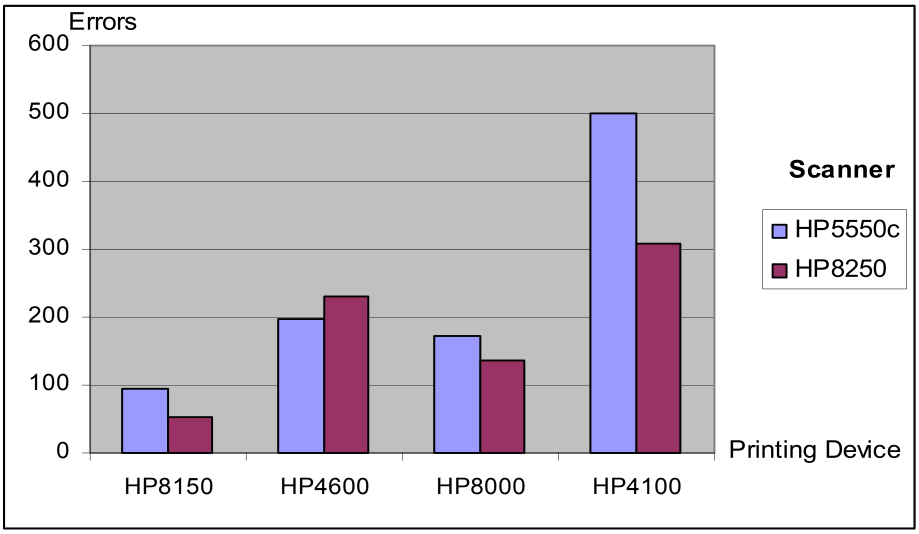


Figure 3.16: Performance (mean error) comparison of two scanners HP5550c and HP8250 for four printing devices.

From the results it can be seen that HP8250 scanner performs better due to its ability to scan small details more precisely as compared with the other one. This fact is more evident while considering other printing devices suffering more from dot gain effects. In contrast to general behavior in case of HP4600 it is found slightly opposite, which is due to the fact that here adoptive binarization filters, in effort to detect patterns suffering from more dot gain effects, result in false positive errors.

To find an optimal over sampling factor, due to the time constraint, only initial study is conducted yet and this is due to the fact that data-reading technique requires lot of careful modifications that could not be accomplished due to the time constraint. To avoid the modifications in data-reading technique for the time being an image initially scanned at lower resolution is over sampled afterwards using image processing techniques, to have same over sampling factor that has been used before. This technique obviously has the drawback that in over sampling process noise is also amplified, which degrades the performance. The results for some experiments are given in Table 3.1.

Table 3.1: Impact of the over sampling factor on recovered data. (Scanner HP8250)

	Test	Test 6	Test 7	Test 7*
Over Sampling Factor	8	54	93	118
	7	111	155	229
	6	62	205	186
	5	105	402	275
	4	151	699	718
	Printer	**HP8150**	**HP8150**	**HP2100**

From the results it can be seen that HP8150 printer with simulated data can be used immediately at 4 times higher over sampling factor (1200 dpi) without any modifications in data-reading technique. Whereas the existing over sampling factor (8) can be decreased by 2 without siginificant performance degradation. The real-data (without adding noise discussed above) results in more errors for 4-5 times over sampling factor and this is mainly due to the over sampling noise. However, it is observed that at 1200 dpi there is sufficient information that can be utilized by the data-reading technique (after necessary modifications) to recover the data with some degradation in performance. Same remarks hold for the results shown for HP2100 printer. It is to be mentioned that Test 7* used for HP2100 printer is obtained by adding noise to the real-data (Test7) as discussed before. The slight unusual behavior encountered at 2100 dpi is also attributed to the over sampling noise and can be elimnated. Finally, based on the initial study it is safe to claim that after necessary modifiacations 4-5 times over sampling would be sufficient for the data-reading techique without significant performance degradation.

3.8.4 Impact of RM-Pattern on Recovered Data

The RM-pattern is investigated with the objective to find any further performance gain and to combat the errors caused by RM-pattern due to unprinted or partially printed marks. This scenario might be encountered while considering relatively old printing devices in which some of the marks might not be printed at all or printed only partially (a more likely scenario) and this would consequently accumulate errors in the identified RM-pattern, resulting in degraded performance. Inspired by the above objectives RM-pattern discussed earlier is modified slightly to increase its robustness against the unprinted or partially printed marks. The modified RM-pattern (MRM-pattern) is similar to the one used before except that now its period is increased from two to three and one single period consists of two consecutive black dots followed by a white one (e.g. 001001001). To see the effects of modified RM-pattern same test images considered are printed with both types of RM-patterns using all the printing devices and the results are shown in Figure 3.17.

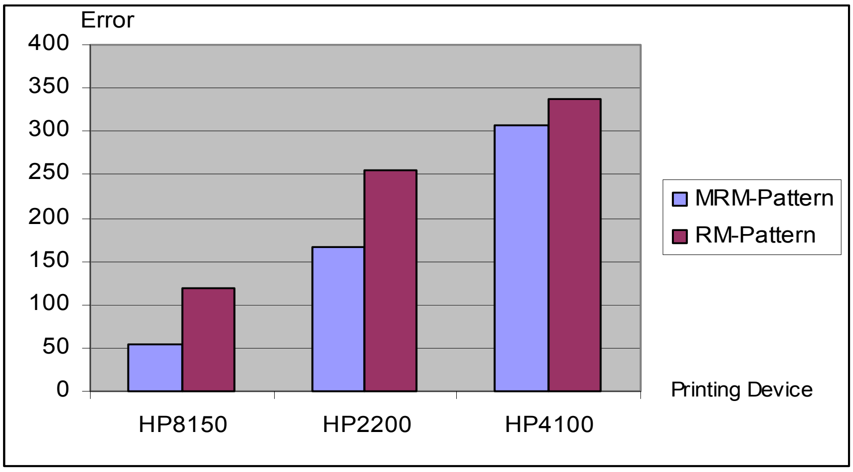


Figure 3.17: Performance (mean no. of errors) comparison for two different RM-patterns using three different printing devices.

From the Figure 3.17 it can be seen that on average MRM-pattern performs better than RM-pattern. This difference in performance does not provide complete picture of the scenario due to the average value shown in the figure. The detailed results given in Table-B5 (appendix-B) show that there is more than 100% performance difference encountered in at least two out of seven tests. It is also observed that linear approximation rather than 2nd order polynomial performs better for the RM-pattern, so the results shown in Figure 3.17 for RM-pattern are obtained using linear approximation. It is to be mentioned that except experiments (Figure 3.13), in the remaining experiments MRM-pattern has been used.

3.8.5 Skewing Distortion

In this work it is observed that regardless the fact how carefully the document being scanned is put on the scanner bed the skewing distortion varying between 0.1-0.3 degrees in clockwise direction is unavoidable in the scanned image. Consequently, the data-reading technique must be robust against this distortion. The novel data-reading technique can successfully count for unintentional skewing distortions and this can be verified from all the results discussed so far. In order to see the robustness of the data-reading technique against the intentional skewing effects, the images are skewed manually during the scanning process and then de-skewed afterwards by utilizing the RM-pattern. A typical skewed image is shown in Figure 3.18. The amount of skewing effects encountered by an image can be calculated by the following relation:

$$\theta = \tan^{-1}(y/x) \tag{3.31}$$

where x and y are the base and perpendicular of the right angle triangle (shown in Figure 3.18), obtained by drawing the projection of rotated HD-DataStripe to the X-axis. Then image can be deskewed by the angle, θ, using MATLAB imrotate routine.

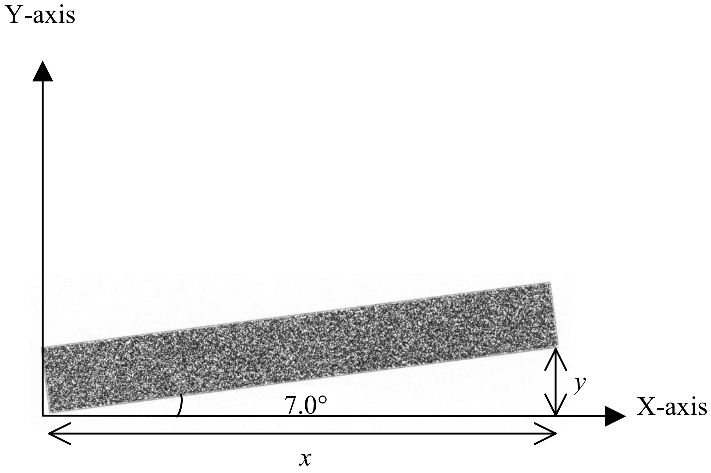


Figure 3.18: An illustration of highly skewed HD-DataStripe.

To evaluate the performance the data-reading technique, the images printed using three different printing devices are considered. Each of the images to be scanned is skewed manually by a random amount either in clockwise (-) or counter-clockwise (+) direction. Then the data-reading technique is applied as before and the number of errors encountered in recovered data are given in Table 3.2. By looking at the results it can be seen that the data is recovered successfully up to ±9°. It is to be mentioned that in some experiments error was increased; however, using 2nd order polynomial approximation resulted in same performance as in case of unintentional skewing effects. Beyond 9° it is found that error increases very rapidly. However, this scenario can be tackled by using the embedded RM-technique in which registration marks are also added at random positions within the information carrying region of HD-DataStripe especially at central region to compensate for nonlinear de-skewing effects encountered at higher rotations. Furthermore, these marks can be used for multiple purposes, that is to infer the parameters of the second order polynomial (discussed in appendix-C) in addition to its application to compensate for higher skewing distortions. In this research skewing distortion beyond 9° is not addressed due to the fact in real-life applications this much rotation is not likely to occur.

Table 3.2: Robustness of data-reading technique against the intentional skewing distortion.

Printer	HP8150		HP4050		HP4600	
	θ (deg)	Errors	θ (deg)	Errors	θ (deg)	Errors
Test1	-3.43	57	+4.89	112	+1.05	94
Test2	+4.10	50	+9.52	130	+5.78	150
Test3	-8.10	36	-7.99	159	-6.04	128
Test4	-4.81	44	+9.16	189	-6.16	130
Test5	-4.47	54	+3.21	129	-4.99	136
Test6	+3.20	50	-3.32	82	+5.04	95
Test7	+3.20	79	-5.61	195	+5.37	234
Mean		53		142		138

- Sign means clockwise rotation
+ Sign means counter clockwise rotation

3.8.6 Robustness of Data-Reading Technique Against Noise

With the objective to see the robustness of data-reading technique against the aging effects, impact of certain types of noise such as contrast reduction, luminance reduction, dust-and-scratches, additive uniform noise and additive Gaussian noise, is investigated.

Contrast and Luminance Reduction Noise: The contrast and luminance reduction noise is inspired by the assumption that with the passage of time document would result in decreased contrast and luminance values due to the accumulation of dust layer on the surface. With this objective 10% contrast and 10% luminance is decreased in the scanned image and then the data-reading technique is applied. The results after 10% contrast and 10% luminance reduction are shown in Figure 3.19 along with the performance without any noise for comparison. The detailed results are given in Table B6 (appendix-B). It can be seen from the results that there is no significant change in performance by either of the two distortions. Additional errors encountered in the recovered data are mainly due to the RLS dot gain effects, which get stronger with additional noise. It is also observed that the errors caused by the contrast reduction can be overcome by changing the value of T_1, filter-1 and this is possible up to 50% contrast reduction; however, it is difficult to predict any advantage of this fact in real-life scenario. The error obtained with 50% contrast reduction by modifying T_1 is 246.

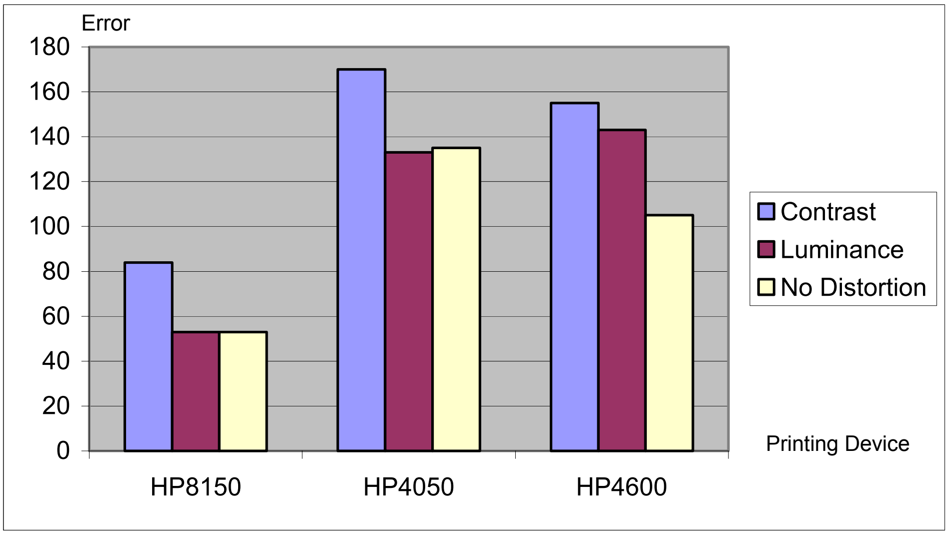


Figure 3.19: Mean number of errors encountered in the recovered data:🟦 10% contrast reduction,🟥 10% luminance reduction, 🟨 without any distortion, considering three different printing devices.

Dust-and-Scratches Noise: As another noise the dust-and-scratches effects are investigated by simulating this behavior using the Adobe Photoshop software. There are two parameters: radius and threshold level that are to be specified. The radius defines the average size of the dust or scratching dot to be added and in this research radius of 8 pixels is considered as one noisy dot. Since one dot printed at 300 dpi is over sampled 8 times, consequently, radius of 8 pixels is assumed to simulate dust-and-scratch effects of one dot. Similarly, to see the effects of dust-and-scratches dots measuring 2, 3, and so on, would require radius of 16 and 24 pixels, respectively. The other parameter is threshold level, varying between (0-255), specifies the region to be considered to add dust-and-scratches noise and it is chosen as 128. The choice is governed by the fact that lower values add too much noise in contrast to higher values that do oppositely. In this research, dust-and-scratches behavior for 2, 3, 4, 5 and 10 dots is simulated for the optimized scenario (Figure 3.15). It is to be mentioned that only two test images, which have been resulting in more errors, are considered due to the time constraint. Furthermore, noise is added selectively, which means that it affects only the information carrying region of the scanned grayscale image. When the entire scanned image is considered, then noise is also added to the RM-pattern and requires additional effort to estimate the RM-pattern from the noisy environment. The distorted marks can be estimated from the locations of the neighboring marks (not necessarily the immediate neighbor); however, this issue is not addressed yet. So to see the initial behaviour noise is added selectively and the results are given in Table 3.3.

Table 3.3(a): Number of errors encountered in recovered data caused by the dust-and-scratches noise for *HP4600* printing device.

	2 dots noise	3 dots noise	4 dots noise	5 dots noise	10 dots noise
Test6	88	379	476	204	616
Test7	186	462	578	295	754

Table 3.3(b): Number of errors encountered in recovered data caused by the dust-and-scratches noise for *HP4050* printing device.

	2 dots noise	3 dots noise	4 dots noise	5 dots noise	10 dots noise
Test6	117	181	221	257	916
Test7	155	396	635	732	1138

Table 3.3(c): Number of errors encountered in recovered data caused by the dust-and-scratches noise for *HP2100* printing device.

	2 dots noise	3 dots noise	4 dots noise	5 dots noise	10 dots noise
Test6	377	736	833	896	2477
Test7	421	951	1232	1263	1240

Table 3.3(d): Number of errors encountered in recovered data caused by the dust-and-scratches noise for *HP4100* printing device.

	2 dots noise	3 dots noise	4 dots noise	5 dots noise	10 dots noise
Test6	329	363	372	375	920
Test7	309	756	1196	1427	1745

From the above results it seems that the Test 7 has almost two times more number of errors, however, this is not always the case as it can be seen from Table 3.3c for 10 dots noise, and this fact leads to the contents independent behavior of dust-and-sractes noise. To have more clear picture of dust-and-scratches noise behavior, it would be necessary to conduct large number of experiments and then take the mean value.

Uniform and Gaussian Noise: In this scenario 5% and 10% uniform and gaussian noise is added selectively on the scanned image to see its impact on the recovered data. As the dust is expected to be uniformly distributed with very small size particles, so it can be assumed that its behaviour is simulated by the gaussian or uniform noise. Similarly, noise encountered from scanner sensors can be assumed to have such behavior. These two noises might also be assumed the noise from the printing process and in this case noisy dots might result from poor quality printing device, which would result in partially printed dots. It is to be mentioned that the gaussian noise is more stronger than the uniform noise and degrades the performance more than the other one. It is also observed that the 5% noise does not affect the RM-pattern and data can be recovered quite successfully. The results for the uniform and gaussian noise are given in Table 3.4.

Table 3.4(a): Robustness of the data-reading technique against uniform and gaussian noise for *HP8150* printer.

	0%	5% UN	10% UN	5% GN	10% GN
Test1	25	94	223	197	1480
Test2	42	77	207	152	1258
Test3	83	57	156	133	1212
Test4	29	65	193	133	1204
Test5	48	75	194	153	1329
Test6	50	57	131	103	1079
Test7	93	114	229	313	2556

Table 3.4(b): Robustness of the data-reading technique against uniform and gaussian noise for *HP4600* printer.

	0%	5% UN	10% UN	5% GN
Test6	83	111	210	198
Test7	184	232	452	389

Table 3.4(c): Robustness of the data-reading technique against uniform and Gaussian noise for *HP2100* printer

	0%	5% UN	10% UN	5% GN
Test6	184	225	415	336
Test7	285	362	804	689

Table 3.4(d): Robustness of the data-reading technique against uniform and Gaussian noise for *HP4100* printer

	0%	5% UN	10% UN	5% GN	10% GN
Test6	326	388	787	683	3226
Test7	278	343	598	512	2972

Table 3.4(e): Robustness of the data-reading technique against uniform and gaussian noise for *HP4050* printer. * Performance after applying blurring operation and (138-4) shows number of errors with 4 times blurring operation.

	0%	5% UN	10% UN	5% GN	10% GN
Test6	83	99	195	191	1370
Test7	139	214	568	458	2955
Test7*	138-4	143-2	207-2	239-2	343-4

The results show that up to 10% uniform noise and 5% gaussian noise do not degrade the performance very much. Similar to the dust-and-scratch noise, Test7 results in almost two times more errors than Test6, however, as before it is observed Table (3.3c and 3.4d) that this is not always the case, and this leads to assume that the behavior is random and to draw solid conclusion more experiments are needed. Furthermore, it is found that uniform and gaussian noise can be compensated by applying the blurring operation. As it can be seen from Table 3.4(e) where number of errors decrease from 2955 to 343 by the application of blurring operation four times consecutively on the image with 10% gaussian noise. This means that scanned image goes through the five operations (1. 10% GN, 2. Blurring, … 5. Blurring) consecutively before applying the data-reading technique. When the blurring operation is applied 4 times to the image without noise, no change in performance is observed. Similar, behavior is observed for uniform noise as well. This fact leads to expect that application of blurring operation before applying data-reading technique would improve the performance against small noise arising from dust, scanner sensor, or printing process.

3.8.6 Computational Time

The computational time for the computer with 2.0 GHz processor and 512 MB RAM for the novel data-reading varies 3-4 minutes, which is quite high for the targeted applications. The higher computational-time is mainly because the data-reading code is written in MATLAB, which is considered less efficient as compared with other the programming languages e.g., C, C++. Initial study shows high potential for computational gain by writing the code in C language. Another factor contributing to the higher computational time is the fact that code remains to be optimized. To give an overview of the time taken by various operations (functions) during data-recovery process, time profile of the most time consuming routines is given in Figure 3.20.

By looking at time profile it can be seen that the computationally most expensive parts are: adaptive binarization, Filter3-5 and Filter5-6. Whereas RM-pattern identification,

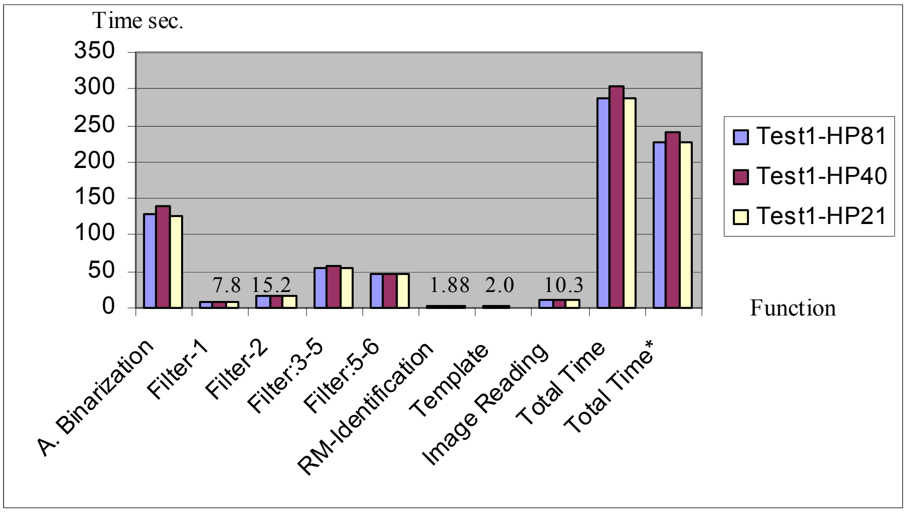


Figure 3.20: Time-profile comparison of different operations for the novel data-reading technique. Total time* is the time taken when profile generation option is de-activated.

Template (partition of scanned image into squares or submatrices), and Filter1-2 have negligible computational time. In adaptive-binarization process time is mainly consumed by the scenario described by eqs. (3.2-3.6). Other computationally expensive part is Filter-5, which appears twice in the time-profile diagram due to the reason that in Filter3-5 this filter marks the patterns only as the candidates patterns belonging to this Filter before applying Fiter3-4. In other words these patterns are not considered by Filters3-4. Once patterns belonging Filters 3-4 have been marked then Filter-5 is applied to recover the information (patterns) characterized by Filter-5. This repeated application of Filter-5 results in higher computational time. In first case, Filter-5 is not used to recover data due to the possible dot gain/loss effects on the immediate neighborhood and it is decided to let the neighbors be characterized first. The potential impact of this repeated application when it is avoided, is not investigated yet and it is left till code optimization. Although in this research primary focus has been to minimize error in recovered data; however, some effort is made in this direction by reducing the computational time for the RM-pattern identification (discussed before).

In the above discussion PS process noise arising from dot gain effects is focused upon. However, in other scenarios when image is printed at lower resolution but it is not scanned at sufficient high over sampling rate this would still result in noisy PS process. Similarly, when the image printed at lower resolution is scanned at sufficient high scanning resolution, but using a scanner with relatively poor quality sensors array this would again result in noisy PS process. Although these scenarios are not considered in this research, however, data-reading technique modified according these scenarios would perform equally-well, which means that it would allow maximum channel utilization (that results in RLS dot gain effects).

Chapter 4
Applications of Novel Data-Reading Technique

4.1 Introduction

The fact that the novel data-reading technique given for *HD-DataStripe* in Chapter 3 offers higher data encoding rate as compared with the existing techniques [FuA02, ST, Wan01, WuL04] has potential usage in many existing applications. The HD-DataStripe can make improvement in large number of applications such as smart identity cards, driving licenses, travelling documents (passport, visa), bank checks by offering more data storage capacity and eliminating the expensive ways of data storage such as IC chips, magnetic stripes etc. Furthermore, while considering HD-DataStripe as a counterfeit-resistant technology, it can be used for product labelling with brand protection capability. The key ideas can be extended to applications using UV, IR and magnetic inks as well. The investigation of possible areas of improvement in existing applications is the objective of this and the proceeding chapters. In this chapter three applications are selected to demonstrate the potential gain that can be achieved by using the HD-DataStripe as a storage media.

The first application considered is in the area of *Brand Protection*, where existing technologies for brand protection such as holograms, KINEGRAMS® etc. are either too expensive or restricted in usage. Recently, a non-expensive anti-counterfeiting product labeling technique is given [Pic04], which uses specially designed copy detection patterns. In this research following the similar way an improved technique is given.

The second application is selected from *Smart Identity Verification* documents, which is a very hot area of research nowadays. One of the key objectives in the context of Smart Identity Documents is to find new efficient data storage techniques that enable to store all the biometrics data rather than biometrics templates of a person in a Smart ID. The existing technologies for Smart ID documents are either less reliable due to small data storage capacity or too expensive due to higher data-storage and data-reading costs and demand for further research to overcome these limitations.

As a third application, *Authenticity Verification of Hardcopy Documents* such as official letters, contracts etc., is considered. This application is selected due to the fact that the conventional ways of hardcopy documents authentication are time-consuming and prone to error due to the human interaction involvement. The application of existing digital signature technique [Zha04] to the present scenario, requires exact contents recovery from the scanned hardcopy document using OCR; however, the existing OCR technology can offer up to 99 % accuracy and this limitation results in other drawbacks.

The novel technique for authenticity verification of hardcopy documents given in this work offers advantages over the digital signatures-based authenticity verification.

4.2 Copy Detection Techniques

Brand protection is a study of developing same technique as HD-DataStripe etc., but opposite application that is targeted to uniquely identify products and is required to be robust against attacks such as photocopying, recreation. Nowadays, it is a very hot area of research due to the easy-access to the high quality digitizing and printing technologies. There are many different technologies [Ren98, Ren05, Phil00, Phil02, Phil04] (e.g. KINEGRAMS®, holograms, security printing, lithography printing etc.), which are being used to protect a document against photocopying attacks. All of the above techniques; however, have the limitation that they are expensive [MAC+04]. Keeping this fact in mind, recently adopting a different approach, a new brand protection technology is developed [Pic04].

According to the new approach a pseudorandom binary pattern of size *x* by *y* pixels is generated with known key and used for the brand protection. This pattern is formally referred as copy detection pattern (CDP) in [Pic04]. The existing copy detection technique [Pic04] is based on the principle that each time the information (CDP with maximum entropy) passes through the channel (printing and scanning process) at *high data encoding rate*, there does occur an information loss. Furthermore, it is claimed that this information loss is unavoidable even with best quality existing printing and scanning technologies and it is assumed that this scenario will continue to exist in future as well. Consequently, the following factors: 1) maximum entropy, 2) higher message size, and 3) information loss through the channel, make the CDP highly resistant against the counterfeiting efforts and encourage its usage as a brand protection label, which can be detected if copied. Two such patterns: a) consisting of pseudorandom binary noise generated with the known key, and b) noise-like pattern combined with a meaningful pattern (a logo), are shown in Figure 4.1.

(a) (b)

Figure 4.1: Two Copy Detection Patterns given in [Pic04], a) pseudorandom binary noise, b) noise-like pattern combined with a meaningful pattern (a logo).

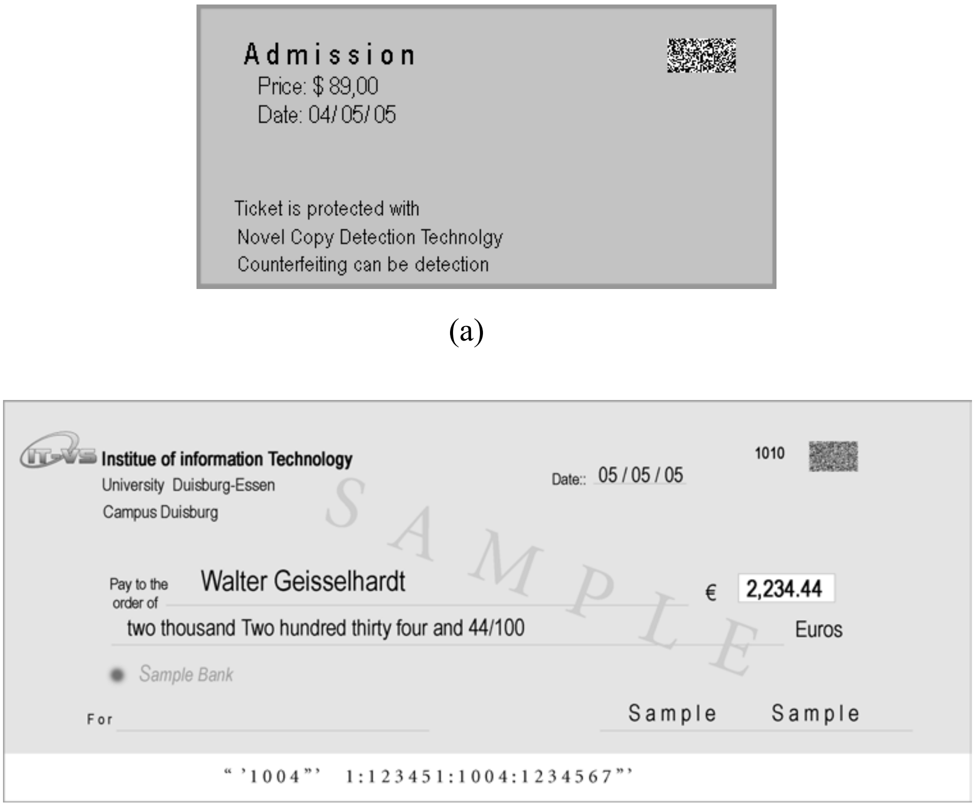
To recover a CDP after print-and-scan process and ultimately to detect copying attack, a data-reading technique is developed, which reads CDP pixels and then correlates both the recovered and the original CDPs, where the original CDP is generated using the known key. A threshold level, which is the percentage of correctly recovered CDP pixels, is established and used to check whether the CDP has gone through the copying attack. While developing threshold levels to distinguish between the original and copied CDPs, images with the known characteristics are used. It is observed in [Pic04] that in each of the following scenarios: 1) re-creation attack when a pseudorandom binary pattern with different key but same statistical characteristics as the original CDP is used as CDP and 2) scanning/photocopying attack where the originally printed CDP is either photocopied or scanned and then reprinted. In either case, the percentage of correctly recovered CDP pixels is found much lower than the threshold level established for the non-copy scenario. It is to be pointed out that in the existing CDP technique CDP is printed at 300 dpi. Furthermore, using existing data-reading technique a threshold level about 50-60 is established for the CDP, which has not gone through a copying attack and it is mentioned that ideally the threshold value must be 100 (i.e. perfect similarity between the correlated patterns). This means that only about half of the CDP pixels needs to be recovered correctly to characterize a scanned CDP as the original, indicating an highly information loss scenario.

In [LoN05] it is suggested to use chipless ID technology in which embedded passive RF tagnets are incorporated during paper making process for assigning a unique machine-readable code (like barcodes) in hardcopy documents. This chipless ID technology offers 100 bits to uniquely identify a document and is resistant against the reproduction of the document. The applications of chipless ID technology are mentioned for postal services, entertainment tickets and hardcopy recording of electronic voting.

Cryptoglyph^{TM} [Cryp] from AlpVision is another anti-counterfeiting technology, being widely-used for brand protection, secure paper etc. A Cryptoglyph^{TM} mark is an invisible pattern of randomly spread tiny printed dots (like CDP *except* invisibility) that are used to encode some useful information (e.g. product identification code, crucial information in a bank check or any other valuable document etc.). The technology does not rely on special security devices/materials and uses conventional printing (inkjet, laser printers) and scanning (scanners, digital cameras, mobile phone cameras) devices. The distinguishing features of this technology are: invisibility, counterfeiting resistance, low cost, and contents security. The security strength of the technology is attributed to the invisibility of cryptogyph with naked eyes, encryption of the encoded data, redundant data and cryptoglyph detection/decoding software. It is also mentionable that to author's knowledge no scientific information has been published until now and this fact consequently restricts to make any solid remarks about the technology. However, based on the findings of this research on PS-process, an assessment about the strength of the technology as an anti-counterfeiting technology will be made in the following sections.

4.2.1 Novel Brand Protection Technology

In this research to develop brand protection technology, HD-DataStripe having same size as the one used in [Pic04] is used as a CDP. The underlying principle is same as in [Pic04] that the information loss during print-and-scan process is exploited to characterize copying attack. The novel technology; however, is much more robust against the copying attacks and offers additional benefits as well. The strength of the novel technique is attributed to the more sophisticated data-reading technique given in chapter 3. The new technology establishes a threshold level corresponding to the original CDP *above 99%* while deciding whether a given CDP has gone through copying attack. This fact demands from the attacker to recover *almost every CDP pixel correctly* to launch a successful copying attack against CDP, in contrast to the rival technology in which about (50-60)% pixels are to be generated correctly. Unlike the existing CDP technology, the novel technology does not require the original message or key in order to recover the CDP information. Furthermore, it allows encoding a message within the CDP. This fact extends its potential usage to other applications such as multi-purpose HD-DataStripe, one-to-one contents verification, digital postal stamps etc. In Figure 4.2 two potential applications of HD-DataStripe as a copy detection technology are shown.



Admission
Price: $ 89,00
Date: 04/ 05/ 05

Ticket is protected with
Novel Copy Detection Technolgy
Counterfeiting can be detection

(a)

Institue of information Technology
University Duisburg-Essen
Campus Duisburg

Date:: 05 / 05 / 05

1010

SAMPLE

Pay to the order of Walter Geisselhardt

€ 2,234.44

two thousand Two hundred thirty four and 44/100 Euros

Sample Bank

For

Sample Sample

“ ’1004”’ 1:123451:1004:1234567”’

(b)

Figure 4.2: Two applications: a) an entertainment ticket, and b) a bank check, protected using the novel copy detection technique.

While considering digital postal stamps, if in the printed digital stamp some information such as sender/receiver postal address or some other unique feature is encoded after encryption, this would make the copying of digital printed stamps extremely difficult. And *even if one stamp is copied* the other stamps would be equally difficult to copy due to encryption and information loss through the print-and-scan channel.

Unlike the existing technique in which pseudorandom pattern generated using a given key is used, the novel CDP allows encoding the product related information such as company name and/or logo, product name, serial number, manufacturing and expiry date etc. And this would allow more efficient product handling.

As a rival to the chipless ID technology, which cannot offer resistance against forgery attacks for applications (e.g. bank checks, entertainment tickets, educational certificates etc.); the novel technology, using HD-DataStripe as a CDP, is less expensive and robust against forgery as well as counterfeiting attacks.

When comparing the novel technology with cryptoglyph technology, latter one offers very less data encoding capacity. The impact of the capacity on application can be seen (in sec. 4.2.2) in context of bank checks. Invisibility of cryptoglyph mark cannot contribute to enhance counterfeiting resistance, as invisible pattern can be made visible by digitizing the printed mark at sufficiently higher over sampling rate (sec. 3.4). The mark invisibility is obtained by decreasing the ratio of black dots per unit area and size of the isolated printed dots. It is shown in chapter-6 that invisible (isolated printed tiny dots) of size 1/600 of an inch have sufficient signal strength that can be exploited in active counterfeiting attacks. A more detailed discussion along with some potential counterfeiting techniques based on the findings of this research is given in appendix-E on page 179.

Experimental results are not reported for copy detection technique due to the reason that CDP has same characteristics as HD-DataStripe, except smaller size. The information encoding process in the CDP is a straightforward problem and is addressed in the following section.

4.2.2 Security Aspects of Novel Copy Detection Technology

While considering security of copy detection technology, it is application dependent. For instance, in bank check application a suitable-sized CDP would allow to encode biometric template (e.g. bioscrypt or dynamic signatures template) and one-time digital stamp (as for online transactions) data along with all other important information on the check in encrypted form. This would allow tackling repudiation attack, resulting in enhanced application security as compared with rival technologies in which very small data can be encoded in counterfeit detecting pattern (e.g. CDP or Cryptoglyph mark). Given that all the contents in encrypted form along with their digital signatures and public-key (using PKI system from trusted third party) can be encoded in CDP would ensure contents authenticity, integrity and confidentiality as well. It is mentionable that here confidentiality does not seem to pose any threat. For applications such as entertainment ticket any critical data (e.g. performance time, date, place etc.) encoded in the CDP would further decrease the possibility to use any previously used CDP in a new application. In this application one potential threat could be broken counterfeiting detection device from which information (recovered CDP) can be obtained and maliciously used. Such threat is possible against other techniques [Cryp, Pic04] as well and is not addressed in this research. However, solution seems to be in strong verifying devices. In above discussion first application is more secure than the second one and this is due to the underlying characteristics of the application, although the main technique is same for both applications.

4.3 Smart Identity Verification Documents

In this research a document (visa, passport, driver's license or national ID) is considered as a Smart ID document, if it allows to store all the data (including some biometrics characteristics) contained in it in digital format. In general a Smart Identity Verification document has the following characteristics: 1) uses both bearer-related information and some biometrics characteristics for identity verification, 2) is robust against forgery and counterfeiting attacks, 3) permits automatic identity verification and 4) offers on-card data storage capability.

Bearer's information usually includes biographical data (e.g. name, birth date/place, address etc.), portrait, and some biometrics information (signature print, fingerprints etc.). The different security layers (e.g. digital watermarking, microprinting, UV/IR ink printing, holograms, KINEGRAMS® etc.) are currently being used to protect the document against the counterfeiting and data tempering attacks. The identity verification mode determines whether the document holder can be verified automatically using some biometrics characteristics (second-line identity check) in addition to the first-line identity verification mode. On-card data storage capability plays a key role in smart documents and is the main focus of this research. It will be seen shortly *how it affects* the performance of all the characteristics 1-4 of a Smart ID Card. Two main components of any smart identity document are biometrics and on-card storage media. Although biometrics are not the main focus of this research, but due to their key role in smart identity documents, are briefly reviewed in the following with the aim to highlight the various requirements and constraints imposed by good biometrics identity verification systems.

4.3.1 Biometrics Identity Verification Systems

Biometrics is a biological or behavioral characteristic of a human being, which is selected under the constraints that it belongs to everybody, differs sufficiently from person to person, does not change with the time and can be measured quantitatively. The well-known biological biometrics include: fingerprints, iris scans, retina scan, face and hand geometry, whereas the behavioral biometrics include: signature scans and voiceprints. A biometrics identity verification system is a real-time pattern matching system, which measures a biometrics characteristic at identification time and compares it with single similar type of biometrics sample (verification mode) or a number of samples (identification mode), which is/are already stored in the system. A generic biometrics identification system is shown in Figure 4.3.

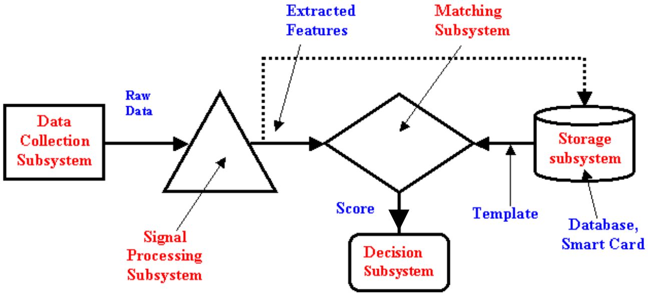


Figure 4.3: A generic biometrics identity verification system.

Data Collection Subsystem (DCS) measures the actual biometrics characteristic using a specially designed device. A key constraint on the DCS is that it should *work actively* to make sure that the person being identified is actually present at that time and an artificial biometrics (e.g. dead fingerprints, already taken static image of an individual, copied signature sample) is not being presented for identification [AnK97].

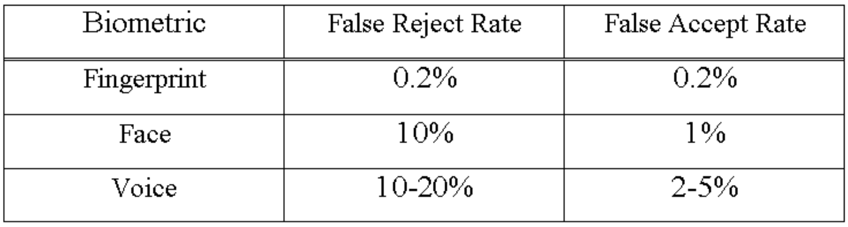
Signal Processing Subsystem (SPS) applies various image processing operations for noise elimination, template extraction, data compression, encryption etc. on the raw biometrics data. It is to be pointed out that *template extraction* is at the heart of the smart identity documents due to the *limited storage capacity available.*

Storage Subsystem (SS) stores the reference biometrics samples and/or templates using different storage media such as database servers, IC chips, optical memory stripes, barcodes, magnetic stripes and *plays a key role* in the performance of any biometrics identity verification system and is the main focus this research.

Matching Subsystem (MS) takes the biometrics characteristics from SPS and SS, compares them using some appropriate pattern recognition technique and passes the matching result, a single value varying between 0-1 to the Decision Subsystem. A match resulting in zero value means that there is no similarity and one indicates that patterns being matched are exactly same. The performance of MS can be *improved* by using *multiple-templates of same biometrics or multiple-biometrics characteristics*.

Decision Subsystem (DS) makes the final decision about the identity verification using confidence intervals, which are based on security risk policy. There are two important parameters False Reject Rate (FRR) and False Accept Rate (FAR) associated with the performance of DS. The confidence interval must be selected in such a way that both FRR, FAR have very small value. It is to be pointed out that FRR, FAR vary from identification to verification mode and also for different biometrics characteristics. The performance of DS can be *improved by integrating more than one biometrics in decision-making process*. The FRR and FAR for some biometrics characteristics when used in verification mode are given in Table 4.1.

Table 4.1: State-of-the-art error rates for fingerprints, face and voice biometrics systems when used in verification mode [JRP04].



Biometric	False Reject Rate	False Accept Rate
Fingerprint	0.2%	0.2%
Face	10%	1%
Voice	10-20%	2-5%

Biometrics identity verification systems can be classified as: 1) Unimodal and 2) Multimodal.

Unimodal Biometrics System utilizes single biometric characteristic for identity verification and this fact could result in the following drawbacks:

1. **Noise in the sensed data:** The sensed data might be noisy, e.g. a fingerprint with scar, voice altered by cold. Noisy data could also be the result of a defective or improperly maintained sensor.
2. **Intra-class variations:** The data acquired during verification might be very different from the one used to generate the template at enrolment time due to the incorrect interaction of the user or modification in sensor characteristics.
3. **Distinctiveness:** Every biometric has an upper bound in terms of its discrimination capability.
4. **Non-universality:** Some users may not possess a particular biometric (e.g. due to the poor quality of the ridges, fingerprint features might not be extracted for certain users).
5. **Spoof attacks:** The possibility of artificial fingerprints, signatures etc. to circumvent the system.

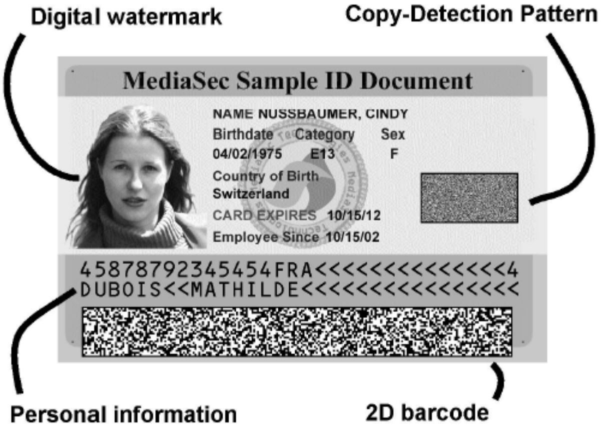
Multimodal Biometrics Systems In the multimodal biometrics systems more than one biometric characteristics are used for identity verification and they can overcome many limitations [AnK97] of the unimodal biometric systems. However, multimodal biometrics systems are more expensive due to:

1. Multiple data acquisition sensors
2. Higher storage capacity
3. Higher computational requirement

From above discussion on biometrics it can be seen and it will be more clearer after discussing some smart identity verification *documents* that one of the key factor influencing the performance of any biometrics-identity verification system is the data storage capacity needed to store the reference biometrics. For example, if sufficient capacity is available multiple-biometrics characteristics or multiple extracted templates can be stored, which would result in an improved performance. In previous biometrics identity verification systems, storage capacity was not an issue due to the fact that all the biometrics data was stored in central database system, which obviously do not suffer from capacity problem. However, central database-oriented identity verification systems pose different problems such as communication link failure, communication cost, database failure threat and the possibility of cyber attacks. Nowadays to overcome these limitations different techniques for on-card data storage are being investigated. In the following section some existing smart identity documents using similar on-card data storage technology as in this research are reviewed. Furthermore, a state-of-the-art brief overview of the capabilities and drawbacks of other technologies being used in Smart cards is provided as well.

4.3.2 Some Existing Smart Identity Verification Documents

Recently J. Picard et al. [PVT04] have proposed a Smart ID Card (known as Fraud-Proof ID card). In this card (shown in Figure 4.4) main focus is to make the document robust against counterfeiting, and data-tempering attacks. For this purpose three different security features are used. To make the document robust against photocopying attack a copying detection technology (discussed in section 4.2) is used. Against the portrait replacement attack a watermark with 16 bytes (biographical data dependent) user-payload is added to the printed image. Finally, an extracted template of bearer's dynamic signatures (116 bytes) rather than fingerprints is used for automatic bearer verification. Bearer's biographical data, dynamic signatures *template* and CDP generation-key are stored in a barcode (PDF417) after encryption. It is pointed out that it would be ideal to store portrait and full dynamic signatures in the barcode, but this demands for higher capacity, which is constrained by the barcode size.



MediaSec Sample ID Document
NAME NUSSBAUMER, CINDY
Birthdate Category Sex
04/02/1975 E13 F
Country of Birth
Switzerland
CARD EXPIRES 10/15/12
Employee Since 10/15/02
45878792345454FRA<<<<<<<<<<<<<<4
DUBOIS<<MATHILDE<<<<<<<<<<<<<<<<

Figure 4.4: A Fraud-Proof ID Card from MediaSec® [PVT04].

Smart ID documents from Canadian Bank Note Company Limited [CBN] use 2-D barcode technology to store biographical data, portrait and an encrypted authentication key. In Smart ID documents from *DATASTRIP* Inc. [DStr], in addition to the biographical data and highly compressed portrait, a fingerprint template to be used for automatic identity verification is stored as well in a 2-D barcode. It is noteworthy that in latter case an increase in capacity is gained by increasing the barcode size rather than higher data-encoding rate. It can be seen that all of the smart identity documents discussed above use only single biometrics characteristic while establishing the true identity of the bearer. Such identity verification systems; however, are not recommended for high security applications due to the fact that each biometrics has certain limitations as mentioned above (Table 4.1) and this fact enforces to consider multimodal biometrics identity verification systems. On the contrary multimodal systems need much higher on-card storage capacity, which is beyond the capability of the existing barcodes and this fact encourages considering other alternatives.

Recently multilevel barcodes are investigated in [DP03, VVK+05] with the aim to further increase the capacity of 2-D barcodes. The key idea behind both techniques is same that multilevel-grayscale symbols are used. In [DP03] a grayscale barcode symbol having size 4 by 4 pixels with 4 graylevels is used to encode 2 bits of information. To avoid intersymbol interference, symbols are separated by one pixel. The barcode is printed at 150 dpi and this results in 625 bytes per square inch data storage capacity. In [VVK+05] using symbol size 2 by 2 pixels and one pixel intersymbol separation, number of graylevels is increased from 4 to 8 and this increases the per symbol information encoding rate from 2 to 3 bits. To further increase the capacity per unit area barcode symbols are printed at 200 dpi and result in 1403 bytes per square inch by taking into account the payload for error correction coding. It is to be pointed out that in [VVK+05] channel coding techniques are used to correctly recover the bar-code symbols. In [DP03] a maximum likelihood detector, which is trained in advance with the symbols to be recognized, is used. Furthermore, in both cases the main emphasis has been on the key idea and strength of the techniques is not reported. Especially, in [VVK+05] it is mentioned that technique is in preliminary stage and might not be evaluated by undertaking independent experiments.

Other storage technologies such as magnetic stripe, IC chip and optical memory are being used as well. The data storage capacity of existing barcodes and magnetic stripe is more or less equal and both technologies have the limitation that data can be copied easily. The highest capacity is offered from optical memory, which uses same principles as the one used in a compact disk (CD) for data storage. An optical data stripe used in *LaserCards*® offers between 1.1-3.0 Mbytes data storage capacity, which is sufficient to store all the important data (including high quality multiple biometrics) contained in the card. However, the cards using optical memory are more expensive as compared with the cards using 2-D barcode technology and this is due to the higher cost of data-readers and optical memory storage media. IC chips are also being used to store data on the card. A comparison of the data holding capacity of the existing storage media [SCO] is given in Table 4.2.

Table 4.2: Data storage capacity comparison (in bytes) of various exiting technologies. (psi means per square inch)

PDF417 (psi)	**Data Strip**	**Magnetic Stripe**	**IC Chip**	**Optical Memory**
212	2.1 K	0.2-0.9 K	1-32 K	1.1-3.0 M

The above discussion can be summarized with the following remarks.

1. The capacity of the existing storage media such as barcodes, magnetic stripes, IC chips is more or less equal and is not sufficient to accommodate high quality biometrics data due to their limited data storage capacity.
2. Extracted biometrics templates are being used for identity verification due to the limited data storage capacity; however, such systems are not recommended for highly sophisticated security applications [AnK97].
3. For highly secure applications it is suggested to use multimodal biometrics systems; but they demand for further increase in data storage capacity.
4. Optical memory offers sufficient capacity, but it is expensive.
5. Finally, it is still highly desirable to increase the capacity of existing storage media at a minimum cost.

4.4 Application of HD-DataStripe Technology to Smart ID Cards

As clear from the above discussion that the lower capacity of the exiting storage media being used in smart cards mainly bounds the performance of biometrics identity verification systems and needs further research. The novel technology for smart ID cards given in this research is developed with this objective (i.e. to increase the capacity of the widely used non-expensive storage media: paper). In this section application of HD-DataStripe technology to the *Smart Identity Cards* is focused upon, in order to demonstrate the potential performance gains of novel storage technology in this scenario. On way to achieve this goal a smart ID card is produced considering real-data as well as simulated data. All the steps encountered in this process are shown in Figure 4.5.

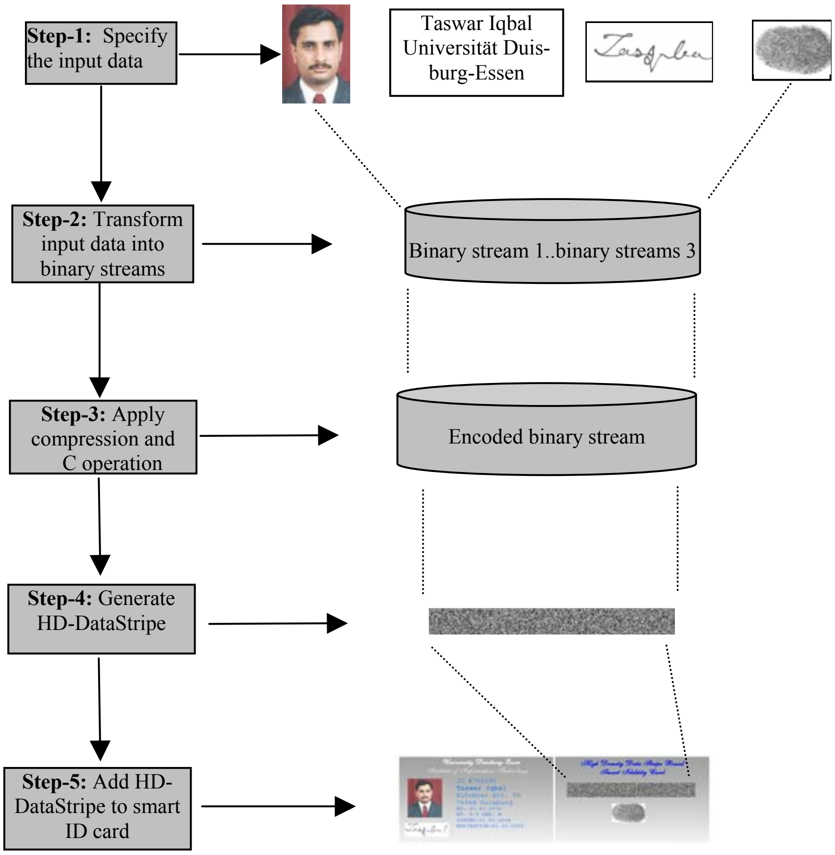

Step-1: Specify the input data
Taswar Iqbal
Universität Duisburg-Essen
Step-2: Transform input data into binary streams
Binary stream 1..binary streams 3
Step-3: Apply compression and C operation
Encoded binary stream
Step-4: Generate HD-DataStripe
Step-5: Add HD-DataStripe to smart ID card

Figure 4.5: Steps followed in this research during Smart ID card production process.

The smart ID-card production process begins with the selection of input data to be stored in HD-DataStripe. The input data consists of all the information that is necessary to establish the true identity of the cardholder, using both first-line and second-line identify verification techniques. However, as in [PVT04] the contents are not secured against the potential threats, targeted to first-line security check. The selection of the key features to be used as input data has fundamental role in the strength of the identity verification system. Some of these features: biographical information and portrait size, along with card layout has been standardized [Asb02]. The most crucial part of the input data feature is choice and quality (i.e. extracted biometrics template or the original biometrics characteristic) of the biometrics characteristics. The fingerprints and signature prints are the oldest, most widely used biometrics, and are currently being used in machine-readable traveling documents in many countries, so these two are focused in this research. After selecting the input data, next these features are converted into binary streams and each binary data stream is compressed using appropriate data compression technique. The compressed binary streams are concatenated and the resulting binary stream is encoded using error correction coding (ECC). Finally, the encoded binary stream is transformed into the HD-DataStripe bitmap image, which is added at the appropriate region in the smart ID-card.

While considering biometrics quality, it is highly desirable [JBP99, JRP04, PVT04] to use complete biometric data files instead of the extracted templates and it is especially required for the fingerprint data, which is most widely used and highly reliable way to identify a person. The digitizing process of the fingerprint image at FBI quality requires image digitization at 500 dpi as a grayscale (8 bits per sample) and this results in 2 M bits file size. Applying the lossy fingerprint data compression standard from FBI, which gives the compression ratio of 18:1, reduces the final size of fingerprint data to ~13.75 KB. This size is far away from the capacity offered by the most of the existing storage technologies (Table 4.2). The raw-data file size for the digitized *dynamic signatures* is 5 KB [PVT04]. It is to be mentioned that in this research static signature prints (sec. 4.4.4), which are less memory demanding than the dynamic signatures, are considered; however, the smart ID-card to be discussed shortly can accommodate both fingerprints as well as dynamic signature prints. As the multimodal biometrics systems can overcome many limitations of unimodal systems, in Table 4.3 template sizes of different biometrics are given with the objective to see the possibility of implementing a multimodal biometrics system.

Table 4.3: Biometric template size comparison (in bytes).

	Fingerprints	Hand Geometry	Iris	Face	Retina	Signatures	Voice
Smallest	256	10	256	84	96	500	1,500
Largest	2,000	20	512	2,500	96	1000	3,000

As the novel data-reading technique can reliably recover the data encoded at 300 dpi (chapter 3), this means that an HD-DataStripe measuring 0.75” by 3” (size of data stripe used in the *existing smart ID-card* from *DATASTRIP* Inc.) would offer 202.5 Kbits of data storage capacity. The novel HD-DataStripe offers 12 times higher capacity than the data stripe used in *DATASTRIP* Inc. cards, and this capacity is sufficient to store all of the data files after compression. Unlike existing storage media where in best scenario highly compressed face image and fingerprints *data template* are stored due the limited data storage capacity. Furthermore, it can be seen from Table 4.3 that an HD-DataStripe can easily accommodate all high quality biometrics templates, resulting in a *multimodal biometrics verification system*. The HD-DataStripe capacity increases up to 400 Kbits when an HD-DataStripe measuring 1.38” by 3.15” (a size used in the *LaserCards*®) is used. In Figure 4.6 a typical smart identity card is shown. In this card, HD-DataStripe measuring 0.75 by 3 inch offers sufficient capacity to store all the information shown in card in compressed form.

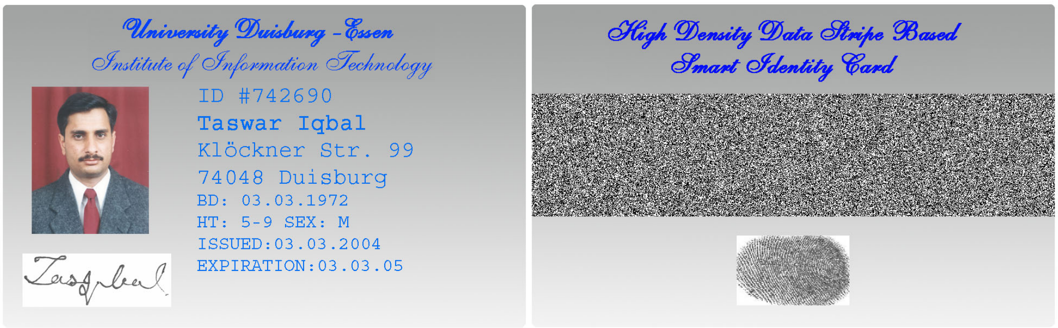


Figure 4.6: Smart ID Card with sufficient capacity to store all information contained in the card in compressed form.

Experimental results for the former HD-DataStripe, considering simulated data, show the same behavior in terms of number of errors encountered in the recovered data as before. A scenario considering real-data for the smart ID-card is discussed below.

4.4.1 Smart Identity Card Representing Practical Scenario

Here smart ID-card with HD-DataStripe measuring 0.35 by 2.68 inches (2-D barcode size in Pakistan national ID-card) is used to store real-data (biographical data, portrait, signatures scans and fingerprint data). The data encoding process begins by converting analog signals: portrait, signatures and fingerprint into the digital format. Digitizing process is accomplished by the conventional document scanner; however, it would be preferable using advanced digitizing techniques such as digital signatures pad, pressure sensitive fingerprints electronics, digital camera to have high quality digitized data. Next each of the digitized data files is compressed using appropriate data compression technique. Finally, all data files compressed/uncompressed are concatenated to get the single binary file, which is encoded using error correction coding (ECC) to count for minor errors encountered during data recovery process and the resulting binary stream is transformed into the HD-DataStripe bitmap image. It is to be mentioned that data compression and ECC operations discussed in the following are intended to see the impact of these operations on recovered data. An investigation focusing on the most up-to-date biometrics data compression techniques (e.g. FBI quality fingerprints, dynamic signatures etc.) and an optimized codeword for ECC techniques (e.g. BCH, Reed Solmon) is left for the application developer.

4.4.2 Data Compression

Due to the very large size of the biometric data files, data compression is at the heart of all smart cards. As so, it is hot topic for the research to reduce biometrics data size. It is to be pointed out that each data type to be encoded needs a different compression technique, as no compression techniques designed for a particular data type works equally well for the other data type. It is to be mentioned that performance (FAR, FRR) of any extracted template is dependent on compression ratio and lower compression ratios result in better performance [KJJ04, PVT04]. Although not used in this research; however, lossy face-image data compression techniques [KJJ04] (e.g. principle components analysis) could be more appropriate in terms of higher compression ratio and good final quality.

Biographic data is not compressed, as the original file size is not very big; however, every effort is made to reduce the size of the photographic data. To achieve this goal, color image is first converted into the grayscale image and to further reduce the data size grayscale image is down-sampled. Even then the resulting file is compressed using lossy compression technique. The quality of the resulting image is still satisfactory and a human analyst can easily detect any alteration made in image printed on the card by visually comparing both the printed image as well as the one encoded into the HD-DataStripe. The objective behind the maximum image data reduction is to spare maximum capacity for the fingerprint data, which is very sensitive to any kind of data losses. Signature data is compressed using lossless run-length encoding compression technique. Finally, fingerprint data is compressed using lossless compression technique. In Table 4.4 data size before and after applying compression are given. All compressed data adds up to 68.744 K bits, which is less than 80 K bits the available capacity and the remaining capacity is left for ECC payload; however, as it can seen in the following section that ECC does not need this much payload in present scenario.

Table 4.4: Size of the compressed and uncompressed data files stored in HD-DataStripe.

	Biographical Data (bits)	Portrait (bits)	Signatures (bits)	Fingerprints (bits)
Raw data	427	61,444	42,020	41,472
Compressed	427	20,015	13,719	34,582

4.4.3 Error Correction Coding

To combat the small number of unavoidable errors encountered during data recovery, binary data stream is encoded by applying ECC. The Hamming linear ECC (63,57, 1) is used, which encodes a 57 bits message into 63 bits codeword and corrects one-bit error whereas detects two-bit error. The reason for choosing the Hamming ECC is that it can detect two-bit error with the same payload that is needed to correct single bit error, unlike other techniques such as Reed-Solomon and BCH in which 12 bits are required to detect two bit errors. This two-bit error detection can be utilized to take some other action rather than using ECC. For example, once two-bit error is encountered in a codeword, an alert message could be sent to the data-reading technique, which can switch to the alert data-reading mode. This means that the template is slightly shifted up/down, left/right, and then the codeword under consideration is read again. The alert message can also be used as a feedback control by the data-reading technique to take some other suitable measure. It is to be pointed out that 63 bits codeword length is not the optimized one, as the number of unavoidable errors is not very high; however, MATLAB "hammenco" routine for higher codeword length did not work so it was decided to use 63 bits codeword length. After encoding the data using ECC, the resulting binary data stream is transformed into the HD-DataStripe bitmap image, which is added to the smart ID-card.

Two-bit errors can also be combated effectively by using the data scrambling technique (to be discussed in Chapter 6 or any other technique). A data scrambling technique selects a pixel from binary image and puts it at another pseudo-randomly selected position and this process is repeated for all binary pixels in the HD-DataStripe. As the size of HD-DataStripe is quite large, this would further decrease the possibility of occurring consecutive errors in any message. It is also to be noted that due to the strength of the data-reading technique two-bit errors are encountered very rarely and this fact can be verified from Table 4.5, which shows two-bit errors detected in all codewords having length 63 for some of experiments given in Table-B1. In combination with data scrambling technique, 1011 codeword length is expected sufficient for the number of errors shown in Table-B1 and this would consequently consume less than 1K bits memory, resulting in ~79 K bits capacity for user payload. Similarly, codewords (255, 247, 1) and (511, 502, 1) in combination with data scrambling technique are expected to eliminate the errors reported in Table-B3, resulting in capacity for user payload more than 78 K bits, which is sufficient to store all the high quality biometrics templates (Table 4.3) for multimodal biometrics identity verification system.

Table 4.5: Number of two-bit errors encountered for 63 bits codeword length, considering the whole data.

Experiment No.	1	2	3	4	5	6	7
Two-bit errors	1	1	1	2	1	1	1
Experiment No.	8	9	10	11	2	13	14
Two-bit errors	2	1	1	1	2	1	2

4.4.4 Identity Verification Process For Smart ID Cards

To recover the data from the HD-DataStripe, first analog signal (printed smart ID card) is scanned at sufficient high over sampling rate. The HD-DataStripe is identified in the scanned document and cropped to reduce the file size. The data-reading technique is applied, which reads the HD-DataStripe bitmap image and transforms it into the single binary data stream. The binary stream is decoded by applying ECC technique and the resulting stream is decomposed into different binary data streams corresponding to the input data features (biographical data and biometrics characteristics). Each of the binary data streams is uncompressed if needed and then passed to identity verification systems. The above process is shown in Figure 4.7. In human interaction-based identity verification process, decoded biographical data and portrait are displayed on the screen to be cross-verified against the information shown on the ID card and the cardholder. For automatic identity verification decoded biometrics characteristics are passed to the biometrics identity verification system, which compares this information with the one obtained from the data collection sensors. In present scenario the decoded information is compared bitwise with the original information to ensure successfully information is recovery. And the biometrics identity verification system implementation is not addressed here.

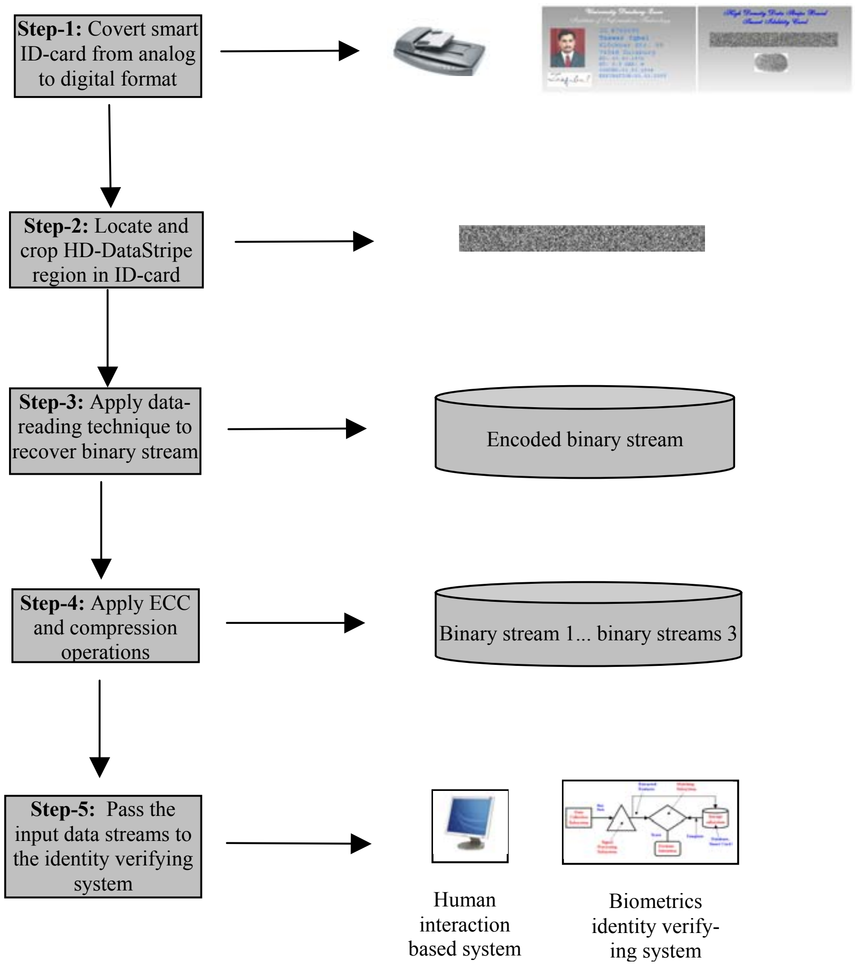

Step-1: Covert smart ID-card from analog to digital format
Step-2: Locate and crop HD-DataStripe region in ID-card
Step-3: Apply data-reading technique to recover binary stream
Encoded binary stream
Step-4: Apply ECC and compression operations
Binary stream 1... binary streams 3
Step-5: Pass the input data streams to the identity verifying system
Human interaction based system
Biometrics identity verifying system

Figure 4.7: Identity verification process for smart ID cards.

The experimental performance of the novel storage technology along with the other application related issues have been addressed in chapter-3, so are not considered here. It is to be pointed out that the novel technology results in lower data-reader cost and this can be seen from Table 4.6 showing that data-reading cost for various technologies. Further, if high quality printing devices used for security printing at 12000 dpi rather than 600 dpi, are used to print the HD-DataStripe, then data storage capacity of the HD-DataStripe can further be increased. This is based on the assumption that the security printing devices can print each and every pixel accurately at very high printing resolutions as such devices are especially designed to reproduce small size patterns.

Table 4.6: Cost comparison of various data-reading devices used in Smart ID technologies.

Technology	Magnetic stripe	IC Chip	Optical Memory	Flatbed Scanner
Data-reader cost US $	750	500	3,500-4,000	100-200

4.4.5 HD-DataStripe As Multipurpose Technology

In addition to the higher data encoding capacity (HD-DataStripe), another advantage of this research is that the need for high quality security printing devices, used to print tamperproof, counterfeit-resistant security documents is decreased due to the fact that all the data stored in the HD-DataStripe can be encrypted. Above statement is true also for the data reading devices, as the data readers to recover data from the optical memory are quite expensive. The reliance on security printing devices is further decreased by the fact that HD-DataStripe can be used as a copy detection technology (discussed before). The novel HD-DataStripe offers much higher resistance against copying attacks due to the following reasons:

1. The HD-DataStripe as a whole is used as a CDP, unlike existing technique consisting of 100 by 100 pixels CDP.
2. In copy detection mode the novel technique distinguishes between the original and copied pattern based-on above 99% correct information recovery, whereas in existing technique about (50-60)% correct data recovery considers the CDP as original.

If it is desired to decrease the copy detection time, a pseudo-randomly selected collection of pixels in HD-DataStripe can be used for copy detection. This has the advantage that for a counterfeiter it is equally difficult as to consider the whole HD-DataStripe whereas for copy detection it is more efficient.

4.4.6 Wear-and-Tear Effects: Some Remarks

An important distortion encountered in real-life applications (e.g. identity documents) is the wear-and-tear effects, which are mainly caused by aging factor and rough handling of the document. Conventionally, these effects are combated by applying ECC; however, this approach has the drawback that it is quite memory consuming, regardless the type of ECC technique being used. Recently, following a different approach, the documents from LaserCards® are being protected against wear-and-tear effects by using a transparent protective cover.

In our case those applications (e.g. passports and visa stickers), which are not prone to wear-and-tear effects because their surface is not directly exposed to dirt and scratches, can be implemented readily. For applications (e.g. identity cards, driving licenses etc.), which are prone to wear-and-tear distortion, it could be advantageous to take some other measures (e.g. using transparent protective cover) rather than using high payload ECCs, as it is not necessary to use ECC although it easy. The above suggestion can be supported by the fact that storage capacity gain for the identity documents is more expensive than the cost for using transparent protective cover.

While using transparent protective cover, for normal operation identity document can be used within the cover, whereas for the official usage when HD-DataStripe needs to be scanned, cover can be removed. Furthermore, as the HD-DataStripe based documents are not expensive, a damaged-document can easily be reprinted. In emergency the record from the central database systems, which would continue to exist in future as well for back-up records, can be accessed. In this case access-key (consisting of information encryption key, document reference number and the URL of central database), needs to be encoded separately in HD-DataStripe in such a way that it can be recovered in hostile situations. This goal can be achieved by: 1) encoding the key at multiple locations, 2) using ECC with higher error correction capability.

4.4.7 Security Aspects of Smart Identity Verification Documents

Some of the security threats that can be overcome by the proposed Smart ID documents are discussed below along with suitable countermeasures.

1. **Contents Confidentiality** Not all the contents encoded in HD-DataStripe are prone to confidentiality threat and only biometric data needs to be confidential. Both secret- and public-key encryption techniques *cannot* fulfil this requirement because once the data is decrypted it cannot be assumed confidential any more. This goal can be achieved using the transformed biometric templates (Ref. [15] in [JRU05]) (obtained from non-invertible repeatable transformation with known parameters) rather than actual templates. Another possibility to deal with biometrics data confidentiality is to use crypto biometrics systems [SSK98] in which biometric data is linked with encryption key at enrolment time. Biometric matching takes place in cryptographic domain and biometric template is never released. This approach also addresses the biometric compromising problem.

2. **Contents Integrity** The fact that all the contents shown on ID document are encoded in HD-DataStripe can ensure contents integrity, given that contents integrity of HD-DataStripe is guaranteed. Contents integrity of HD-DataStripe can be achieved using the digital signatures (DS) of the contents and requires encoding digital signatures and public-key of issuing authorities in HD-DataStripe. Finally, by comparing the hash value of contents encoded in HD-DataStripe with the one decrypted from the digital signatures, contents integrity can be ensured.

3. **Contents Authenticity** This goal can be achieved using secure PKI system from trusted third party for data encryption and contents authenticity is ensured from the private-public key pair (assumed cryptographically strong) of the document issuing authorities that has been used in DS generation process. It is also assumed that contents used to generate DS are itself authentic and DS is generated from document is-

suing authorities so only authenticity of content encoded into HD-DataStripe is concerning to us. In other words authenticity of the contents encoded into HD-DataStripe for the smart document lifecycle, starting from document issuance time and onwards, is ensured. Another approach for the authenticity verification of the biometrics data could be to use digital watermarking techniques (FMF+02, Ref. [13] in [JRU05]).

4. **Non-Repudiation** The fact that multiple biometrics characteristics (multimodal biometrics mode) can be used for identity verification would further decrease repudiation threats as compared with the identity verification systems, which use only single biometric characteristic that have limitations encountered from noise in the sensed data, distinctiveness, intra-class variations, non-universality and system circumvention.
5. **Key Management** Apart from using PKI system discussed above to address key management problem, another solution could be to use bioscrypt™ [SSK98] to encrypt full contents or only biometrics data encoded in HD-DataStripe. This would link the access to these contents with the permission of true person rather than any cardholder due to the PKI system.
6. **Counterfeiting** As the HD-DataDtripe cannot be copied this eliminates the possibility of counterfeiting threat.
7. **Cyber Attacks** On card data storage capability eliminates the threats posed by data link failure and central database systems.

Of course the threats discussed above does not cover all potential threats [JRU05] that can be encountered by a biometrics identity verification system and additional measures such as secure verifying device in which matching results cannot be manipulated neither biometrics templates can be copied would be still needed. Similarly, multimodal biometrics identity verification systems cannot address all potential threats arising from data capturing devices, replaying attacks etc. and further work is needed in these directions. Based on the above discussion it can be claimed that the proposed smart ID documents are *relatively more secure* as compared the documents using similar technologies for on-card data storage and could be *good competitors* for other expensive technologies (e.g. optical memory). It is mentionable that *LaserCard*^{R} using optical data storage technology also needs secure identity verification devices.

4.5 Contents Integrity Verification of Hardcopy Documents

As another application of the novel HD-DataStripe, hardcopy documents such as official letters, contracts etc., are focused upon in this research with the aim to find possible improvement in this context. This type of documents is to be secured against data-tampering attacks and for this purpose both analog and digital techniques are being applied. The mainly used analog methods in this context are: analog seals, special inks and papers [Ren98, Ren05]. As the analog security technologies are not addressed in this work, as a brief remark it can be mentioned that these techniques have the drawbacks: the authenticity verification process is expensive, time consuming and less-reliable due to the human-interaction dependence. The authenticity verification gets more involved while chemical analysis are required to validate documents printed with special ink as the original document is not available for comparison. In case of widely used conventional analog seals, one copy of the document is kept in record for future *manual* verifications.

While considering digital techniques for securing analog contents: 1) digital signatures, and 2) digital watermarking, have already been investigated. Although, some watermarking techniques for printed text [BBG01, BLM95, BLM99, LoM98, LoM00, AlA04] were reported as earlier as the idea of digital watermarking emerged; however, there has not been reported much work afterwards. Furthermore, the capacity offered by the existing techniques is not much (about few hundred bits) [SMS03]. Considering *digital signature techniques* for hardcopy documents, recently one such technique is patented in [Zha04] and is reviewed in the following.

This technique divides the hardcopy documents into two classes. The documents belonging to first class include bank checks and similar applications. Here some selected information consisting of critical contents, is encrypted using public-key cryptography and is used as digital signatures. For these applications message digest is not generated due to the small content size. Furthermore, to combat unavoidable errors due to OCR-reader the critical information is constrained (i.e. bounded to lie in special boxes and is printed using special font size and type). In our case such applications have been considered in section 4.2. Second type of applications has large contents (contracts, official letters etc.) that have to be secured against data tampering. Unlike before in second case the digital signatures are obtained from message digest, which is encrypted using public-key cryptography. It is to be mentioned that the in both cases size of the digital signatures is same (few hundred bits) and the signatures are encoded either into a barcode or embedded into the background image as watermark. Furthermore, to protect digital signatures against copying attack, digital signatures are required to be printed using magnetic or fluorescent inks.

4.5.1 HD-DataStripe in Digitally-Signed Analog Documents

The digitally signed analog contents generation process begins with the digital copy of the document to be secured and applies on it the following operations: lossless data compression, encryption, error correction coding, digital-seal generation, document signing and analog contents generation. The resulting document is nothing but a secured hardcopy of the original digital/digitized document. The complete process is shown in Figure 4.8. The original information might be a digital copy (e.g. doc/txt file) or the digitized version of an existing hardcopy document. The need for the latter one arises from the fact that in many cases (e.g. the old classified documents) only hardcopy is available. The key ideas can be extended to other scenario as well, however, in this research only the digital contents are focused upon.

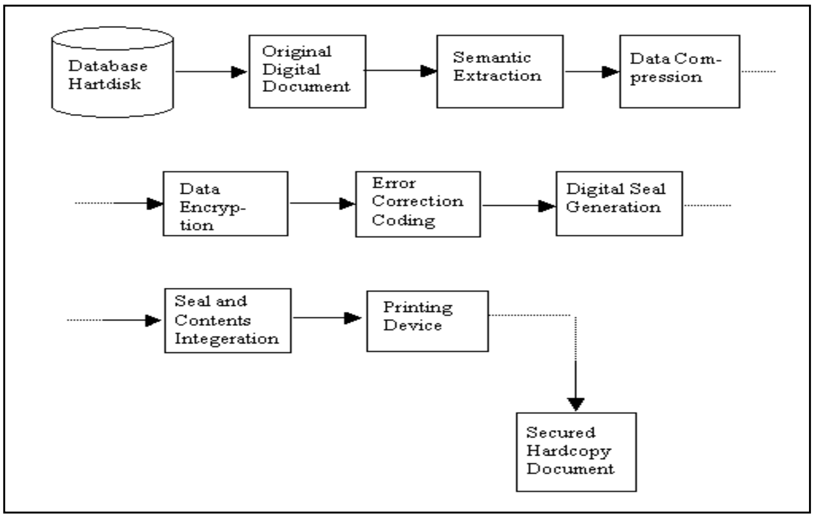
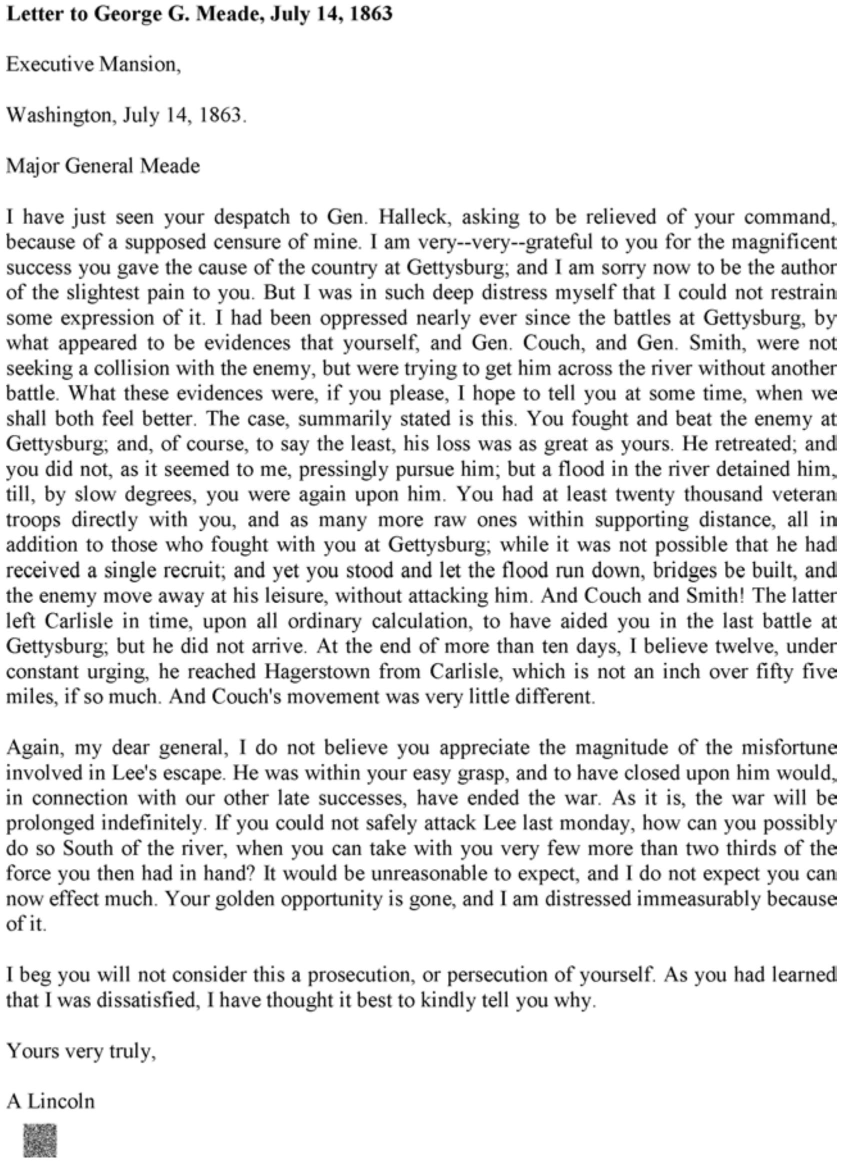


Figure 4.8: Analog contents protection process.

As a first operation the semantic information, which is visually perceptible by the human eyes, is extracted from the digital information (e.g. word document with extension doc or txt) and this information is compressed using any appropriate data compression technique for text documents. The objective behind the semantic information extraction and data compression operations is to reduce the processing time for the proceeding operations. The compressed data is passed to the data encryption stage, which produces digital signatures using public key cryptography. The digital signatures computation is a two-phase process: 1) all the information to be protected is passed to the hash function, which computes a small size message digest using lossy data compaction technique, 2) the resulting message digest is encrypted. The need for message digest, used in [Zha04], is triggered by the limited data storage capacity. In this research message digest is not computed and the digital signatures consist of full contents, encrypted using public-key cryptography (private key of the document issuing authorities).



Letter to George G. Meade, July 14, 1863

Executive Mansion,

Washington, July 14, 1863.

Major General Meade

I have just seen your despatch to Gen. Halleck, asking to be relieved of your command, because of a supposed censure of mine. I am very--very--grateful to you for the magnificent success you gave the cause of the country at Gettysburg; and I am sorry now to be the author of the slightest pain to you. But I was in such deep distress myself that I could not restrain some expression of it. I had been oppressed nearly ever since the battles at Gettysburg, by what appeared to be evidences that yourself, and Gen. Couch, and Gen. Smith, were not seeking a collision with the enemy, but were trying to get him across the river without another battle. What these evidences were, if you please, I hope to tell you at some time, when we shall both feel better. The case, summarily stated is this. You fought and beat the enemy at Gettysburg; and, of course, to say the least, his loss was as great as yours. He retreated; and you did not, as it seemed to me, pressingly pursue him; but a flood in the river detained him, till, by slow degrees, you were again upon him. You had at least twenty thousand veteran troops directly with you, and as many more raw ones within supporting distance, all in addition to those who fought with you at Gettysburg; while it was not possible that he had received a single recruit; and yet you stood and let the flood run down, bridges be built, and the enemy move away at his leisure, without attacking him. And Couch and Smith! The latter left Carlisle in time, upon all ordinary calculation, to have aided you in the last battle at Gettysburg; but he did not arrive. At the end of more than ten days, I believe twelve, under constant urging, he reached Hagerstown from Carlisle, which is not an inch over fifty five miles, if so much. And Couch's movement was very little different.

Again, my dear general, I do not believe you appreciate the magnitude of the misfortune involved in Lee's escape. He was within your easy grasp, and to have closed upon him would, in connection with our other late successes, have ended the war. As it is, the war will be prolonged indefinitely. If you could not safely attack Lee last monday, how can you possibly do so South of the river, when you can take with you very few more than two thirds of the force you then had in hand? It would be unreasonable to expect, and I do not expect you can now effect much. Your golden opportunity is gone, and I am distressed immeasurably because of it.

I beg you will not consider this a prosecution, or persecution of yourself. As you had learned that I was dissatisfied, I have thought it best to kindly tell you why.

Yours very truly,

A Lincoln

Figure 4.9: A sample digitally signed hardcopy document.

The encrypted information is encoded using the ECC to combat the unavoidable errors (discussed before) encountered during PS process. Finally, the digital seal (HD-DataStripe) is created from the encoded data and like analog seal; it is added to the document at suitable location. A digitally signed analog document using above procedure is shown in Figure 4.9.

4.5.2 Contents Authentication Process

The content integrity authentication process begins with the scanning process (as described in Chapter 3). Next the digital data encoded in the digital-seal is decoded using Data-reading technique for HD-DataStripe and the resulting data goes through all the operations performed during digital-seal generation process in reverse order. Care must be taken during the decryption process where public-key of the document issuing authorities has to be used. Finally, both the original (recovered from digital seal) and scanned contents are shown on the monitor screen in parallel and the human interaction (as in conventional authentication techniques) is prompted for contents verification. Based on the fact that the strongest existing encryption technique is employed, it is safe to claim that the primary goal of this research, the protection of large content-size valuable document against the forgery, has been achieved. It is to be mentioned that using the existing technique [Zha04] absolute protection against the forgery is not possible (as mentioned before).

To eliminate the possible flaws associated with human interaction involvement, the authentication process must be automatic and this goal can be achieved by selecting an OCR-friendly font size and type for the characters that do not cause errors during the OCR-reading process. This would not pose new challenges for the applications under consideration due to the fact that in official letters and contracts, there is no constraint for strictly using a particular font size and type. In this research initial results show that a document printed with character type courier, font size 12 and slightly higher (0.3 point) word-space, causes no error during semantic information extraction process by the OCR-reader. Any inconvenience encountered in document handling using new approach would be still acceptable due the benefits of new technology, which guarantees highly secure (i.e. one-to-one basis contents comparison) and automatic contents authentication. In case that both contents are not matched a data-tampering detection message is generated along with both contents being shown on the screen with highlighting modified areas.

The fact that full contents are encoded in the HD-DataStripe could be utilized to make further improvement in OCR performance for the more sophisticated scenarios, which are most likely to cause error. Such research can be undertaken by OCR technology developers with the aim to investigate the possible performance improvements when the contents of the document to be extracted, are known in advance to the OCR-reader.

4.5.3 Novel Versus Existing Digital Authentication Techniques

The fact that the novel technique is independent of hash functions offers the following advantages over the exiting message-digest dependent technique.

Typically, the hash functions are quite difficult to develop due to their desired properties and many hash functions, which have been considered quite strong in the past, are no more considered secure against cryptanalysis attacks [MOV96]. For example, a hash function used in [GR98] for contents integrity is successfully attacked in [KJJ04], resulting in same message digest for two different contents. This fact demands for continues improvement in the hash function algorithms. Data *compaction* and compression done in message-digest computation can be exploited to launch off-line attacks against the digital signatures.

The new digital-seal (HD-DataStripe) offers sufficient capacity to store full contents after encryption, *eliminating the need for hash functions*. Furthermore, very large size of digital signatures eliminates the possibility of launching off-line attacks. The usage of full contents as digital signature eliminates possibility of collusion attack.

In the existing technique to protect the authentication information (digital signatures) against the copying attacks, the information is printed using either the magnetic or fluorescent ink. However, the new technique (as discussed in section 4.2) is robust against the high quality copying attacks and consequently does not require other analog security features and results in less-expensive product.

The hash functions are *unavoidable* in the existing technique due to the small size digital signatures constraint imposed from the on-document data storage technologies used in [Zha04]. At the heart of hash functions; however, is OCR-technology, especially at authentication stage. Whereas, the existing OCR technology with its full advancements can guarantee in ideal case (with special font size and type) between 92-99% accuracy [Zha04]. Consequently, these facts leave the reliability of technique questionable. By exploiting these limitations, in the following a possible attack on the existing technique is described.

4.5.4 A Novel Attack Against the Existing Technique

Inspired by the fact that most of the practical applications (with unconstrained and large-size contents) demand for the exact contents authentication, in the existing authentication technique three different methods are given to *count for the unavoidable errors* in the OCR contents extraction process. According to the first method all the OCR-confusing characters (specified in advance) are ignored by the hash function during the message digest generation process when such characters are encountered. In second approach the whole document (semantic information) is scanned sequentially and each time an OCR-confusing character is encountered, it is enlisted. This way a sequence of OCR-confusing characters is obtained in which such characters are placed in the same order as they are encountered. This sequence is encoded using the appropriate data compression and error correcting techniques and the resulting data is appended to the message digest. Finally, in the third approach again the sequence of confusing characters is generated as before, however, this time both the confusing character and its location are enlisted and encoded.

Now imagine the scenario that an OCR-confusing character is replaced with another confusing character during data-tampering effort. In this case the data tampering would be undetectable by the existing technique due to the fact that in first approach an OCR-confusing character is simply ignored by the hash function. Whereas in the other cases an OCR-confusing character at a specific position is substituted by another predetermined OCR-confusing character, taken from predetermined sequence of characters. Consequently, the resulting message digest would be same as the one obtained from original document, although document has been tampered.

The consequences of interchanged confusing characters could be devastating. A simple example could be a contract having alphanumeric characters in which the OCR-reader confusing information (e.g. digits 0, 1) can be interchanged for data-tampering purpose. The above discussion gives the impression that the existing technique is effective only for the applications (e.g. bank check, paper cash etc.) with smaller and *constrained* contents and it is *not very reliable for applications* (contracts, official letters) with large-size unconstrained contents.

4.5.5 Benefits of the New Technology

1. This would allow on-line document verification, eliminating the cost and time associated with conventional document authentication procedure.
2. It results in highly reliable verification process due to the absence of human interaction and one-to-one content matching.
3. It results in low-cost end-products by eliminating the need for expensive analog document protecting techniques.
4. Application can readily be implemented using the existing printing devices and scanners described in Chapter 3.
5. Access to the full contents, encoded in digital-signatures, offers possibility for further gain in OCR-performance.

Chapter 5
Data Hiding in Printed Halftone Images

5.1 Introduction

Easy access to higher quality, lower-price desktop publishing technology has made the counterfeiting and forgery of the identity verification documents much easier and posed new challenge for the researchers. To make the documents robust against these attacks analog document protection techniques: optical variable devices (e.g. holograms, KINEGRAM®), microprinting, special inks (UV, IR, magnetic, fluorescent), special papers etc. [Ren98, Ren05] are in use since long time. However, these techniques have the disadvantage that they are expensive and usually such techniques are restricted in their usage e.g. KINEGRAM® are available only for governmental applications. Inspired by the technology advancements and advantages (low-price, high reliability) of digital authentication techniques, potential usage of digital watermarking as a counterfeiting and data tampering resistant technologies is focused upon nowadays. According to this technique a watermark (message usually consisting of the name, birth-date of document holder, a company logo etc.) is hidden in digital contents (e.g. bearer portrait) in such a way that the hidden message is robust against the print and scan process. This encoded message is recovered from the printed and scanned document and used to authenticate the contents integrity. A brief introduction to digital watermarking is given in the Chapter 2.

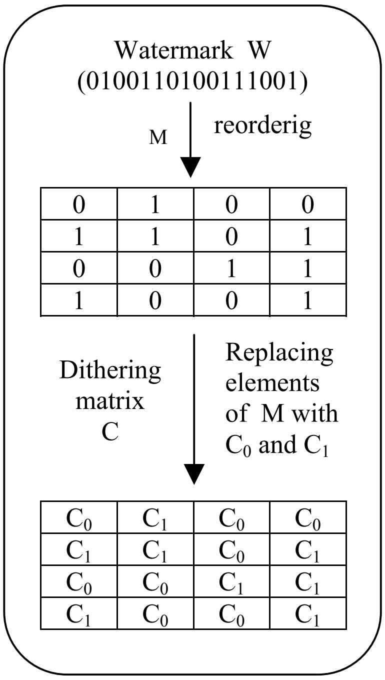
The existing research on digital watermarking mainly focuses upon digital contents: still images, video and audio and a lot of literature dealing with digital contents is available and can be found in [International Conference on Information Hiding, SPIE Conference on Security Steganography and Watermarking of Multimedia Contents, SPIE Conference on Optical Security and Counterfeit Deterrence Techniques, IEEE Transaction/Conference on Image Processing, are some of well-known sources]. In contrast to digital contents there has been reported very less work, which deals with analog contents (hardcopy). In latter case the major obstacle arises from the strong noise encountered during printing and scanning (PS) process. Furthermore, the existing techniques for hardcopy contents do not satisfy many of the requirements (imperceptibility, robustness, capacity, security, uninformed watermark decoding) of a good watermarking technique. In [CKL+97] it is claimed that the given technique allows authenticating hardcopy contents; however, the technique offers one bit watermark payload and requires original contents for watermark decoding. In addition to [HVH99, FDG01], there are techniques patented from MediaSec® [ZPT04] and DIGIMARC® [Tia04], which offer 8-16 bytes watermark capacity and work in transform domain. It is reported in [Her04, Zha04] that existing techniques are vulnerable against watermark copying attack, which allows a watermark to be copied to another document that can be used as an authentic one. In [KJJ04] it is mentioned that one serious disadvantage of existing watermarking technologies for ID cards is that the secret information hidden in printed photographs must be present in verifying devices as well, and consequently this approach has the limitation that a single broken verifying device renders the entire system broken. To overcome this problem a public-key watermarking technique is given; however, this requires much longer host signal than the existing photograph does offer. Consequently, in [KJJ04] it is concluded that the modern-watermarking-based technologies result in least robustness and performance for secure identity verification. There have been reported some techniques [HeO00, FuA02] for hardcopy contents, which work in spatial domain. These techniques transform the original contents using halftone process and the resulting halftone image is watermarked. These techniques are focused in this Chapter with the aim to gain further improvement in terms of data hiding capacity and printed image quality.

5.2 Related Work

The fact that the most of the printing devices use only one ink (black) to print a grayscale image requires that the grayscale image is converted into binary image and this grayscale-to-binary conversion, known as halftoning process, is done within the printing device. This halftoning characteristic of the printing devices is used to hide data in the printed grayscale images, which are actually black and white (binary) but are perceived as grayscale due to the low-pass filtering characteristic of the human visual system. In the research literature only few techniques are given in which it is claimed that the data hidden *in a halftone image* can be recovered after printing and scanning (PS) process. A critical review of those techniques is given below from the following perspectives: quality of the printed image, data hiding capacity and data-reading technique efficiency.

In [HeO00] the data hiding algorithm is integrated in the Ordered Dithering halftone process. This choice of the halftoning method is not random, as we shall see later on and it is governed by the requirement that the data hidden in the halftoned image being printed has to be recovered after PS process, which causes small information loss at lower printing resolutions and severe at higher resolutions.

In an Ordered Dithering halftoning a dithering cell, which is a square or rectangular block of predefined values, is used repeatedly to threshold the grayscale image. The elements of the dithering cell are selected in such a way that no artifacts are introduced in the half-toned image. To integrate the data hiding technique in dithering method, the binary sequence of the data bits (watermark) to be hidden is transformed into a square matrix having only binary elements. Then each element of the resulting matrix is replaced by another square matrix, which is selected from the two different matrices each representing one of the binary symbols “0” and “1”. The above data hiding process is shown schematically in Figure 5.1.



0	1	0	0
1	1	0	1
0	0	1	1
1	0	0	1

C_0	C_1	C_0	C_0
C_1	C_1	C_0	C_1
C_0	C_0	C_1	C_1
C_1	C_0	C_0	C_1

Dithering matrix generation process.

$C_0 = 4*$

51	27	6	46	59	12	54	7
16	63	40	23	0	42	24	33
2	34	11	49	31	15	61	47
55	26	53	17	57	38	5	21
10	43	4	41	8	28	52	39
60	20	29	62	22	44	13	32
1	48	36	9	50	3	58	25
35	14	56	18	30	37	19	45

$C_1 = 4*$

17	57	38	5	21	55	26	53
41	8	28	52	39	10	43	4
62	22	44	13	32	60	20	29
9	50	3	58	25	1	48	36
18	30	37	19	45	35	14	56
6	46	59	12	54	7	51	27
40	23	0	42	24	33	16	63
11	49	31	15	61	47	2	34

Dithering matrices C_0 and C_1 corresponding
to the watermark binary symbols “0” and “1”

Figure 5.1: Schematic diagram of Data Hiding Ordered Dithering technique.

The matrices used to represent binary symbols are selected in such a way that they do not introduce artifacts in the watermarked halftone image and *differ significantly* from each other. The resulting matrix is a dithering cell in which watermark data is encoded and this matrix is used repeatedly to binarize the grayscale image. It is to be noted that the watermark data is hidden at the multiple locations in the halftoned image as the same dithering cell is used repeatedly during the entire halftoning process. The reason for hiding the watermark at the multiple locations is to make the watermark robust against the PS process. To recover watermark after PS process two matrices (sub-dithering cells), used during watermark encoding process, are identified from the scanned image. Since each watermark bit is encoded at multiple locations, the final decision about each bit of watermark data is based on voting.

Now the fact that the *complete sub-dithering cell* (representing a binary symbol) is used to encode a single watermark bit and *same dithering cell* C is applied repeatedly increases the robustness of the hidden data against the PS process. However, this strategy of data hiding results in lower capacity for the watermark and this is evident from the 64 bits watermark payload, used in the work under consideration. Consequently, it can be said that the data-reading algorithm to recover data after PS process is not very efficient, as a lot of overhead is used to combat the PS noise. It is also mentioned in the work under consideration that the data hiding technique does not work for the images having extreme colors, covering most of the image area (e.g. images with mean graylevel above 200 or under 25). This can be explained as follows. One of the key constraints on the sub-dithering cells is that for each graylevel there should be a significant difference between the half-toned patterns obtained using both of the dither cells, so that it can easily be decided, which sub-dithering cell has been used in the encoding process. However, this constraint is not satisfied for the images having extreme color values covering large image areas, as a result patterns are not significantly different and results in decoding errors. Another weakness of the data-reading algorithm is that it enables to recover the data from the images printed at lower resolution and consequently does not offer good visual quality, a key requirement from the real-life applications.

In another work [FuA01, FuA02] by M. S. Fu et al. five different techniques for data hiding in a halftone image are given. The main focus of all the techniques except the first one is to overcome the salt-and-pepper noise, introduced during the data hiding process. In the first three techniques it is assumed that only halftone image is available. On the other hand last two techniques require that *the original continuous tone image and the halftoning algorithm* are available and the error diffusion halftoning process is used.

In the first technique called data hiding self-toggling (DHST), *N* seed-based pseudo random locations are used to hide data. To hide a single data bit at any given location the pixel value at that location is forced to change according to the data bit to be hidden. The DHST technique has the advantage that *it is simple*, but it results in many unpleasant clusters of black as well as white pixels, which resemble to the salt-and-pepper noise. The salt-and-pepper noise is mainly present at mid-tone level and is caused by the random toggling of a pixel in a checkerboard pattern formed during the halftoning process. Another side effect of the forced self-toggling is that it causes an abrupt change in the local average intensity.

Next technique called data hiding pair toggling (DHPT) addresses the issue of abrupt change in the local average intensity caused by the forced self-toggling. According to DHPT, when a pixel is toggled to hide a message bit, another pixel (slave pixel) in a 3 by 3 neighborhood is selected randomly and toggled oppositely to the first pixel so that the change in local intensity can be compensated. Although DHPT controls the local average intensity, it has the drawback that the possibility of salt-and-pepper noise still exits and now the noise is due to slave pixel, which is selected randomly and toggled oppositely to the first pixel.

To eliminate the large number of clusters of pixels, DHPT is modified with the data hiding smart pair toggling (DHSPT), according to which the slave pixel, which is used to compensate the effects of the first pixel, is selected in such a way that the connectedness of clusters is minimized. For this purpose a filter is applied, which calculates the intensity value change due to different pixels in the 3 by 3 neighborhood and the pixel resulting in minimum value of the connectedness is used as a slave pixel. It is pointed out in [FuA02] that although the DHSPT results in better image quality, however, there are still observable salt-and-pepper artifacts, especially in the regular patterns formed in the mid-gray smooth regions. Another drawback of DHSPT is that it increases the computational cost of the data hiding process.

In the data hiding techniques discussed above it is assumed that the original continuous tone image is not available. However, when the original continuous tone image is available in that case error-diffusion technique is used to eliminate the salt-and-pepper noise and two different techniques called data hiding error diffusion (DHED) and modified data hiding error diffusion (MDHED) are given. Both DHED and MDHED start with the DHST. Next rather than compensating the self-toggling distortion with the complementary toggling of one neighboring pixel (as in DHSPT), DHED and MDHED use error diffusion filter to diffuse the self-toggling error to many neighboring pixels to achieve higher visual quality. In DHED a causal kernel is used to diffuse the error. However, it is pointed out that in certain situations salt-and-pepper noise still exits, especially in the fine structures. The reason for the existence of noise is associated with the inability of the error diffusion kernel to diffuse error in the whole neighborhood. To overcome this limitation in MDHED a non-casual kernel, which makes it possible to diffuse error in the whole neighborhood, is used. It is to be mentioned that a significant effort is made to integrate the kernels in the data hiding process.

Key points of the above discussion:

a. Data hiding technique given in [HeO00] is developed by keeping in mind that the hidden data has to be robust against the PS process and this constraint results in the following drawbacks:

   1. Results in lower capacity data hiding technique.
   2. Does not work for the images having extreme mean graylevel values.
   3. It is halftoning process dependent (i.e. works only for the ordered dithering halftone process).
   4. The data reading technique is not efficient (i.e. not very robust against PS process) and that is evident from the fact that each watermark bit is encoded using a special pattern and each bit is encoded at multiple locations.

b. In [FuA01, FuA02] to hide data in a halftoned image when the original continuous tone image is not available, regardless the fact which method (DHST, DHPT and DHSPT) is used salt-and-pepper noise is unavoidable and this noise results in a poor quality printed image.

c. To overcome the salt-and-pepper noise MDHED algorithm is given, which has the following drawbacks:

   6. The MDHED algorithm is *halftoning dependent* and requires that error diffusion halftoning is used. However, the error diffusion halftoning techniques have a limitation that they are computationally expensive.
   7. The fact that Iterative halftoning techniques result in better image quality than the error diffusion halftoning techniques associates another weakness to the MDHED and demands for such techniques, which are independent of the underlying halftoning process.
   8. In case when there is a relatively large mid-tone level, a situation very likely to occur in grayscale pictures, using error diffusion salt-and-pepper noise is shifted to the neighborhood region rather than being eliminated. To be more precise consider the scenario when MDHED is applied to an image consisting of only mid-tone level.

d) One common limitation of both of the techniques discussed above is that they enable to recover data from the images printed at lower resolution (only up to 150 dpi) and this fact makes them less attractive for the real-life applications.

5.3 Data Hiding Technique For Printed Images

In this research it is found that mere improvement in data hiding algorithm is not sufficient and the task of data hiding in high quality printed images depends mainly on the *strength of data-reading technique*. Inspired by this fact a data hiding technique for the printed images while taking into account the limitations of watermarking techniques discussed above is given in this research. The strength of the proposed watermarking technique comes from both data hiding and data reading algorithms. However, the data-reading algorithm plays a major role, as it has been observed in [HeO00] that a less efficient data reading algorithm results in poor image quality and in some cases lower capacity as well. The watermarking technique given in this work results in:

1. Higher data hiding capacity.
2. Higher quality of the watermarked printed image.
3. Possibility to hide data in the images having extreme mean graylevels.
4. It is independent of the underlying halftoning process.
5. More sophisticated watermark decoding technique.

In the following sections each of these improvements is discussed.

5.3.1 Data Hiding Technique

The novel data hiding technique starts by computing the capacity of the image being watermarked and categorize the computed capacity as minimum or maximum. The minimum capacity is computed for images in which data hiding technique in [HeO00] was not successful. A 64 bits watermark payload is used as a minimum capacity in this research in contrast to [HeO00] where the watermark consists of 64 bits. After capacity computation, next the data-hiding algorithm is applied. Due to the fact that the capacity computation and data hiding algorithms are interdependent, they can be treated together. The data-hiding algorithm is independent of the underlying halftoning process and assumes that either a good quality halftone image or the original grayscale image is available. When original grayscale image is available then any halftoning technique, resulting in high quality printed images, can be used. In this research Iterative halftoning technique given in [Goo01] is used. Data hiding capacity is computed using the halftone image.

5.3.2 Watermark Capacity

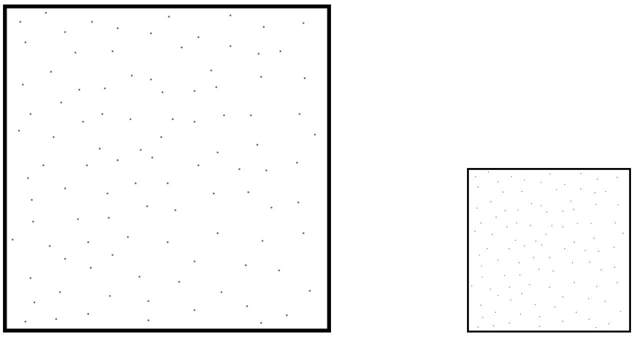
The halftone image is divided into *N* equal size regions of size *x* by *x* and each region is checked for a specific characteristic to see whether it can be used for data hiding. The selected region is characterized as a suitable location to encode single data bit, if its histogram has at the least few black pixels, otherwise, it is ignored and next region is considered. This procedure is repeated for all the regions and results in data-hiding capacity. Finally, the capacity is checked for the minimum, maximum capacity values and if the capacity value is less than the minimum value, then the number of regions is increased from *N* to *M* by reducing the size of the region and the above procedure is repeated again.

Using the above method capacity is computed initially for only few images some of which are normal grayscale images while others are special images considered in [HeO00] having single extreme mean graylevel with value either below 25 or above 200. The results are given in Table 5.1 from which it can be seen that both types of the images provide higher data hiding capacity than capacity offered by the work under consideration.

Table 5.1: Data hiding capacity for two types of images using the proposed algorithm. Note that the capacity is computed for the images of size 512 by 512 pixels and 256 by 256 pixels, respectively. NP (Not Possible)

Image type	Capacity (bits)	Capacity (bits)
Normal grayscale image (512 by 512)	26656	4096 [FuA02]
Grayscale image with extreme tone level (256 by 256)	165	NP [HeO00]

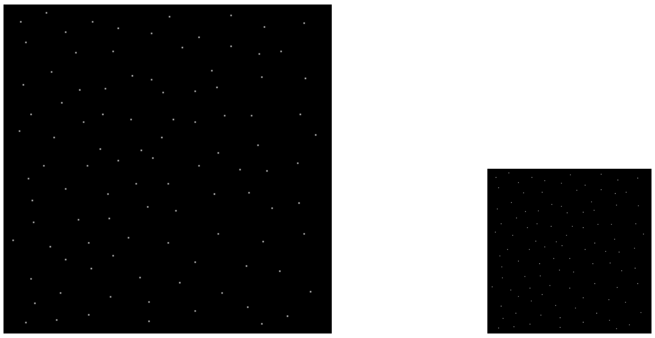
Now the reason for choosing few black pixels in the selected region is governed by the fact that a region *consisting of only white pixels* should not be used to embed data bit, as a black pixel surrounded by all the white pixels is more perceptible than the white pixel in black region. In contrast to this no constraint is imposed on the complete black background (a region consisting of all black pixels) and this is due to the reason that when a white pixel is added in the black region, the modification is imperceptible at 300 dpi. The imperceptibility is caused by the two factors: 1) very small size of printed dot at 300 dpi, 2) dot gain effects of the neighboring black pixels. It is to be noted that when a binary pattern such as white pixel surrounded by all the black pixels is printed, actually no white dot is printed due to white surface of the paper unlike black pixels where a dot corresponding to each black pixel is *supposed to be printed* (although sometimes it is not printed). Consequently, small white area suffers from the higher dot gain effects due to all the neighboring black dots, resulting in *higher imperceptibility*. The above criteria for the location selection is in agreement with experimental results as well and this can be seen from Figures 5.2 and 5.3. In Figure 5.2(a) about 100 black pixels are added at the randomly selected locations in an image having size 256 by 256 and the image is printed at 150 and 300 dpi. From the Figure 5.2 it can be seen that pixels are visible very clearly at 150 dpi and more or less are still visible at 300 dpi as well. In Figure 5.3 about 100 white pixels are added at the randomly selected locations, in a completely black image measuring 256 by 256. The image is printed at 150 and 300 dpi, respectively. From the Figure 5.3, it can be seen that modifications introduced at 300 dpi are almost imperceptible, in contrast to 150 dpi where such modifications are clearly perceptible. It is to be mentioned that the watermarked images in [FuA02] are printed at 150 dpi where noise due to PS process is not very severe.



(a) 150 dpi

(b) 300 dpi

Figure 5.2: Image having white background is modified by black pixels at randomly selected locations and printed at 150 and 300 dpi, respectively.



(a) 150 dpi

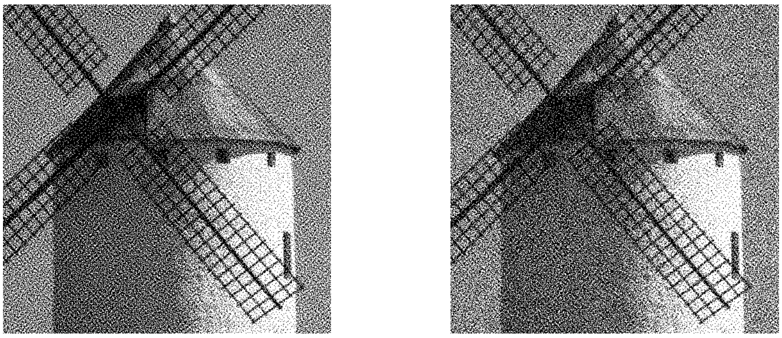
(b) 300 dpi

Figure 5.3: Image having black background is modified by white pixels at randomly selected locations and printed at 150 and 300 dpi, respectively.

The constraint requiring *more than one black pixels* in a given region is imposed from data-reading technique, which is intended to ignore the white regions during data recovery. Now if there is just one black pixel in the region, this might be flipped to white pixel during data embedding process or due to PS process noise and this would consequently result in synchronization loss for hidden data.

5.3.3 Data Hiding Algorithm

It starts with generating a fixed-size short binary stream, to be utilized in watermark decoding process to find the region-size used in data embedding process and the resulting binary stream is appended by two other binary streams: 1) representing the fixed-size binary stream showing the watermark size, and 2) watermark bit-stream. Next, a random sequence, having values varying between one and the number of elements in a *region,* is generated with the known key. To embed the binary data bit at first location the process checks the region for the condition used for the capacity computation and if the condition is satisfied, then the location corresponding to the first element of the random sequence is chosen and used for single data bit embedding. To encode "0" bit the pixel value at that location is flipped to "0", and for "1" the pixel value is flipped to "1". This procedure is repeated until the whole binary sequence has been embedded. The objective of using random location in data embedding regions is to secure the watermark locations as well as to eliminate any periodic effects caused by embedded data. In Figure 5.4 two images: a) the original, and b) after embedding 26656 data bits, are shown.



(a) Original

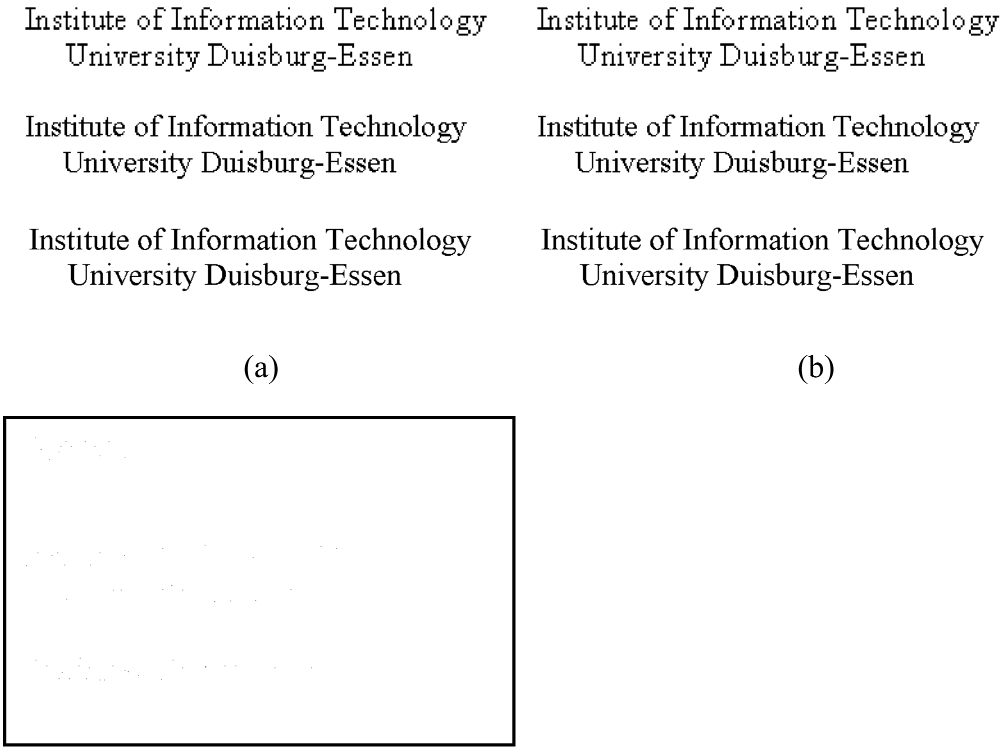
(b) with 26656 embedded bits

Figure 5.4: An illustration of quality difference between the original and watermarked images printed at 300 dpi.

It can be observed from Figure 5.4 that unlike before [FuA01, FuA01] now there is no salt-and-pepper noise introduced in the printed watermarked image. The absence of salt-and-pepper noise is attributed to two points: irregular dot placement order used in the Iterative halftoning process, and the *three times smaller* dot size modification used to encode single watermark bit during the printing process. Furthermore, data hiding algorithm *is very simple* and it differs from DHST given in [FuA02] that it checks whether a randomly chosen location is suitable for data hiding purpose or not. The condition used to check suitability of a location for data bit hiding is also very simple and does not increase the computational cost significantly as compared with the computational cost associated with MDHED [FuA02]. In addition to this, the above mentioned condition results in higher quality watermarked images *by restricting the modification* due to data bit embedding at completely white background regions where too modifications due to data hiding would degrade the image quality. The completely white background region gets more importance when there is large white background where too many embeddings would degrade printed image quality; however, for isolated small white regions this problem is not significant and especially at 300 dpi, which is used in this research.

5.3.4 Quality and Data Hiding Capacity of the Printed Images

Two very important factors, which affect the *quality of a printed document,* are halftoning process and the resolution (dots per square inch) used to print the image. To illustrate the impact of each of these factors on the final quality of the printed document, each one is treated separately in the following. To illustrate the impact of the resolution on the printed document and/or image, in Figure 5.5 an image consisting of a short text data is printed at resolutions 75, 150 and 300 dpi, respectively.


Institute of Information Technology
University Duisburg-Essen
Institute of Information Technology
University Duisburg-Essen
Institute of Information Technology
University Duisburg-Essen
Institute of Information Technology
University Duisburg-Essen
Institute of Information Technology
University Duisburg-Essen
Institute of Information Technology
University Duisburg-Essen

(a)

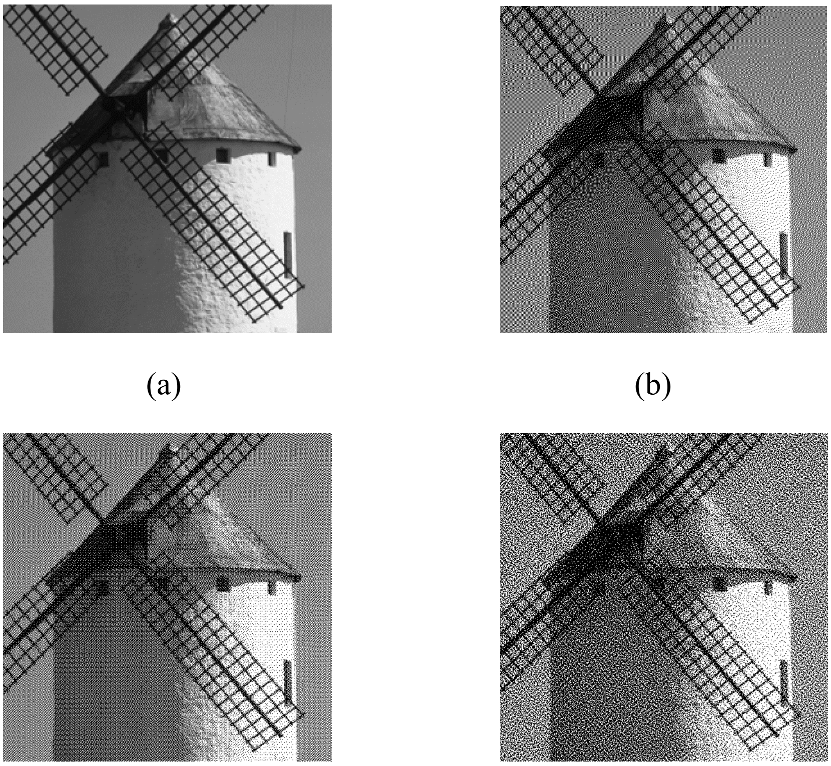
(b)

(c)

Figure 5.5: a) A piece of text printed at three different resolutions, b) same as (a) except that modifications are introduced, (c) difference between the original and the marked image. Note that the difference is visible only when the image (c) is printed at 300 dpi.

An improvement in the quality of the printed document can easily be observed with an increase in the printing resolution and from the Figure 5.5 it can be seen that at lower resolutions even individual pixels can be identified whereas at higher resolution only a smooth pattern is perceived by the eye, which is due to the fact that the human eye cannot distinguish among dots printed at 300 dpi or higher. This fact can be cleared further by the fact illustrated in Figure 5.5(b), where images are modified and as it can be seen that modifications are imperceptible at 300 dpi whereas at the lower resolutions modifications are noticeable. Consequently, from the above discussion it becomes clear that the higher resolution results in better image quality as claimed in the beginning.

Another factor contributing to the image quality is the halftoning algorithm and this can be seen from Figure 5.6 in which an image by applying four different halftoning techniques: printer's internal driver, error diffusion, ordered dithering [HeO00] and iterative halftoning [Goo01], is printed. Except halftoning process, other printing conditions such as ink, paper, printing device, printing resolution are kept same in Figure 5.6.



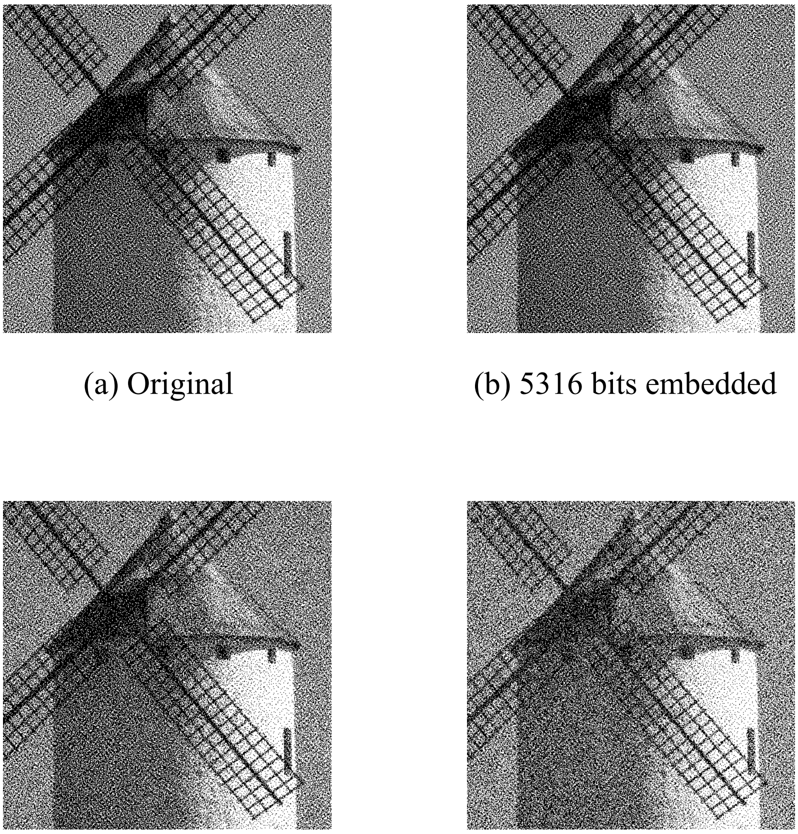
(a) (b)

(c) (d)

Figure 5.6: An illustration of the impact of halftoning technique on image quality: (a) printer driver, b) error diffusion, c) ordered dithering d) iterative halftoning technique. The images are printed at 300 dpi.

By looking at Figure 5.6 it can be noticed that Iterative halftoning technique used in this work has better quality than the ordered dithering and error diffusion halftoning techniques used in [FuA02, HeO00]. The halftoning technique used by printer driver performs better than others; however, no information about the halftone technique is available and consequently iterative halftoning is used in this research. The fact that data embedding techniques used in [FuA02, HeO00] are halftoning dependent results in dual weakness, 1) poor image quality, and 2) lower data hiding capacity in [HeO00]. These limitations verify the need to search for the halftoning independent data hiding technique. The data-hiding technique given in this research is halftoning technique independent and allows using any good quality halftoning technique.

In addition to the higher image quality, the smaller dot size at 300 dpi results in the higher data hiding capacity. This is due to the fact that an image printed at 300 dpi has three times more number of pixels than at 150 dpi. Now as the halftone image has three times more pixels as compared with [FuA02, HeO00], this would result in three times higher data hiding capacity.



(a) Original

(b) 5316 bits embedded

(c) 26656 bits embedded

(d) 47492 bits embedded

Figure 5.7: An illustration of quality of the printed image with different amounts of hidden data.

However, this smaller dot size poses new challenge, as data recovery after PS process gets more difficult. In Figure 5.7 an image is printed at 300 dpi after embedding different amounts of data. In Table 5.2 data hiding capacity offered by [FuA02, HeO00] and in this work is given. It is to be noticed that there is not significant quality difference in 5.7c-d.

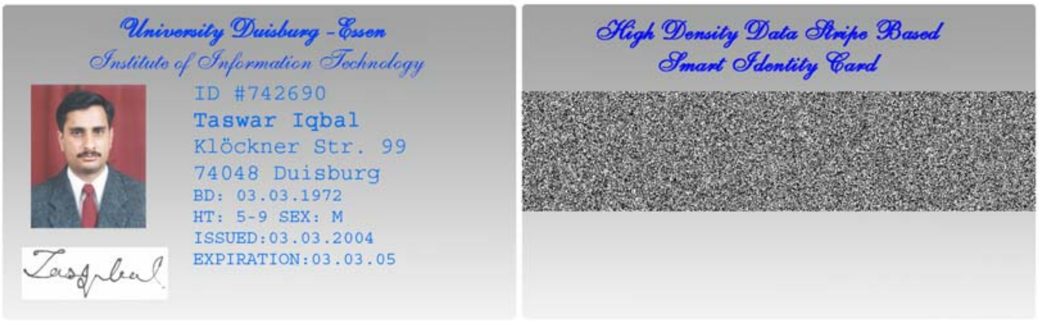
Table 5.2: A capacity comparison for different data hiding techniques. Note that the capacity is computed for the fixed image size 1.707” by 1.707”.

M. S Fu et al.	Z. Hagit	Proposed
4096	128	26656

5.4 Grayscale Images Having Extreme Mean Values

Another issue, which is raised in [HeO00] *without* mentioning its significance in real-life applications is the data hiding in special images having extreme mean graylevel (i.e. either above 200 or below 25). Inspired by the fact that it would be necessary to find some practical applications for this scenario before making any further investigations in this area, in the following some possible areas of application are described:

1. Images having the mean graylevel above 200 can be used as the background images in the documents such as identity cards, visas, passports, traveling tickets, entertainment passes, etc. As an example, consider an identity document shown in Figure 5.8, where a grayscale image having mean grayvalue 200 is used as a background image.
2. For images having bimodal mean characteristic (i.e. having extremely high as well low mean grayvalues), practical applications exists as well. Possible applications one could think about are digitized images of daily-use signatures, analog seals in hardcopy documents. Exemplary signatures and seal, shown in Figure 5.9, have only two mean (extremely high and/or low) grayvalues.
3. The images having mean graylevel below 25, which results in almost black color, might be encountered in the normal photographs, too. Imagine the scenario: grayscale picture with dark background of a person having very long hair, wearing a black dress. In this case the dominating black color may pose challenge for the watermarking technique given in [HeO00].
4. Finally, logos, portraits used in postal stamps might fall in the above scenarios. Also the special images having irregular patterns with extremely high and/or low bimodal means, considered in [HeO00] can be used in this context.



University Duisburg -Essen
Institute of Information Technology
ID #742690
Taswar Iqbal
Klöckner Str. 99
74048 Duisburg
BD: 03.03.1972
HT: 5-9 SEX: M
ISSUED:03.03.2004
EXPIRATION:03.03.05

High Density Data Stripe Based
Smart Identity Card

Figure 5.8: A smart ID-card having grayscale background with mean value 200.

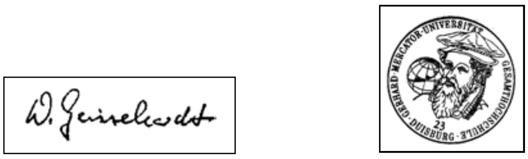


Figure 5.9: Images of signatures and seal having bimodal mean gray-value.

After having discussion about the practical application for the images with extreme mean grayvalues, next it comes to develop watermarking technique for such images. Keeping this point in mind, the data hiding technique discussed above is developed, which works for special images as well as for the normal images. The proposed technique offers the advantage that it results in the *highest data hiding capacity* for the images, which are completely black (highest graylevel), in contrast to [HeO00] where watermarking technique results in complete failure. On the other hand the images having low grayscale values, which are usually used as background image, the minimum capacity (64 bits) for the watermark is chosen. To tackle the effects of data hiding in completely white regions, where modifications results in image quality degradation, special constraint is imposed on the data hiding technique, which excludes such region in data hiding process. For initial experiments images having very much similar characteristics (size and mean grayscale values) as in [HeO00] are simulated and are converted into the halftone images, which are used for the capacity computation. In Figures 5.10 and 5.11 such images are shown along their corresponding data hiding capacity. It can be seen from Figure 5.10(b-c) that there is no quality difference before and after data embedding process and this fulfils the imperceptibility demand of the data embedding. In Figure 5.11(c) minor noise appears when the embedded white pixel has another white pixel as immediate neighbor; however, this can be avoided by flipping the previous white pixel. The quality difference between Figure 5.10(a-b) is due to the ordered dithering halftoning process used in [HeO00] and this difference would decrease by using iterative halftone technique as shown in Figure 5.6, showing the quality comparison of halftoning techniques.

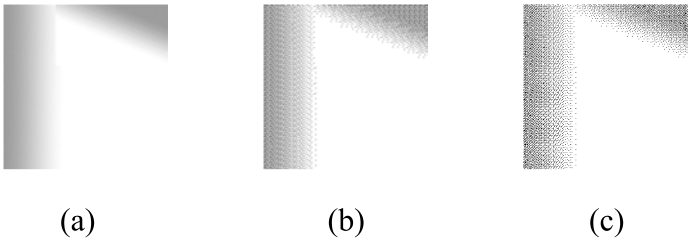


Figure 5.10: An illustration of data hiding in the images having very small mean grayvalues. In (a) original with mean graylevel 228, (b) image is halftoned using ordered dithering, (c) halftoned image after embedding 323 bits.

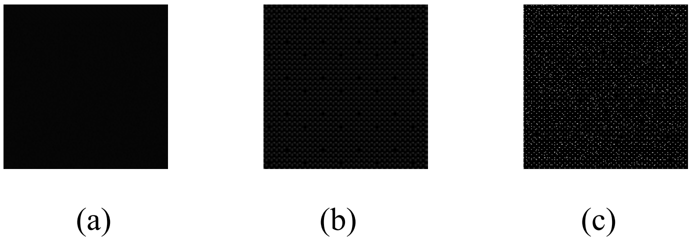


Figure 5.11: An illustration of data hiding in the images having very high mean grayvalues. In (a) original with mean graylevel 6, (b) image is halftoned using ordered dithering, (c) halftoned image after embedding 1296 bits.

5.5 Watermark Decoding Method

All the improvements discussed so far in this chapter, are made possible mainly due to the data reading technique, described in chapter 3, which can recover the data from the scanned images printed at 300 dpi. In present scenario the binary image recovered using data-reading technique is passed to the watermark decoding process that performs all the steps used in data embedding process in reverse order and proceeds as follows.

It starts by generating with the known seed value the pseudo-random sequence that has been used in the data hiding process. Next, the region-size used in data-embedding process is found by starting with default value for the region and reading fixed-length synchronization bit stream at pre-determined locations given by random sequence and comparing the resulting bit stream with the known one. During region-size determination different known size are considered. Once the region-size has been found then fixed-length binary bit stream representing watermark payload is decoded (to know how many samples are to be taken) by sampling data encoding regions at the locations determined by random sequence. Finally, watermark bit stream is read by taking fixed number of samples while taking into account the constraints (i.e. region having at least few black pixels, sampling the region at predetermined random location) used during the data hiding process. The experiments for the quantitative performance measures are not yet conducted; however, based on the experiments results for HD-DataStripe (chapter 3), it is claimed that hidden data can be recovered successfully

5.6 Security Aspects of the Data Hiding Technique

The proposed data hiding technique satisfying two important demands: higher capacity and improved quality of watermarked image, offers only a good hidden communication channel and anyone knowing the algorithm can modify the hidden contents. Furthermore, according to Kerchoff's theorem in a secure system it is assumed that algorithm and its parameters are publicly known so they cannot contribute to system security and additional measures for contents security are needed. While considering existing work in this context, there have been proposed different techniques, allowing both contents integrity and authenticity verification discussed in chapter-2, but have the drawbacks as discussed before. In the following, using the key principle given [Kim05], it is shown how the cryptographic security can be achieved for the data hiding technique given in this chapter.

5.6.1 Semi-Fragile Watermarking Technique for Printed Images

The technique is based on the existing principle, according to which host image is divided into two regions and digital signature (DS) of one region (set of pseudorandomly selected locations generated with public-key) is embedded in other region. The main challenge in present scenario is encountered from innocent noise (unavoidable errors) arising from PS-process and potential wear-and-tear effects. This issue can be tackled using a probabilistic (as in inverible watermarking techniques) contents integrity verification approach with minimum false reject rate (FRR). Broadly speaking, contents integrity verification process separates the host image in multiple regions of two types and the DSs of one type of region are embedded in other type of region. The size and pixel selection method for a region used in DS computation is governed by innocent noise behavior.

To be more specific the host binary image is partitioned into two types of regions (primary, secondary), where the number of primary/secondary regions is two or more. Furthermore, all primary regions are non-overlapping, whereas secondary regions are overlapping. The size of all primary regions is equal and determined by the size of DS and ECC overhead (if applied). A secondary region consists of 80-90 % of randomly selected pixels, except those included in any of the primary regions. Pixels belonging to each secondary region are selected pseodorandomly with uniform distribution, but with different publicly-known keys. The DS of each secondary region is computed and embedded in the corresponding primary region. For contents integrity verification DSs are extracted from the primary regions and compared with the DSs computed using corresponding secondary regions. If extracted and computed DSs for all the primary and secondary regions are matched then contents integrity is ensured. Finally, given that private-public key pair(s) is generated from trusted third party, would ensure authenticity of the contents.

5.6.2 Robustness Against Innocent Noise

The selection of secondary region size is governed by unavoidable errors caused by PS-process and wear-and-tear effects. It is to be mentioned that although errors from PS-process at optimal channel utilization is less than 1% (as shown in chapter-3), there have been used only 80-90 % pixels in a secondary region. The reason for ignoring (10-20)% pixels is to count for dust-and-scratches noise. In practical-life (10-20)% noise might be too high as pixels are selected pseodorandomly with uniform distribution, which minimize the effects of burst errors.

5.6.3 Robustness Against Malicious Attacks

While considering potential malicious attacks, only (10-20)% of pixels that are uniformly spread over the entire contents, are available and this fact would restrict to make any meaningful contents changes. Another possibility could be to modify all pixels in a secondary region with the objective to attack the DS. This is also not realistic (apart from strength of DS), as it would require changing all pixels of secondary region, consequently resulting in an image that is degraded beyond recognition. The aim of using multiple secondary regions is to cover the most of host image and results in more contents tampering sensitivity against the malicious attacks, but might increase the false reject rate (FRR). Of course, only one primary and secondary region would work as well with probably larger secondary region. Here general approach is discussed and selection of multiple or single secondary regions will be decided by the application developer. Also, either same or different private-public key pairs can be used, determined by the security-level of the final application.

One important attack in printed images authentication is watermark copying attack in which watermark is estimated from high quality scanned image and used in forged image [PVT04]. However, in the proposed technique as watermark is host image dependent this fact restricts the decoded watermark to be copied to the contents other than the intended one.

5.6.4 Miscellaneous Issues

The selection of primary regions must take into account the visual impacts of the embedding process (as discussed in previous sections) and this may not allow to select primary regions randomly; however, even if region is found deterministically it will not affect the security any way. There could be another way that would not only allow choosing the primary regions pseudorandomly but also results in slightly higher capacity of watermarking channel. This can be done by *mapping the gamut* of host grayscale image from 0-250 to 0-220 before halftoning, which slightly degrades the halftone image quality by changing the completely white regions with slightly darker regions. But, the resulting halftone image not only offers slightly more capacity than before but also relaxes the constraint on embedding process, requiring to ignore completely white regions, as they do not exist any longer. The impact of grayscale gamut mapping on image quality can be seen from Fig. 5.12, which shows that the resulting image quality is still satisfactory. Furthermore, in context of *identity verification* applications small quality difference is not important. In Fig. 5.12c mapping of the fully back (0) graylevels to slightly light (30) graylevels has no impact on the data embedding process but can be helpful to tackle the minor noise in Fig 5.12c and also seems to be more pleasing than Fig. 5.12b.

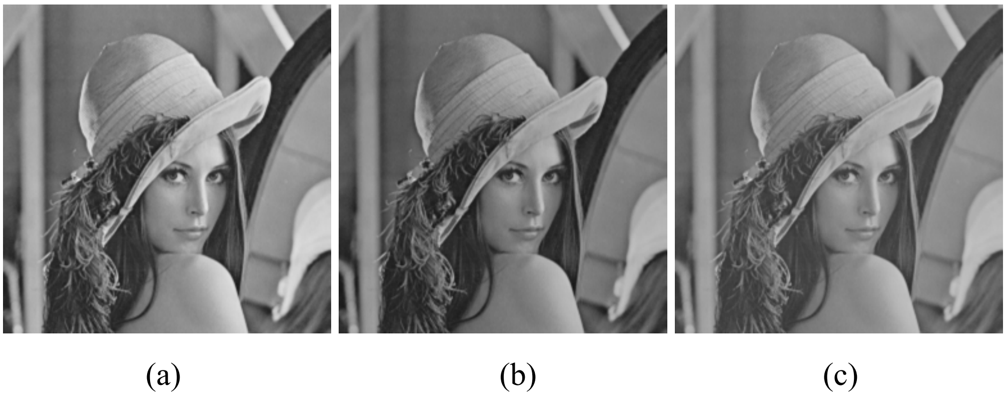


Figure 5.12: Illustration of slight gamut mapping effects, a) original Lena image with full color gamut, b-c) after 0-220 and 30-220 gamut mapping, respectively.

It is mentionable that capacity consumed by embedded multiple DSs is much smaller than the total available capacity and the remaining capacity can be used to embed some biometrics template (as in (Ref. [13] in [RSU05]) whose integrity can be ensured as well. As mentioned earlier another possibility could be to integrate the fragile watermarking technique given in [Ditt01] and this would offer two benefits: 1) possibility to locate modified region and 2) alternative way of contents integrity detection, resulting in more robust technique. However, this would require modifying the existing visual feature extraction techniques for binary images by taking suitable measures. Then accordingly the watermarked binary image (not watermark) recovered from PS-process can be used to detect and differentiate between the innocent and malicious changes as well as locating maliciously modified regions. The higher data hiding capacity could be attractive for hologram watermarks technique given in [DSF02, FMF+02] as well.

The security of proposed technique given above can be further improved by binding the hash value of the contents (secondary region) with some suitable biometric characteristic of the person whose contents (face image) are targeted to be authenticated. This would eliminate the threat posed by replacing watermarked face image of a person on an ID card with that of another person and threat arises from the fact that two watermarked contents (e.g. face image on the ID card) obtained using secured PKI system cannot result in identity verification failure when one is replaced with another one. This threat could be particularly posed to identity verification applications. The selection of biometrics characteristic is to be governed by the size of the biometric template so that the size of the hash value of the contents plus biometric template (not its hash value that is not guaranteed to be always same) along with the other constraints (size of DS and public-key) remains within the capacity limit. Here transformed biometric template (Ref. [15] in [JRU05]) or any other biometric template (Table 4.3 pp. 89) can be used. In verification process contents integrity of the face image and the fact that this face image belongs to genuine person is authenticated.

Chapter 6
Data Hiding in Background Images

6.1 Introduction

Recently a data hiding technique for hardcopy documents such a Cinema tickets, contracts etc. is given in [SMS03] by Suzaki et al. This technique allows encoding *Hidden Message* in a *Constant Grayscale Background Image* (CBGI) and claims higher data hiding capacity as compared with the previous techniques given for similar applications. In this research an improved data hiding technique for CBGI is given and discussed in this Chapter. The new technique uses CBGI of the same quality as in [SMS03] to encode contents integrity related data, but it offers much higher capacity that is sufficient to encode both contents integrity related extracted features as well as the full contents of the document. And this fact allows developing much stronger methods for contents integrity verification and offers some additional benefits too. The novel technique uses different data encoding technique, but still results in same quality of the background image as in [SMS03]. It is also possible with the encoding technique to get different graylevels. The data-reading technique given in this work enables to recover the encoded information from noisier environment as compared with the existing technique. For performance evaluation of the novel technique more than one printer are used. Finally, in the existing technique no results are reported for practical applications, whereas in this research issues related to the practical applications (ECC, data dispersion, superposed foreground text, skewing distortion) are considered as well. The results of the novel technique are found promising while considering another technique DataGlyphs® that is also being used to encode data in background image. Finally, this chapter ends with a comparison between the novel technique and cryptoglyph technology discussed in chapter 4.

6.2 Brief Review of Existing Work

To encode hidden data in hardcopy text documents different techniques have been proposed. In [BLM+95, BLM99] three methods (exploiting lines, words and individual character characteristics) for information (source and/or destination fingerprints) encoding in text documents are given. Whereas [LoM98, LoM00] deal with performance analysis and capacity derivation of these methods. In first method every other (even) line is slightly shifted up or down to encode single information bit. For information decoding odd lines are used a reference and data is decoded by estimating the distance of information carrying lines with respect to the reference lines. The information decoding process is robust against the print-and-scan process and does not require the original contents. The second method divides the information on each line into groups of words and slightly shifts left or right every even group to encode single information bit, whereas the odd groups are used as a reference to decode the information. To decode the information correlation and centroide-based methods are suggested, however, both of these methods require original contents for information decoding from the printed and scanned document. The third method encodes data by modifying individual characters, resulting in more capacity, but needs original contents for information decoding.

In another work Marshal Bern et al. [BBG01] destination related information (fingerprints for traitor tracing) is encoded by slightly stretching or shrinking specially selected characters and requires *original contents* while proving unauthorized document transfer at court. In the same work contents integrity is focused upon as well by following a new approach similar to the one used in [SMS03 to described shortly]. There is anther technique [MWM01] in which shape of each of the characters is slightly modified to encode hidden message, however, the performance of this technique is not reported for hardcopy documents and is used to encode secret message in softcopy of a text document. Recently, in [AlA04] fingerprints data is encoded in text documents containing justified paragraphs and irregular line spacing by slightly increasing/decreasing spaces between the words and lines. Spread-spectrum technique is used to combat for irregular line or word spacing. To make the document robust against printing and scanning the payload is protected using BCH error correction coding. The data is decoded by measuring the distance between words and lines and correlating it with the spreading sequence. All of the above techniques have one common drawback that their capacity is contents dependent and is not sufficient for many applications (e.g. contents integrity verification) of hardcopy documents.

There is another technique given by Suzaki et al. [SMS03], which uses a different approach for data hiding and claims higher data hiding capacity as compared with the existing techniques mentioned above. This technique differs from the existing work that its capacity is not contents dependent. As this technique is the main focus of present research, so it is reviewed from the perspective of this research in the following.

6.3 Existing Data Hiding Technique for Background Images

In this technique a constant background grayscale image (CBGI) is superposed to the foreground text and this background image is used as a channel for hidden communication to encode information related to the foreground contents. To encode data in the background image two different symbol patterns are used to encode “0”, and “1” bits. As a hidden message some selected features of the foreground text are used for contents integrity verification. To recover the hidden data after PS process the 2-D Gabor filter is applied to recognize each of the symbol patterns, used to encode the information bits.

The CBGI is obtained by repeatedly applying a specially designed fixed-size binary pattern, known as Null Symbol (NS) pattern. Two *different symbol patterns* used to encode data in background image are obtained from the NS pattern with the constraint that a good symbol pattern should have the following characteristics: offers higher capacity, difference in symbol patterns is visually imperceptible and can be recognized efficiently during data recovery process. The information encoding symbol patterns along with the NS pattern, given in [SMS03], are shown in Figure 6.1. A small part of the two CBGI used in [SMS03], one with the hidden data using information encoding Symbol Patterns and the other one without hidden data obtained by repeatedly applying the NSP, are shown in Figure 6.2.

It can be seen from Figure 6.2 that the quality of CBGI in both cases is same. To differentiate between the symbol patterns representing "0" and "1" bit, two parallel lines (indicating the direction of the standing-axis) each consisting of 4 black dots within the symbol pattern, are aligned in a specific direction and this difference in alignment/standing-axis is used to identify a particular symbol pattern after PS process. The capacity offered by an A-4 size background image (6684 x 4900 dots at 600 dpi) with symbol size (18 x 18 dots) without taking into account noises encountered during practical applications is 95,347 bits. To compensate for the errors encountered in decoded symbol patterns due to the foreground text overlapping, BCH ECC with 2047 bits code length is used, which reduces the resultant capacity to 51.5K bits, 25.0K bits, 11.5K bits for 5%, 10% and 15% errors due character overlapping, respectively. It is mentionable that 324 dots are used to encode single information bit.

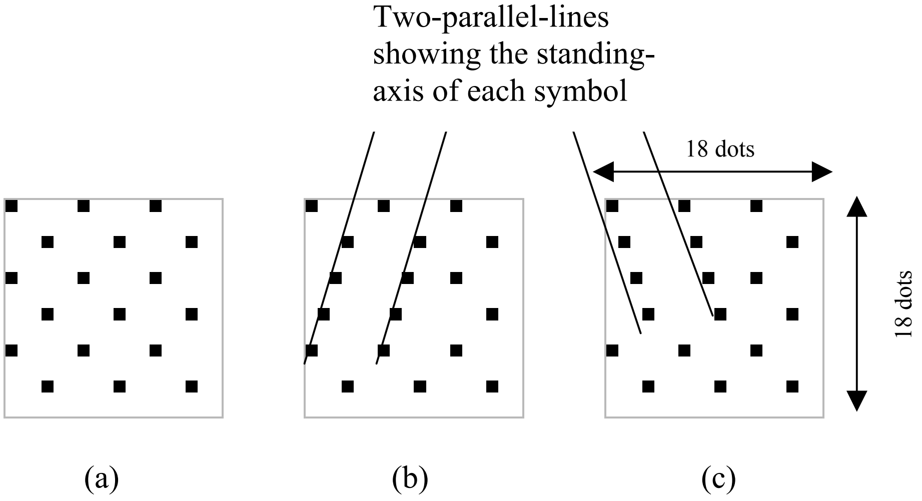


Figure 6.1: Data encoding symbol patterns (18 x 18 dots) used by Suzaki et al., (a) Null Symbol Pattern, (b) "1" bit encoding Symbol Pattern and (c) "0" bit encoding Symbol Pattern.

Figure 6.2: (a) Small part of the constant grayscale image obtained using Null Symbol Pattern given in [SMS03], (b) image with encoded data using Symbol Patterns shown in Figure 6.1.

It is clear from above discussion that to gain any further increase in the capacity offered by [SMS03] either symbol pattern size has to be decreased or the number of different symbol patterns is to be increased, while keeping the symbol pattern size fixed. However, either of these approaches poses challenge at symbol identification stage when the encoded data is to be recovered after the PS process. Consequently, according to the existing technique while designing symbol pattern to get further increase in capacity, the size and shape of the symbol pattern should be selected in such a way that it can be *identified correctly* during data recovery process.

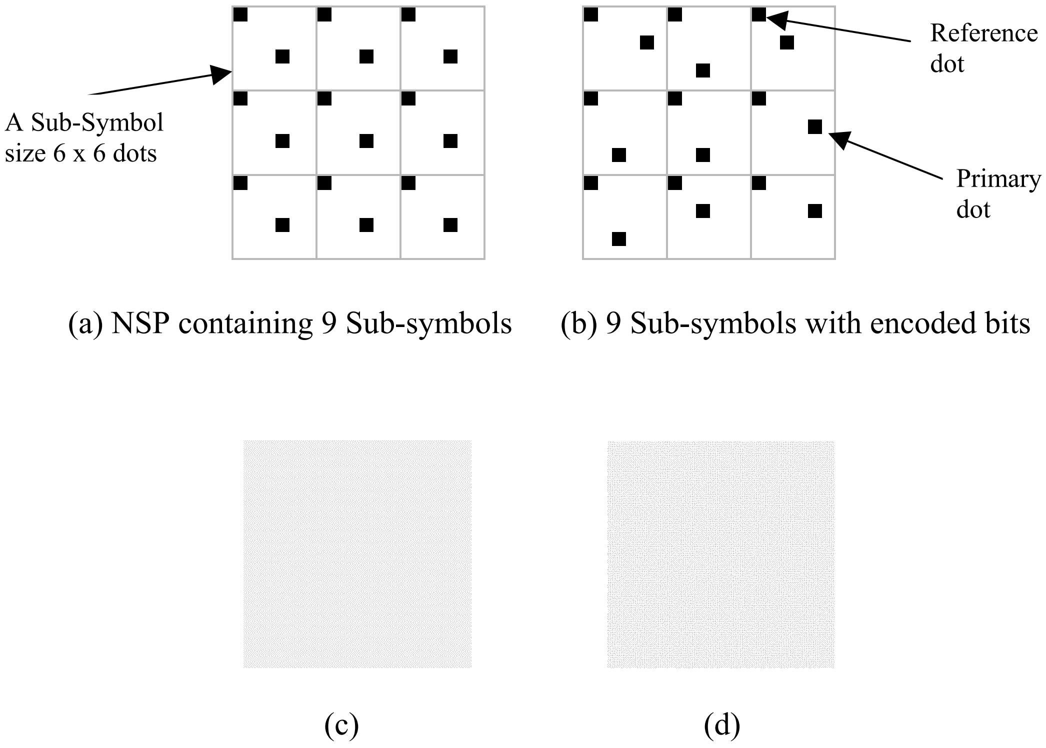
There is another technique called DataGlyphs® [Hec94, MBB04] developed by Xerox PARK, which allows encoding data in the background image. In DataGlyphs two different symbols: BACKWARD SLACH "\" and FORWARD SLACH "/", each measuring 1/100th of an inch are used to encode “1” and “0” bits. This technique allows encoding *most of the foreground text* in full-page size background image and is used by Marschall Bern et al. in [BBG01] for contents integrity authentication.

6.4 Novel Data Hiding Technique for Background Images

The main objective of the novel data hiding technique for background images is to get further gain in the capacity while using similar approach for data encoding as one discussed above. In order to achieve this goal a single small-size information encoding symbol pattern with multi-bits data encoding capability is employed. The usage of such symbol pattern is encouraged by the capability to identify the individual dots reliably in the noisy environment. Furthermore, this technique takes into account the underlying characteristics of the printing device as well to get further gain in capacity. While considering errors caused by the foreground character overlapping, instead of relying on ECC it is decided to ignore the overlapping symbols and replace such areas with null symbols to eliminate any visual artifacts. To minimize ECC payload to combat for unavoidable errors, the encoded data is scrambled all over the background image. The nature of information encoding symbol *allows multiple graylevels to be used* with the same data encoding capacity. In the following sections each of these points is discussed.

6.4.1 Novel Data Encoding Symbols

In this research the *Null Symbol Pattern* given in [SMS03] is used, so that it results in the same background image quality. Next the 18 x 18 Null Symbol Pattern is partitioned into 9 sub-symbol patterns and each New Symbol Pattern (NSP) with size 6 by 6 contains only two black dots, which are known as primary and reference dots. The primary dot is used to encode the information, whereas the reference dot is intended to assist in data recovery process and with respect to this dot the location of primary dot is found, in information decoding process. In this technique multiple bits of information are encoded in one NSP and this is achieved by shifting the position of the primary dot within the symbol pattern at *four different* locations. In Figure 6.3 a Null Symbol Pattern and various new symbol patterns with encoded information are shown. In Figure 6.3(b) a Null Symbol Pattern is shown in which 18 bits of information are encoded using New Symbol Patterns. In Figure 6.3(c-d) a small part of CBGI is shown to illustrate the quality difference with and without encoded data in the background image.



(a) NSP containing 9 Sub-symbols (b) 9 Sub-symbols with encoded bits

(c) (d)

Figure 6.3: (a) Nine sub-symbols within a Null Symbol Pattern (18 x 18 dots) used by Suzaki et al., (b) Nine New Symbol Patterns, encoding 18 bits of information, (c) a resulting grayscale image with hidden data, (d) encoded using [SMS03].

It is also mentionable that here only one dot (primary dot) is used to encode multiple information bits and *no strong constraint* like Standing-Axis in [SMS03] is imposed on data encoding symbol. The alignment constraint used in the existing technique would make it more sensitive against the skewing distortion in data recovery process as compared with the new approach. In Figure 6.4 some graylevels offering same capacity as before and obtained by varying the number of black dots in information encoding symbol are shown. Obviously, more graylevels can be obtained by using other printing colors: Cyan, Magenta and Yellow.

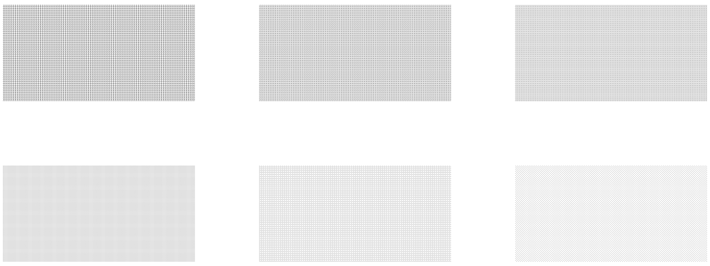


Figure 6.4: Illustration of the multiple graylevels for the novel data encoding symbol.

The proposed data hiding technique to encode data in background images is categorized into two classes. In first class data is simply encoded into the CBGI, using information encoding symbols, given in section 6.3. In second category while using the same information encoding symbol as the one used in first category the characteristics of the underlying printing device are utilized with the aim to get further gain in data encoding capacity. This technique, which is called *An Improved Information Encoding Technique,* is described after giving the data-reading algorithm for the first class.

6.4.2 Capacity Offered by the Novel Technique

In general the capacity, *C*, offered by either of the techniques under consideration, without taking into account the noises encountered during practical applications, can be computed using the following relation:

$$C = [(x \cdot y)/\sigma^2] \cdot \omega \qquad (6.1)$$

where x , y is are number of dots in the horizontal and vertical direction of CBGI, respectively. σ is symbol size in dots and ω denotes the number of bits encoded per symbol.

Now the existing technique with $x = 4629$, $y = 6685$, σ=18 and ω=1, results in $C = 95.5$ K bits. Whereas the new technique with $x = 4749$, $y = 6775$, σ=6 and ω=2, results in $C = 1721$ K bits, which is 18 times more than the capacity offered by the existing technique. It is to be pointed out here and afterwards 1 Kbits represents 1000 and not 1024 bits.

6.4.3 Data Encoding Algorithm

The data encoding technique can be described as follows: 1) extract the selected features from the text data, 2) encode the information (selected features as well as the full contents of the text document) using appropriate error correction code against the unavoidable errors, 3) encode the information in the grayscale background image, and 4) superpose the foreground text to the CBGI. The data encoding process is shown schematically in Figure 6.5. Each of these points will be discussed in the following sections.

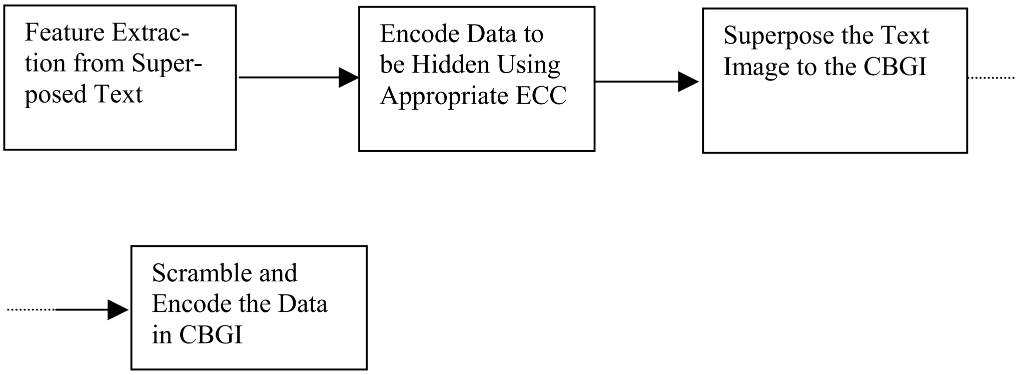

Feature Extraction from Superposed Text
Encode Data to be Hidden Using Appropriate ECC
Superpose the Text Image to the CBGI
Scramble and Encode the Data in CBGI

Figure 6.5: Schematic diagram of data encoding process.

6.5 Data Recovery from Background Images

Despite its higher capacity as well as simplicity, the new technique is of any value only if it enables to recover the data successfully, whereas the size of the each and every isolated dot is 25% of the size used in HD-DataStripe (Chapter 3). Also the new technique has only one dot (primary dot) for recognition, unlike [SMS03] where a certain pattern is identified to decode single bit of information. The strength of noise being encountered during printing and scanning process can be envisioned from the fact that an 18 by 18 size symbol pattern (means 324 dots) is used in [SMS03] just to make the encoded symbol robust against the PS process. Now, the task of the data-reading algorithm is to identify each of the printed dots, especially the primary dots, used for information encoding. It finds the position (middle point) of the primary dots with respect to the neighboring reference dots and eliminates the noises introduced during the PS process. From the research on HD-DataStripe it is found that in order to develop a successful data recovery algorithm it is helpful that the underlying characteristics of the printing device going to be used later on are well-studied and are taking into account in advance. The data-reading algorithm developed in this research can be divided into two categories. The data-reading algorithm belonging to the first category has relatively lower capacity and is applicable to the devices with 600 dpi. The other data-reading algorithm is more sophisticated and is applicable to the scenario in which the underlying characteristics of the printing device are taken into account during data encoding process with the aim to have further gain in capacity.

6.5.1 Category-1: Data-Reading Algorithm

This data-reading algorithm is developed for the LaserJet printing technology in which image is printed at full resolution (600 dpi). The algorithm proceeds as follows:

1. Printed CBGI is scanned at sufficiently higher resolution as grayscale image, resulting in *a dot* consisting of a cluster of many pixels of same type (i.e. having gray-value above certain level).
2. The position of each of the reference dots is located using Filter-1.
3. The position of all of the primary dots is estimated using Filter-2. Filter-2 takes into account the noises due to PS process, which results in the inaccurate positions of the primary dots. Filter-2 considers some other noises in the neighborhood as well.
4. Finally, the encoded information is decoded back using the position of the primary dot with respect to the neighboring reference dots.

Each of the above Filters is described in the following.

Filter-1: Reference Dot Recognition

The operation of this filter can be described as:

Step-1. Start with the given initial point having coordinates (*x, y*).

Step-2. Select a region of fixed length and width around the initial point given in step-1 and finds the global minimum value within that region. The coordinates of this minimum value point are considered as reference point.

Step-3. A fixed value is added to the coordinates of *global minimum* found in step-2 and these new coordinates are used as a starting point used in step-1 to identify the next reference dot. Then steps 1-2 are repeated.

Filter-2: Primary Dot Recognition

The purpose of this filter is to eliminate noise in the surroundings of the primary dots. The noise being eliminated is due to the fact that the primary dot is printed at a critical region where it is not possible to find its shortest-distance from the four neighboring reference dots. The operation of this filter can be described algorithmically as follows:

Step-1. For a given reference dot, finds neighborhood region, where the primary dot is supposed to exist.

Step-2. Within the region formed by four reference dots surrounding the primary dot, fixed area is selected and primary dot is searched for. The primary dot is characterized by a pattern of connected pixels having value more than a certain threshold value and result from over sampling process.

Step-3. Finds the center (coordinates) of the primary dot and checks whether it is at critical position. The critical region is formed by the fixed-width horizontal and vertical stripes passing through the center point that has coordinates as the average value of the central points of reference dots. So if primary dot is found on any of the critical regions formed above then additional measures are taken.

Step-4. If *primary dot* is found at critical region then a small fixed region around it is selected and a gradient of luminance value is computed and the direction in which slope of the gradient value decreases slowly, the coordinates of the *primary dot are shifted in that direction* and the information is decoded with respect to these new coordinates of the primary dot.

Step-5. To decode the information, minimum distance of the primary dot from the four neighboring reference dots is counted and procedure used for information encoding is used in reverse order.

Step-6. The steps 1-4 are repeated for all reference dots.

Results and Discussion

The results of the above data-reading algorithm for a CBGI, which measures 4200 by 3000 dots and offers 700 Kbits, are given in Table 6.1. By analyzing the errors reported in Tables 6.1, it is found that the errors are mainly caused by the following factors:

1. **Unprinted Primary Dots:** This is main cause of the errors encountered in decoded symbols, which are printed with HP8000 printing device, might be attributed to toner behavior (i.e. getting empty) or relatively old printing device.
2. **Inaccuracy in the Position and Size of the Primary Printed Dot**: This is the main cause of the errors encountered in decoded symbols, which are printed with HP4600

printing device. The primary dot is printed at the center (a critical region) where no decision can be made reliably about data decoding. The dots are printed bigger than the expected size and usually their size is so large that it extends to the region of the neighboring reference dot, which is not the closest one. Also the reference dots cause error and some kind of duplication is noticed in these dots as well. Although, the positions of the reference dots are recognized correctly, but their influence on the primary dots is found beyond recovery.

3. **Noise in the Neighborhood of Primary Dot**: This may arise either from the printing process or due to other factors such as stains on the scanner or paper surface.

Table 6.1: Number of errors encountered in recovered symbols for 350 K symbols (700 Kbits) considering two different printing devices at 600 dpi.

Experiment No	Errors Printer-1	Errors Printer-2	Experiment No	Errors Printer-1	Errors Printer-2
1	>2000	22	6	63	1574
2	75	1920	7	91	
3	>1500	38	8	167	
4	56	1288	9	37	
5	60	1179	10	27	

Printer-1: HP8000 Printer-2: HP4600
Note: Due to poor performance further experiments are not conducted for Printer-2

Before proceeding further it is to be mentioned that for HP8000 printer a 2 by 2 inch CBGI offering 80 Kbits capacity is investigated as an application in which a grayscale image of size 100 by 75 is encoded. And it is found that BCH (127, 99, 4) not allows correct information recovery; however, optimized BCH code is not investigated. The data-reading time is found 60 seconds.

6.5.2 Category-2: Data-Reading Algorithm

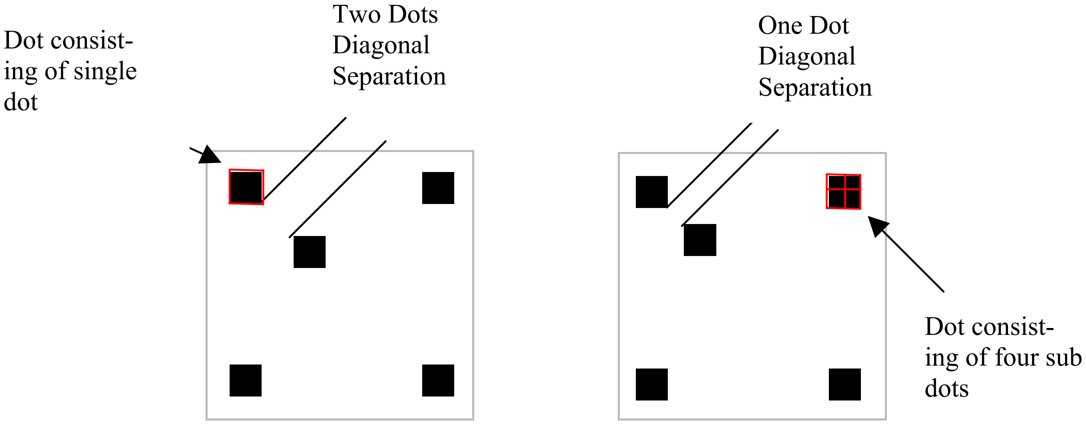
Unlike data-reading algorithm described above, now the data-reading algorithm is developed for the scenario in which characteristics of the underlying printing technology are taken into account during data encoding process with the aim to get further gain in performance. For this purpose first the information encoding technique, which allows integrating the characteristics of the underlying printing device during data encoding process is described. And then the Data-Reading Algorithm is given.

An Improved Information Encoding Technique

This technique is similar to first one (uses same information encoding symbols and background image) except that it utilizes the characteristics of the underlying printing device as follows:

Higher Resolution: The device offering higher resolution is used due to the fact any good quality LaserJet printer should be able to print reliably at half of its resolution. So the printing devices offering resolution 1200 dpi are considered for the further improvement in terms of higher capacity and lower error rate.

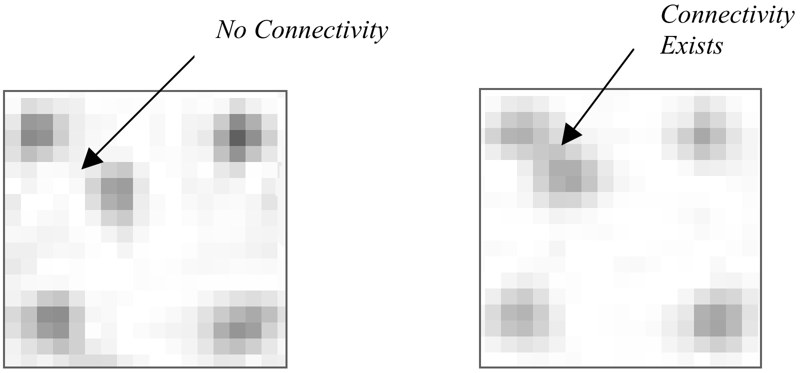
Primary Dot Position Modulation: As the same background image quality as well as symbol pattern are used, but the image is printed using the device offering resolution 1200 dpi. Now each dot can be represented by a 2 *x* 2 dots size square dot. As shown in Figure 6.6 that at 600 dpi *the minimum diagonal-distance* between the primary dot and its nearest neighboring reference dot is one dot. However, at 1200 dpi this *minimum diagonal distance* is reduced 50 %, as it is shown in Figure 6.6(b).


Dot consisting of single dot
Two Dots Diagonal Separation
One Dot Diagonal Separation
Dot consisting of four sub dots

(a) 600 dpi (b) 1200 dpi

Figure 6.6: Illustration of the size and diagonal-distance between the reference and primary dots for two *Symbol Patterns*: (a) Symbol Pattern is used at 600 dpi (b) at 1200 dpi diagonal-distance is decreased one half while dots size is kept same.

This change in diagonal distance is made by keeping in mind that when two dots, separated diagonally by one dot, are printed, it would provide more robustness against the errors due to the positional inaccuracy as well as unprinted dots. This is due to the fact that now the possibility that a primary dot is printed at critical region is further decreased, as the distance between the critical point and primary dot is increased 50%. Another factor contributing in improved performance is the fact that now there is much lower possibility that an isolated black dot is not printed. This is due to the fact that when two dots separated diagonally by only one dot are printed at 1200 dpi, then either primary dot is printed or at least some slightest hint (noise) is made (due to 50 % less distance between the primary and reference dots), which results in very slight connectivity as illustrated in Figure 6.7. And this slight connectivity can be utilized in information decoding process (e.g. while developing a filter for noise elimination).



(a) Unmodulated SP (b) Modulated SP

Figure 6.7: An illustration of *connectivity* after printing and scanning process for the symbol patterns (SP) shown in Figure 6.6.

This *slight connectivity* is attributed to the physical dot gain effects (i.e. error or inaccuracy due to the inability of printing device to precisely transfer the toner while making the primary and reference dots, separated by very small *diagonal* distance). The connectivity might also be resulting from heating and pressing process when toner is being fixed permanently to the paper surface.

Dot Amplitude Modulation

As mentioned above that at 1200 dpi a dot printed at 600 dpi is represented by 4 dots, which has another advantage as well that it allows to vary (with 25% step size) size of primary dot during data encoding process and this process is called as *Dot Amplitude Modulation* (DAM). The DAM may be used to improve the performance of relatively poor quality printing devices (e.g. old devices offering 1200 dpi resolution, not able to print isolated dots) by varying the size (amplitude) of the primary dot so that it results in a minimum error. Although it is not implemented yet, but it is expected that it would provide further improvement for the devices mentioned above (relatively poor quality printing devices).

Data-Reading Algorithm

The data-reading algorithm proceeds as follows:

1. As before printed CBGI is scanned at sufficiently higher resolution.
2. The position of each of the reference dots is estimated using three different filters known as Filter-1, Filter-2 and Filter-3 to be discussed in the following sections. It is *mentionable* that in the present scenario the *reference dots* are noisier and require more sophisticated techniques to correctly identify their central points.

   2.1) The first filter identifies only the isolated reference dots.

   2.2) The second filter identifies the reference dots, which have been influenced from the neighboring information carrying dots (number of such dots vary from one up to four) and results in the noisy reference dots.

   2.3) The third filter checks as well as corrects if there is an error in the estimated position of any of the reference dots, estimated using the previous filters.
3. Using Filter-4, identify and eliminate noise in the possible region where information might have been encoded.
4. Recover the encoded information by identifying the location of the primary dot and measuring its distance from each of the neighboring reference dots.
5. Steps 1-4 are applied repeatedly until all the data has been recovered.

In the following each of the above filters is described.

Filter 2.1. Recognition of Isolated Reference Dots

It is to be mentioned that this filter is not same as the one described previously due to the fact it has to work in noisier environment, although the objective of both filters is same.

The filter operation can be described as follows.

Step-1. First reference point at upper-left corner is identified and used as initial point.

Step-2. Selects a region of fixed width and height around the initial point found in step-1 and finds global minimum within that region for a given threshold level.

Step-3. Computes the width and height of the region for another threshold level, which is different from the threshold level used in step-2.

Step-4. If the width and height values are within the threshold level (third threshold level), then the coordinates of the global minimum value are considered *only as a candidate* single isolated reference dot.

Step-5. A fixed value is added to the coordinates of *global minimum* found in step-5 and these new coordinates are used as a starting point used in step-1 to identify the next isolated reference dot.

Step-6. Steps 2-5 are repeated for the whole image.

Filter-2.2: Recognition of Non-Isolated Reference Dots

When a given reference dot is surrounded by one or more primary dots, then from a minor to severe amount of noise is added to the reference dot and this noise restricts the possibility to use filter-1 to recognize these noisy reference dots. The objective of this filter is to identify such reference dots and its operation can be described as:

Step-1. Starts with the same initial point, which is used by Filter-1, which is responsible for recognizing the central coordinates of all isolated reference dots.

Step-2. Selects a region of given length and width around the given center points. Finds the global minimum value within that region and considers its coordinates as central point. Next it selects a sub-region within the previous region and looks for the *global minimum* within the region under consideration. If (the coordinates of the both global minima are same) minimum value found is unique in the region then this point is again considered only as *a candidate reference point.*

Step-3. A fixed step-size value is added at the coordinates found in step-2 and these new coordinates are used as a starting point for the next possible candidate. Then step-2 is repeated.

Filter-2.3: Error Detection and Correction in the Reference Dots Positions

This filter checks if there has been an error in any of the positions (middle points) of the reference dots, which are detected using Filters 1-2. This type of error is due to the slight shift in one isolated dot from its actual position and this slight error is *usually* transferred to the subsequent reference dot positions and ultimately results in completely wrong center points for the isolated reference points. The possibility whether to integrate the function of this filter in Filter-1 and Filter-2 and to evaluate its performance, remains to be checked. The filter operation can be described as follows:

Step-1. The recognized position of each of the reference dots is compared with the average value of certain number of neighboring dots.

Step-2. If the difference between the position of reference dot under consideration and the average of the neighborhood reference dots positions is greater than a threshold value, then the neighborhood average is used as starting point and filters 1-2 are applied sequentially.

Step-3. Once an error is detected in steps 1 and 2, then all reference dot positions in that row are considered as doubtful and are recomputed using step-2.

Filter-2.4: Noise Elimination from the Information Encoding Region and Information Recovery

The purpose of this filter is to eliminate noise in the region in which information could have been encoded before trying to detect the position of a primary dot, which has been used for information encoding. This noise can be attributed to various sources such as printing as well as scanning process. During printing process as mentioned before it is mainly caused by toner spreading on the paper surface and might be contributed from each and/or all of the following: toner transfer, pressing and heating processes. The noise may arise from the stains or dust on the paper or scanner surface as well. The filter operation can be described as follows.

Step-1. Start with the central coordinates of the first reference dot.

Step-2. By considering the four reference dots, which are surrounding the information encoding primary dot, a central point is estimated.

Step-3. Fixed region is selected around this central point and within that region specific characteristics for the primary dot are searched for. Initially, procedure starts with the idea that minimum pixel value within the region is selected as candidate primary dot.

Step-4. This candidate is checked for the noise, i.e. is it noise or the actual primary dot. The criteria used to check whether it is noise or the actual dot is that its connectivity is checked with the neighboring reference points. This means that it is checked does this dot (cluster of grayscale pixels) connects to any of the neighboring reference dots and if so what its minimum distance. If it does connect to one of the neighboring reference dots and the minimum distance lies in certain range, then it is considered as primary dot. Otherwise it is considered as noise and above procedure is repeated by considering next isolated dot found in step-4 as a possible candidate.

Step-5. Once the primary dot has been found then its minimum distance from all of its neighboring reference dots is found and with respect to the closet reference dot the information is decoded. The above procedure is repeated for the reference points and the information is decoded.

Results and Discussion

In this phase of experiments HP LaserJet 4100 printer offering 1200 dpi resolution is considered. The same background image as before is used at least from visual quality point of view, however, now the image is modified as follows. The image is transformed into 1200 dpi by representing each dot at 600 dpi by 4 dots at 1200 dpi. At 1200 dpi the minimum distance between the primary and the reference dots is *changed to one dot* (half of the diagonal distance at 600 dpi) with the aim that it results in minor connectivity between the reference and the primary dots, which is helpful for noise characterization and elimination. Next, the 700K bits data is encoded into the background image and multiple copies of the image are printed. The results of the data recovery after PS process are given in Table 6.2. As it can be observed that improvement in the performance is visible and the maximum number of errors encountered is not very significant.

Table 6.2: Number of errors encountered in data recovery process using novel data encoding technique in grayscale background images.

Experiment No.	No. of errors	Experiment No.	No. of errors
1	15	6	21
2	20	7	8
3	18	8	8
4	17	9	14
5	17	**Average**	**15.33**

By comparing the new results with the existing work it can be seen that the new technique not only provides higher data encoding capacity but it also results in lower error rate as compared with [SMS03] in which 90 errors are encountered for 98,568 data encoding symbols. While considering a full A-4 page with printable area measuring 4629 x 6585 at 600 dpi, it results in 860K symbols or 1720K bits of information as compared with the 95.5 K bits from Suzaki et al. It is to be pointed out that while considering *error rate*, in the existing work the error rate is given for symbol patterns, when only one type of patterns are encoded and printed in the whole image. For instance an image with 49K symbols of same type is printed and the decision error rate is given for the case when the symbol is not identified correctly. In this research the real information is encoded into the background image and the number of errors are reported in Table 6.2.

6.6 Countermeasures Against Unavoidable Distortions

As in all practical applications of PS process zero bit error in the decoded data is required. And this is in contrast to the scenarios considered so far in this chapter, where it is found that certain amount of errors is unavoidable, especially while considering state of the art desktop publishing technologies. The causes of such errors have been discussed already. In this section, the possibility to overcome such errors is focused upon, while considering even stronger case (A-4 size CBGI). It is to be pointed out that usually the performance of the printing devices gets poor while considering A-4 size CBGI as compared with the images discussed so far and considered in [SMS03].

Now to count for unavoidable errors in this research, being inspired by others, BCH error correction coding (ECC) technique is used. However, the payload used for ECC is very small as compared with the one suggested in [SMS03] and yet the net capacity available for data encoding is still much higher. Furthermore, to maximize the capacity, a Data Scrambling (DS) technique is used, to keep the payload due ECC at its minimum level. While considering A-4 size CBGI with superposed text image, Data Encoding Technique is given, which does not use ECC to count for the errors caused by the character overlapping, as suggested in [SMS03]. In the following subsections first Data Encoding technique is described, which is followed by the Data Scrambling technique for CBGI with superposed text. Finally, the experimental results are provided while considering A-4 size CBGI with and without superposed text, and a discussion on the results is given as well.

6.6.1 Data Encoding in CBGI With Superposed Text

As the CBGI under consideration usually will be superposed by the text image in the final applications, so this scenario is investigated for the novel technique as well. It is to be pointed out that in existing technique [SMS03] it is suggested to use ECC with higher payload to overcome the errors in the data encoding symbols that are overlapped by the superposed text.

In this research only those areas, which are not overlapped by the superposed text, are used for data encoding purpose. And this choice is governed by the fact that the net capacity for novel technique while considering only those regions, which are not overlapped by the characters, is much higher as compared with the scenario that the data is encoded at each location and then errors caused by the character overlapping are eliminated using ECC with higher payloads. In the following a *general* (i.e. enables to encode data in certain areas that can be overlapped by superposed text) capacity computation technique, given in this work is described.

Let ***X*** be a matrix of size *I* by *J, where* each element of ***X*** represents an information encoding symbol. After text image superposition an element of ***X*** is defined as:

$$x_{i,j} = \begin{cases} 1 & if \sum_{\varepsilon_1=1}^{\omega}\sum_{\varepsilon_2=1}^{\omega} x'_{\varepsilon_1,\varepsilon_2} \neq 0 \\ 0 & \sum_{\varepsilon_1=1}^{\omega}\sum_{\varepsilon_2=1}^{\omega} x'_{\varepsilon_1,\varepsilon_2} = 0 \end{cases}$$

where $x'_{\varepsilon_1,\varepsilon_2}$ is sub-element (single dot) within the information encoding symbol and ω is size of the information encoding symbol. It is to be noted that $x_{i,j} = 1$, means that there is an overlapping on a given symbol due to the superposed text image.

Then, the capacity Y_c can be found as follows:

$$Y_c = \sum_{i=1}^{I} J \cdot \alpha_i + \sum_{i=1}^{I} \sum_{j=1}^{J} \beta_i \cdot \gamma_j \tag{6.2}$$

where $\alpha_i = \begin{cases} 1 & if \sum_{j=1}^{J} x_{i,j} \le \sigma \\ 0 & \sum_{j=1}^{J} x_{i,j} > \sigma \end{cases}$, $\beta_i = \begin{cases} 1 & if \sum_{j=1}^{J} x_{i,j} > \sigma \\ 0 & \sum_{j=1}^{J} x_{i,j} \le \sigma \end{cases}$

and $\gamma_j = \begin{cases} 1 & if \sum_{i=}^{I} x_{i,j} = 0 \\ 0 & \sum_{i=1}^{I} x_{i,j} \ne 0 \end{cases}$

In eq. (6.2) first summation increments by the factor *J* whenever the constraint given by α_i is satisfied (i.e. $\alpha_i = 1$). Whereas the second summation increments by one whenever $\beta_i \cdot \gamma_j = 1$.

By varying the value of parameter, σ, the capacity can be controlled and this is possible due to the fact that for *each text line* of the superposed image, the top as well as bottom 4 rows of information encoding symbols have only small number of symbols which are overlapped by the text characters. And the errors caused by the overlapping characters in these regions can be tackled using either of the two methods: 1) these rows can be encoded separately using maximum run-length encoding technique, which would identify the sequence of connected locations where information can be encoded, and 2) other possibility is that information being encoded in the area under consideration is encoded with ECC with slightly higher error correction capability. It is noteworthy that using top and bottom four rows (i.e. $\sigma = \lambda$, λ is a fixed constant, means how many overlappings are allowed in a given row) corresponding to each line of the superposed text image, an additional 200-300 K bits of information can be encoded, which is a significant gain in capacity. In this research parameter σ takes the value zero.

Finally, those regions, which are not used for information encoding, are encoded separately, and these regions are identified first from the printed and scanned (PS) image and are ignored while recovering original message. Due to the fact that this information is responsible of synchronization recovery and if synchronization is lost, then the remaining operations will be of no usage. This information is encoded using ECC with higher error correction capability.

6.6.2 Data Scrambling

As certain amount of errors, which varies from printer to printer and for different technologies as well, is unavoidable during the data recovery from PS process, this fact forces to use error correction coding ECC techniques, which allow to recover the original data without corruption. However, ECC techniques has the drawback that it adds significantly higher payload for error correction and some times this payload even increases than the message payload. This limitation of ECC techniques can up to certain extent be reduced by dispersing the encoded data over a larger/entire area available to encode the message. And encouraged by this fact it is decided to use *Data Scrambling* (DS) technique in combination with ECC to keep the capacity maximum. Due to the fact that the DS technique used in this research, is not taken from the existing work, is described in the following.

Let $X = [x_1, x_2, ..., x_N]$ denote the vector of size N of symbolic values being encoded in CBGI and $Y = [y_1, y_2, ..., y_N]$ is a *set* of random values with each element y_λ taking random value from distribution Φ and lies within a fixed range 1 to N. And the vector ***Y*** is generated as follows:

$$Y = [\,y_i \,|\, b_i \neq 1,\, b_i = 1,\;\; y_i \in \Phi, \forall\, i = 1,2\cdots N\,] \qquad (6.3)$$

where ***B*** is initially a null vector of size N, which successively turns into a unit vector. In (6.3) an element b_i of ***B*** changes to one when its corresponding element of y_i is occurred.

The scrambling of ***X*** over ***Y*** can be described as:

$$Z = \Im(X,Y) = [x_{y_i}\;\; \forall\, x_i \in X,\;\; y_i \in Y \; and \; i = 1.2...N]. \qquad (6.4)$$

The operator, $\Im$, changes the index i of element x_i with the corresponding value of y_i at index *i*.

Next the vector $\mathbf{Z}$ is transformed into the matrix $\mathbf{Z}'$ of size *I* by *J* and an element of $\mathbf{Z}$ with index, $i = \lambda$, is transformed to the pair of coordinates (i', j') as follows:

$$i' = \lambdabar(\lambda, J) + 1\,,$$

where the operator $\lambdabar$ performs integer division, returning the remainder value and j' is the quotient of this integer division.

For reverse scrambling all of the operations are performed in reverse order.

It is to be pointed out that although the above DS technique works well, however, while considering an A-4 size CBGI with 850,000 symbols to be dispersed, the computational time for the DS process gets higher and it is of significant value when dispersion process enters in final phase. This increase in computational time is associated with the fact that as the DD process approaches towards the end, collisions are encountered before finding a position where the new scrambled symbol can be placed. However, this computational time can be decreased significantly by ignoring the final few thousand positions for data dispersion. Finally, while selecting ECC, it could be helpful to consider in advance the maximum number of errors that are encountered when the data has already been dispersed.

6.6.3 Experimental Results: CBGI With And Without Superposed Text

In first set of experiments an A-4 size CBGI without superposed text image, shown in Figure 6.8, is considered. The quality of printed image shown in Figure 6.8 is degraded due to the down-sampling operation performed during size reduction, which consequently destroy binary data encoding pattern and results in noisy rather smooth background image. The actual quality of this image can be seen from Figure D-1 shown in appendix-D. The data being encoded is generated using the MATLAB routines. Three different types of printers are considered for experimental purpose. To achieve the zero bit error rate data is encoded using BCH ECC technique and then dispersed all over the CBGI of size 6675 by 4649 dots at 600 dpi. The capacity for user data with zero bit error rate (BER) along with used BCH parameters, are given in Table 6.3.

It can be seen that the capacity varies between 1508.1-1626.9 K bit, which is sufficient to encode a word document file having 49-53 pages of text. Even the higher number of pages 72-77 with text contents can be encoded when only text information rather than ".doc" file is encoded. This capacity is more than 16 times higher than [SMS03]. The error correction capability of BCH in each experiment is determined by the underlying printing device, whereas the codeword length is selected based on the processing time to encode message. Although, BCH with codeword length 1011 or 2047 could have been better choice; however, in former case message encoding time is found very high whereas in the latter case the MATLAB routines does not work at all. Concerning the data scrambling, it is found that it improves the capacity significantly and it is found that for HP 8000 printer, in some cases BCH (511, 313, 22) instead of BCH (511,455, 6) would be needed if the data has not been dispersed. The usage of BCH in experiment 2 and 3 with higher ECC payload is intended to count the errors caused mainly by the unprinted dots or stains on the scanner surface. The data-reading time, excluding BCH decoding and data de-scrambling processing time, is found 15 minutes, which is quite high.

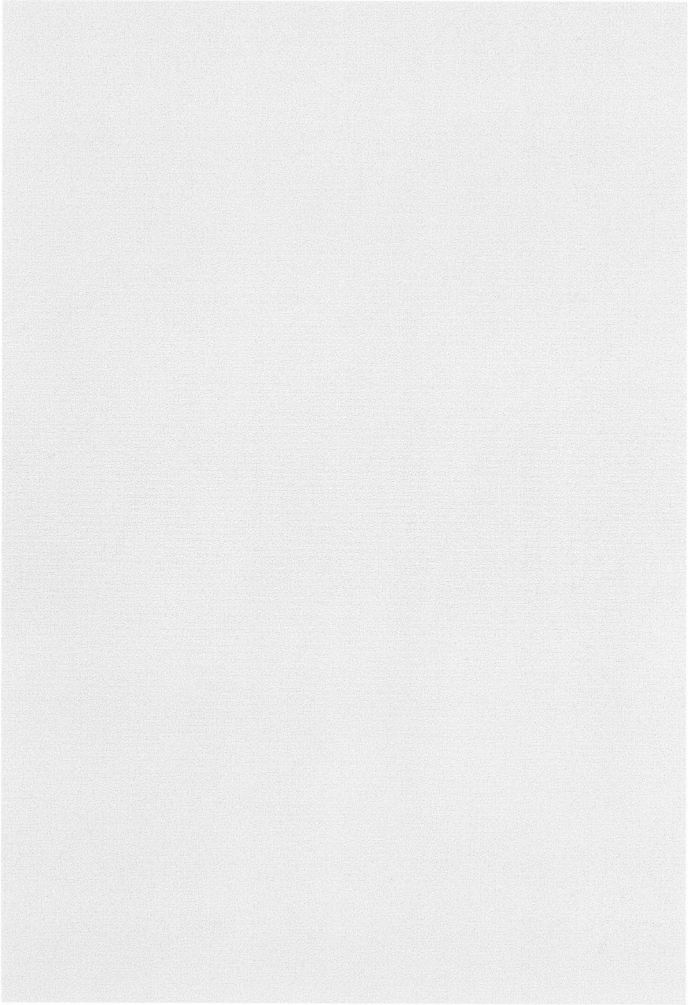


Figure 6.8: An A-4 size constant background grayscale image with 1709 K bits of embedded data.

Table 6.3: Data recovery results for the encoded data in the background image ***without*** superposed text.

Exp. No.	Device	ECC	User payload K Bits	Capacity-1	Capacity-2
1	HP 4100	BCH (511,493, 2)	1626.9	53	77
2	HP 8150	BCH (511,455,6)	1508.1	49	72
3	HP 8000	BCH (511,455,6)	1508.1	49	72

Capacity-1: File-size for the number of text pages in word document file (i.e. a .doc file).

Capacity-2: File-size for the number of pages with each page having 2,623 characters (8 bits per char), excluding space character.

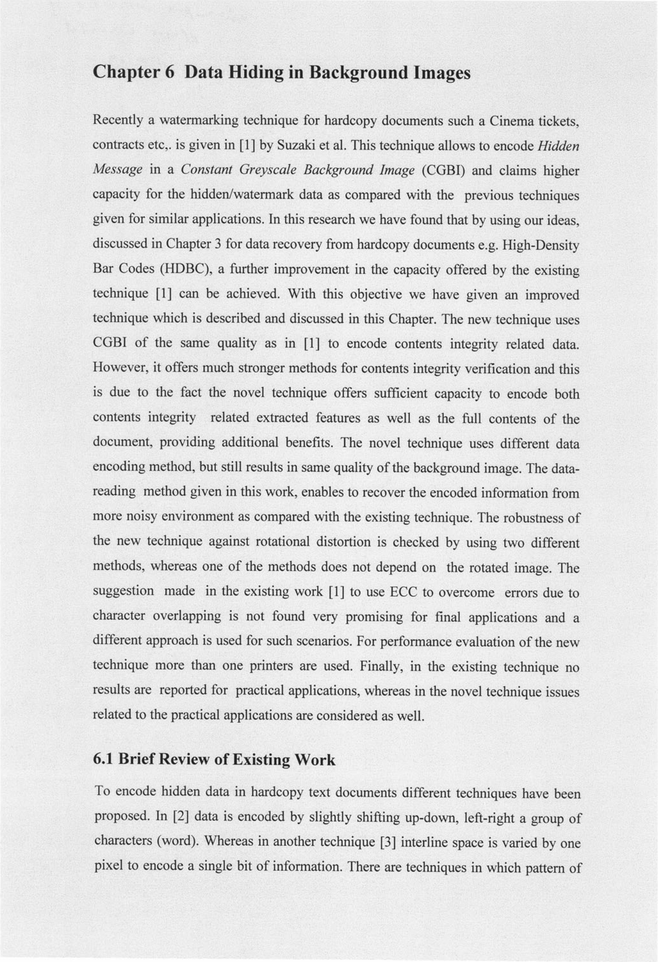
In second set of experiments data is encoded in an A-4 size CBGI in the presence of superposed text, shown in Figure 6.9. Due to the same reason as for Figure 6.8, the quality of Figure 6.9 is not the actual one and true quality can be observed from Figure D-2 given in appendix-D. For this purpose three different printers are considered and the results are given in Table 6.4. As it can be seen that now capacity varies between 909.36-1068.33 K bits, which is sufficient to encode a word document file having 27-33 pages of text. The higher number of pages 43-50 with text contents can be encoded when only text information rather doc file is considered. The variation in capacity is again associated with the printing device under consideration. As mentioned earlier that a further gain (i.e. a few hundred K bits) in capacity can be achieved by considering all those rows in which there are *relatively* minor number of errors caused by character overlapping, unlike the present scenario in which rows with all non-overlapping symbols are considered only. It is to be pointed out that this gain in capacity is much higher as compared with the capacity offered by the existing work [SMS03] and this gain in capacity can eliminate the need for any feature extraction algorithm to verify the contents and allows one-to-one contents verification. The higher capacity gives a direction to investigate novel applications for the hardcopy documents. In this scenario data-reading time, excluding BCH decoding and data de-scrambling processing time, is found 10 minutes, which is less than the previous scenario; however, it is still quite high. The lower data-reading time in this case is due to the fact that overlapping regions are not considered in data-reading process, as these regions have been taken into account during the data encoded process (discussed before).

Table 6.4: Data recovery results for the encoded data in the background image *with* superposed text.

Exp. No.	Device	ECC	User payload K Bits	Capacity-1	Capacity-2
1	HP 4100	BCH (511,493, 2)	1068.33	33	50
2	HP 8150	BCH (511,455,6)	1009.36	31	48
3	HP 8000	BCH (511,455,6)	> 909.36	27	43

Capacity-1: File-size for the number of text pages in word document (i.e. a .doc file).

Capacity-2: File-size for the number of pages with each page having 2,623 characters (8 bits per char), excluding space character



Chapter 6 Data Hiding in Background Images

Recently a watermarking technique for hardcopy documents such a Cinema tickets, contracts etc,. is given in [1] by Suzaki et al. This technique allows to encode *Hidden Message* in a *Constant Greyscale Background Image* (CGBI) and claims higher capacity for the hidden/watermark data as compared with the previous techniques given for similar applications. In this research we have found that by using our ideas, discussed in Chapter 3 for data recovery from hardcopy documents e.g. High-Density Bar Codes (HDBC), a further improvement in the capacity offered by the existing technique [1] can be achieved. With this objective we have given an improved technique which is described and discussed in this Chapter. The new technique uses CGBI of the same quality as in [1] to encode contents integrity related data. However, it offers much stronger methods for contents integrity verification and this is due to the fact the novel technique offers sufficient capacity to encode both contents integrity related extracted features as well as the full contents of the document, providing additional benefits. The novel technique uses different data encoding method, but still results in same quality of the background image. The data-reading method given in this work, enables to recover the encoded information from more noisy environment as compared with the existing technique. The robustness of the new technique against rotational distortion is checked by using two different methods, whereas one of the methods does not depend on the rotated image. The suggestion made in the existing work [1] to use ECC to overcome errors due to character overlapping is not found very promising for final applications and a different approach is used for such scenarios. For performance evaluation of the new technique more than one printers are used. Finally, in the existing technique no results are reported for practical applications, whereas in the novel technique issues related to the practical applications are considered as well.

6.1 Brief Review of Existing Work

To encode hidden data in hardcopy text documents different techniques have been proposed. In [2] data is encoded by slightly shifting up-down, left-right a group of characters (word). Whereas in another technique [3] interline space is varied by one pixel to encode a single bit of information. There are techniques in which pattern of

Figure 6.9: An A-4 size constant background grayscale image with superposed text image, containing 1111.52 K bits of embedded data.

In both set of experiments (i.e. CBGI with and without superposed text), in experiment 3 the errors are mainly caused by the unprinted dots in a certain region, and such behavior is, especially, more *evident* when considering A-4 size CBGI and possible causes of such behavior have been discussed earlier. In order to overcome such regions data is scrambled, otherwise BCH code with much higher error correction payload would be needed. For the HP 8150 printer the errors are mainly due to the inaccuracy in position of the printed dots, i.e. the primary dots are printed slightly bigger and cause interference in the neighborhood as well. Finally, the HP 4100 printer (experiment-1) in both sets of experiments, Table 6.3-6.4, performs better due to its ability to print precisely primary dots and the errors are still due to unprinted dots, however, the number of such dots is not significant. The fact that many copies of the foreground text are encoded in CBGI can be utilized to increase the robustness against wear-and-tear noise as well as to decrease data-reading time; issues not yet addressed.

6.7 Robustness Against Skewing Distortions

As a one of the key geometrical distortion encountered during PS process, it is necessary to consider how a new technique performs against this distortion. While considering robustness against the skewing distortions two different approaches are considered to investigate such effects. According to the first approach, image being scanned is skewed manually during scanning process, to investigate the effects of intentional or unintentional distortion. The second approach takes the scanned image without skewing distortion and adds skewing distortion using some image processing software. As skewing/deskewing is a non-linear transformation so when image is skewed digitally and then deskewed afterwards, it suffers from the information loss twice higher as compared with conventional method. Now, if the encoded data can be recovered successfully, then it can be considered that technique is robust against the skewing distortions as well. The second method is intended to eliminate the need for practically scanning the image to check its robustness against the skewing distortions. For experimental purpose images are skewed at different skewing angles and the results of data recovery for both techniques are given in Table 6.5. As it can be seen that regardless the fact how much and in which direction the image is rotated, data is recovered successfully. The small number of errors can easily be combated using ECC. It is to be mentioned that the CBGI used here measure 4200 by 3000 dots (used in in Table 6.1) and the choice is driven by the fact an A-4 size image do not fit on scanner bed for the skewing angles considered here.

Table 6.5: Robustness of data-reading technique against skewing distortion.

Exp. No.	Errors*	Rotation (deg)	Errors
1	15	+4	21
2	15	12.5	24
3	20	- 3.5	7
4	18	-20	13
5	17	-16	12
6	17	-21	13
Average	**17.4**		**15.0**

* Errors with unintentional rotation

In contrast to HD-DataStripe where RM-pattern surrounding the information carrying area is utilized to combat the distortions caused by the skewing effects, in present scenario higher robustness is attributed to the reference dot pattern that is dispersed uniformly over the entire CBGI (i.e. near to the each information carrying symbol). Furthermore, it is observed that although in present scenario information from CBGI is recovered successfully against the skewing noise generated by two different ways discussed above; however, both approaches do not show similar behavior when applied to HD-DataStripe. For HD-DataStripe 20 degrees skewing distortion introduced using second approach, results in 50 more errors, whereas the distortion introduced during scanning process results in complete synchronization loss, resulting in very large number of errors. This leads to conclude that digital approach cannot simulate the skewing distortion effects in general.

6.8 Alteration Detection Method

While considering applications of above data hiding in background image, the new technique allows to encode many copies of the superposed text image (a full A-4 size text page) in the background, eliminating the need for any feature extraction algorithm. However, as the *extracted features* might be useful for some applications in which processing time is critical or one-to-one contents integrity verification might not be necessary. By this in mind, a general purpose alteration detection algorithm, which means that features set being encoded in the CGBI, have both types of data: 1) extracted features and 2) the full contents of the page, is described in the following:

1. Select the different types of input features to be encoded:
    - Full contents of the superposed text for one-to-one contents integrity verification.
    - Selected features of the text message: first character of each word of foreground text or set of characters resulting after sampling the superposed text image using any suitable sampling process that is reversible.
2. Encode the contents integrity related information found in step-1 using appropriate ECC.
3. Superpose the foreground text image to the background image.
4. Encode the contents from step-2 into the background grayscale image at the locations obtained using capacity computation technique.

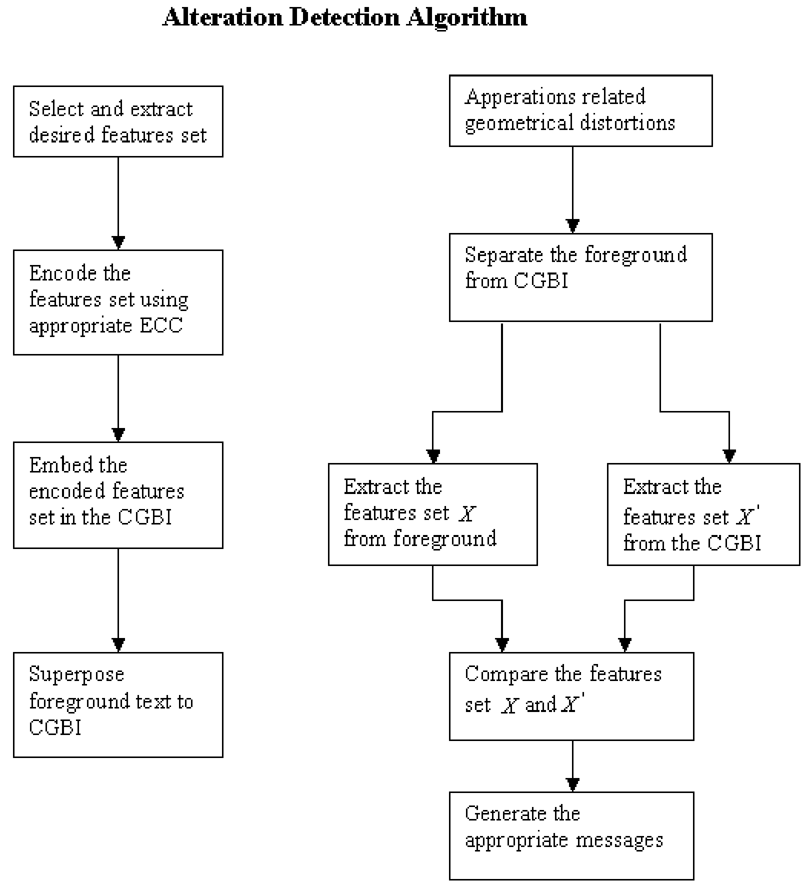
The above procedure is shown schematically in Figure 6.10(a).

The data decoding and contents integrity verification process proceeds as follows:

1. Apply the appropriate image processing operations such as re-rotation etc. on the scanned image.
2. Applying the appropriate image processing operations on the scanned image and extract the desired features set defined for contents verification purpose from the *superposed text image*.
3. Decode the features set from the CBGI as well.
4. Compare the relevant features.

5. Generate the appropriate messages based on the information from step-4 for each category of the features. For example, a generated message could be that the full contents of the text message are shown on the screen for visual verification with the modified parts being underlined.

The above steps are shown schematically in Figure 6.10(b).


Alteration Detection Algorithm
Select and extract desired features set
Encode the features set using appropriate ECC
Embed the encoded features set in the CGBI
Superpose foreground text to CGBI
Apperations related geometrical distortions
Separate the foreground from CGBI
Extract the features set X from foreground
Extract the features set X' from the CGBI
Compare the features set X and X'
Generate the appropriate messages

(a) Encoding Process (b) Decoding Process

Figure 6.10: A schematic diagram showing different stages encountered during alteration detection process.

6.9 Cryptoglyph Versus Proposed Technology

As the proposed document authentication technique uses data encoding in very smooth superposed background image (CBGI), it could be advantageous to refer here the cryptoglyphs technology in which *almost* invisible cryptoglyhs mark is used for document/product authentication and counterfeiting detection. A general comparison of both techniques is given Table 6.6.

Table 6.6: A comparison of the Cryptoglyphs and proposed superposed CBGI. * Without ECC payload

	CryptoGlyphs™	**Superposed CBGI**
Size	Flexible (usually 2 x 2 cm)	Flexible (usually covers full background)
Visibility	No	No
Capacity	Small (~ 128 bits)	High (~ 2.5* Kbytes PSI)
Synchronization Marks	No	Yes
Counterfeiting Resistance	Passive attacks (yes) Active attacks (?)	Passive attacks (yes) Active attacks (no)
Printing Technology	Laser, Inkjet with 600 DPI	Laser with ≥ 600 DPI
Scanning Technology	Scanners, digital cameras and mobile cameras with 600 PPI	Scanners with ≥ 1200 PPI
Applications	Legal document authentication, brands protection, bank checks etc.	Invisible data stripe, one-to-one legal document authentication, authentication of languages with complex structures restricting MAC computation etc.

Important point here in context of this research is that in cryptoglyphs technology it is mentioned that the printing devices with resolution 600 dpi are needed to print cryphtotglyph mark. However, in this research it is shown that the invisible tiny printed dots measuring 1/600 of an inch have sufficient energy (signal strength) that can be utilized for original signal recovery with high accuracy, given that digitization is done at sufficient higher over-sampling rate and other suitable measures by taking into account the findings of this research (chapter 3 & 6) are taken as well. This fact consequently raises questions concerning the strength of cryptoglyphs as an ant-counterfeiting technology against the active attacks rather than passive attacks usually considered by anti-counterfeiting technologies. A detailed discussion about the potential threats to cryptoglyphs technology is given in appendix-E on page 179. It is to be pointed out that unlike cryptglyphs technology DataGlyphs technology has much higher signal strength and consequently cannot be used for copy detection and is irrelevant to the present discussion.

Chapter 7
Conclusions and Future Work

7.1 Conclusions

In this research high capacity analog channels: 1) HD-DataStripe, 2) data-hiding in printed grayscale images (watermarking) and 3) superposed constant background grayscale image (CBGI) and their applications in smart documents are investigated. On way to develop high capacity analog channels noise encountered from printing and scanning (PS) process is investigated with the objective to recover the digital information encoded at nearly *maximum* channel utilization. By utilizing noise behavior counter measures against the noise are taken accordingly and data-reading techniques are given. The main contributions of this research are summarized in the following:

7.1.1 Novel HD-DataStripe Technology for Smart ID Documents

A novel data-reading technique, which allows recovering data from HD-DataStripe, is given. On way to develop data-reading technique, which is intended to recover data encoded at 300 dpi, as a countermeasure against the unavoidable geometrical distortions, RM-pattern is chosen in such a way that it results in accurate sampling points (*a necessary condition* for reliable data recovery at higher data encoding rate). For more sophisticated distortions caused by the physical dot gain effects (intersymbol interference), the countermeasures such as application of sampling theorem, adaptive binarization and post-data processing, each one of these providing *only a necessary condition for reliable data recovery*, are given. Finally, combining the various filters corresponding to these countermeasures, a novel Data-Reading technique for HD-DataStripe, is given.

The HD-DataStripe is a printed binary image similar to the conventional 2-D barcodes (e.g. PDF417), but it offers much higher data storage capacity and is intended for new machine-readable identity verification documents (e.g. visas, passports, ID cards, driving licenses, educational certificates, entertainment tickets etc.). The capacity offered by the HD-DataStripe is sufficient to store high quality biometrics characteristics rather than extracted templates, in addition to the conventional bearer related data contained in an ID card. It eliminates the need for central database systems (except for backup records) and other expensive storage media: magnetic stripes, IC chips, optical stripes etc. In addition, the novel technique results in superior performance than existing work [FuA02, DP03, VVKP05, Wan01, WuL04], which deals with the data reading from printed media. For experimental evaluation different printing and scanning devices are considered using both simulated and real-data. Robustness of data-reading technique against skewing distortion and simulated dust-and-scratches noise is also considered.

As HD-DataStripe allows encoding multiple high quality biometrics characteristics, consequently the smart identity verification documents, using HD-DataStripe, would result in *improved identity verification process* in terms of FRR and FAR at lower cost as compared with the rival technologies [CBN, DStr, PVT04]. The security of the biometric identity verification system against spoof attacks would be enhanced by implementing multimodal biometrics characteristics and using randomly chosen characteristics in verification process. The verification process would also be secure against the potential threats: access to central database failure, cyber attacks on the central database system, privacy of the biometrics data etc., attributed to central database systems.

Some other factors that contribute to system security include: contents confidentiality, integrity, authenticity, non-repudiation and key management for data encoded in HD-DataStripe and on abstract level it is shown how these issues can be tackled. Contents confidentiality can pose threats only to biometric data (e.g. identity theft, revealing sensitive health information) and can be tackled using biometric encryption [SSG+], biometric cryptosystems [UPP+04] and transformed biometric templates (Ref. [15] in [JRU05]). Contents integrity, authenticity and key management issues can be addressed by using secure and trusted PKI system and requires digital signatures (DS) and public-key to be encoded in HD-DataStripe. Repudiation threat can be addressed using multimodal biometrics systems.

7.1.2 HD-DataStripe as a Copy Detection Technology

The copy detection technique is based on the principle that each time the information (copy detection pattern) passes through the channel (PS process) at *higher transmission rate*, there does occur an information loss and the amount of information loss in recovered information (data) from the scanned image is used to distinguish between the original and copy document. While considering application of novel data-reading technique for copy detection, a small size HD-DataStripe consisting of a pseudorandom binary sequence generated with known key is used as a copy detection pattern (CDP) and a threshold level requiring above 99% correct information recovery is used to characterize the CDP as the original. The proposed copy detection technique offers the opportunity to encode the product related information in CDP, resulting in more efficient product handling.

The novel technique is more resistant to copying attacks as compared with the existing copy detection technology [Pic04], which uses 50-60 % threshold level for copy detection at the same data-encoding rate as in this work. The existing technique is non-blind and requires the original CDP for copy detection, whereas the novel technique is blind. In [PVT04] three different technologies: copy detection, digital watermarking and PDF417 barcode are used to secure the contents of a Fraud-Proof identity card. In this context, HD-DataStripe having size of a conventional 2-D barcode can be used as three-in-one (multi-purpose) technology. The need for digital watermarking technology is eliminated by the fact that bearer portrait can be stored in HD-DataStripe due to its higher capacity. The novel technology as compared with cryptoglyph^{TM} technology [Cryp] offers much higher capacity and is robust against both active and passive counterfeiting attacks, whereas robustness of the rival technology against active counterfeiting attacks is questionable in the light of findings of this research. The potential threats to the cryptoglyph^{TM} technology arising from active counterfeiting attacks are discussed in this research. It is also found that the invisibility of cryptoglyphs technology cannot enhance its security against the counterfeiting attacks.

The security threats posed to copy detection technique are application dependent, for instance, entertainment tickets application is more prone to security threat as compared with bank checks. For entertainment tickets main threat encounters from contents confidentiality and once encrypted CDP is decrypted for counterfeiting detection, the original CDP can be copied from the compromised verifying device and used again as original CDP. However, this threat is also possible against other copy detection techniques [Cryp, Pic04] regardless of the technology being used and solution seems to be only in strong verifying devices. A countermeasure to reduce the effects of this threat is given in this research. On the other hand, contents confidentiality of CDP for bank checks application does not pose any security threat because in this case CDP (appropriate size HD-DataStripe) can be consisting of digital dynamic signatures template, one-time pad and critical information on the bank check. Given that all of these contents are encoded in encrypted form along with digital signatures and public-key from secure and trusted PKI system, bank check can ensure content integrity, authenticity, *non-repudiation* and key management issues, whereas confidentiality (availability of the original CDP) cannot pose any threat because nature of the contents does not allow using the CDP again.

7.1.3 Contents Integrity Verification of Hardcopy Documents

While considering contents integrity verification of hardcopy documents such as official letters, contracts etc., the existing technique [Zha04] uses digital signatures; however, this approach has limitations associated with the message digest generation algorithms and OCR performance. Many message digest generation algorithms considered very strong once, are vulnerable nowadays. Similarly, OCR performance in ideal case reaches up to 99% and to overcome this limitation of OCR technology some measures are given in [Zha04]. However, in present research it is found that the *given measures* have limitations, which can be exploited to launch data tampering attacks and possible attacks are discussed as well. In the existing work, resulting digital signatures are stored in a conventional 2-D barcode (PDF417) and the barcode image is printed using magnetic or fluorescent inks to secure the barcode against copying attack. It is also mentioned in [Zha04] that although digital signatures could be encoded in a background image using digital watermarking technique; however, watermarks are also vulnerable against photocopying attacks and consequently different media is used. In this context, a small size HD-DataStripe (see Figure 4.9) offers sufficient capacity to encode full contents of a page in encrypted form and makes it possible to verify the contents on *one-to-one* basis. Furthermore, it eliminates the need for magnetic and fluorescent inks due to its robustness against copying attack, is independent of the limitations attributed to OCR technology and message digest algorithms. Contents integrity, authenticity and key management issues can be addressed as discussed before using secure and trusted PKI system and encoding DS and public keys (needed to decrypt DS and other contents) in the seal.

7.1.4 Data Hiding in Printed Grayscale Images

As the printed grayscale images are obtained by the halftoning process, which converts grayscale image to binary image, in this research the potential benefits of the data-reading technique for HD-DataStripe (a binary image) are investigated for digital watermarking techniques. Here the objective is to develop a watermarking technique, which offers higher data hiding capacity as well as superior image quality as compared with existing work [FuA02, HeO00, Wan01]. It is to be mentioned that in general watermarking techniques working in frequency domain (e.g. [PVT04]), offer lower capacity (8-16) bytes; whereas the new watermarking technique, which works in spatial domain, offers *capacity* above 1Kbytes.

The *higher quality* of printed watermarked image is attributed to: 1) the higher printing resolution, and 2) better halftoning process. In existing techniques, images cannot be printed at more than 150 dpi and this constraint is imposed by the data-reading techniques. However, quality of the printed images improves significantly at higher resolutions and 300 dpi (used in present research) is the minimum resolution at which human eye cannot resolve the printed dots. Furthermore, halftone process also plays a significant role in image quality and in this research recently given iterative halftoning technique [Goo01] is used. The technique given in this research also works for the scenario (i.e. images having very high or very low mean graylevel) where given technique [HeO00] does not work.

The watermark reading process does not require any other knowledge except the public key used to generate pseudorandom locations for data hiding. The computational time for watermarking decoding process has similar behvior as for HD-DataStripe data-reading technique given for HD-DataStripe. Whereas the computational time for the data embedding process is not significant (in seconds) and computational associated with the halftoning process is not known as the test data used in this research are already halftoned.

The data hiding technique is robust against PS-process (DA/AD conversion) due to the data-reading technique given in chapter-3. The robustness against gamut mapping (grayscale to halftone transformation) is due to the data embedding in halftone image. The robustness against unavoidable errors from PS-poress and dust-and-scratches noise is addressed at abstract level in context of security aspects discussed below.

While considering security aspects of data hiding technique, here confidentiality does not seem to pose any threat. To address contents integrity, authenticity and key management problems, *on abstract level* a semi-fragile (robust against unavoidable errors from PS-process) technique, which ensures *probabilistic contents integrity* with low false reject rate (FRR) using digital signatures of the contents, is given. The technique enables automatic contents integrity verification. The public-key is embedded as watermark payload along with digital signatures in the host image. The higher data hiding capacity here allows developing more strong techniques. The higher channel capacity can be used to embed some biometric templates, in addition to the data related to semi-fragile watermarking technique. The higher data hiding capacity can be used by/for the other fragile-watermarking techniques [DFV01, Ditt01, DSF02], which not only ensure contents integrity but also locations of malicious content changes.

7.1.5 Data Hiding in Background Images

Here a data hiding technique with distinguishing characteristics: complete transparency and high data embedding capacity (two highly-desirable but conflicting requirements for analog media authentication), is given and is again targeted for hardcopy documents such as ID cards, cinema tickets, contracts, official letters etc. The data hiding technique uses the superposed constant background grayscale image (CBGI) as a channel for hidden communication. The higher capacity and transparency are attributed to the data encoding symbol that is used repeatedly to obtain superposed CBGI. The *visual quality* (transparency) of the printed superposed CBGI with hidden data can be considered similar to the grayscale image of constant value, printed using black and white printer. Furthermore, it is possible to get different gray levels for the CBGI. The *capacity* (Table 6.3 and 6.4 pp. 145-146) offered by the CBGI without error correction coding is 10 Kbits per square inch that is much higher as compared with the rival technologies [DataGlyphs, SuS03, Crypto] and a CBGI of A-4 size (measuring 4749 by 6685 pixels at 600 dpi) offers above 1700 Kbits. For practical scenario with BCH (511, 493, 2) for full-page foreground text, the resulting capacity is above 1068 Kbits that is sufficient to encode word document consisting 33 pages of text, where the capacity increases to above 1626 Kbits (word document with 53 pages of text) without superposed text. One of the key challenges encountered in the proposed technique is the noise encountered from PS-process for small-sized data encoding symbols and this is tackled by the blind data-reading technique, which requires the CBGI to be digitized at two times higher scanning resolution than the printing resolution. Data-reading time while considering A-4 size CBGI with and without superposed foreground text is 15 and 10 minutes respectively without taking into account the computational time for BCH decoding and descrambling process. Data-reading time for 2 by 2 inch CBGI (intended for ID-cards backgrounds) encoding 80Kbits data is found 60 sec. The higher data-reading time is due to the unoptimized code and its MATLAB implementation. The robustness of the data-reading technique against skewing distortion is also investigated. For experimental purpose laser printing devices with resolution 600 dpi or more are considered.

While considering security aspects, the data hiding technique would result in higher security due to the following factors. Contents integrity, authenticity and key management issues can be addressed using secured and trusted PKI system as discussed above. Here it is assumed that the private key is time stamp dependent or generated with suitable measures so that if second (false) DS is embedded then it can be figured out from the key, which one is authentic. Similarly, full-contents encoded in encrypted form using PKI system enable one-to-one visual contents integrity authentication, which is not possible with other techniques that use *selected features* for authentication due to the constraint from data hiding capacity, or difficulty arising from feature extraction techniques (e.g. OCR limitation etc.). The higher capacity enables to embed multiple watermarks without putting strong constraint on the payload (e.g. hologram watermarks [DSF02, FMF+02]). As multiple copies of foreground contents can be encoded in CBGI, watermarked digital contents in addition to the encrypted ones can be encoded as well.

7.2 Future Work

While considering paper as high capacity communication channel (e.g. HD-DataStripe), it is new area of research and there is a lot of potential for the future work. Before discussing new application areas, first the future work in the context of the applications considered in this research is discussed.

The computational time for the novel data-reading technique for HD-DataStripe used in smart ID-cards varies 3-4 minutes, which is quite high for the targeted applications and remains to be minimized. The higher computational-time is mainly contributed from the fact that the data-reading code is written in MATLAB, which is considered less efficient as compared with other the programming languages e.g., C, C++. Initial study shows high potential for computational gain by writing the code in C language. Another factor contributing to the higher computational time is the fact that code remains to be optimized yet. Some computational gain can be achieved by finding the optimal separation between two consecutive neighboring marks and it is expected that by increasing the separation few more pixels should provide good accuracy for the sampling points without compromising the performance.

Scanning resolution is another important area that remains to be investigated thoroughly. In this work initial study shows that four to five times more over sampling factor rather than eight (used in this research) is sufficient to scan HD-DataStripe without significant performance degradation. The choice of higher scanning (sampling) resolution used in this research is governed by the fact that it gives more clear understanding of the noise from PS process and this fact helps in noise characterization. Therefore, the aim to find optimal resolution has been set as a second goal. The lower scanning resolution is attractive for the portable identity verification devices, which currently offer 1200 dpi resolution. Furthermore, as the lower scanning resolution reduces 50% image size, it is safe to assume that it would further reduce the data-reading time.

While considering digital watermarking technique for high quality printed images, in this research only grayscale images are investigated and *high capacity* watermarking technique for color images remains to be investigated. In this research halftone images are printed at 300 dpi that is two times more than the resolution considered in the *existing work*; however, it would be still highly desirable to consider 600 dpi resolution, which is conventionally used for printing halftone images. Investigation for the halftone technique, which offers similar quality as the one obtained by using printer's internal driver and using this for data hiding is another direction for future work for high quality printed images with hidden data.

Another direction for further investigation is to see OCR performance gain when full knowledge about the semantic information to be extracted is known in advance. While considering contents integrity verification of hardcopy documents, as full contents are stored in the digital-seal (small size HD-DataStripe), this fact offers possibility to utilize this knowledge to improve OCR performance. In this context it is expected that OCR performance would reach to 100% as compared with the present scenario where it reaches up to 99% in ideal case. Furthermore, this approach would increase the robustness of OCR technology for the scenarios (character types, size and fonts) for which the existing OCR technology performs poorly.

While considering data hiding in constant background grayscale images the data-reading technique is again implemented in MATLAB, which results in higher computational time. The code optimization and its implementation in C or any other appropriate language still remains as a future work. Here, as multiple copies of the foreground text can be encoded in background image, this would *usually require less* data-reading time because once the first copy is recovered successfully; the remaining data needs not be recovered and processed. Another area yet to be investigated is to check wear-and-tear effects and by taking into account these effects for the specific application requirement some error correction coding needs to be implemented accordingly. However, as the multiple copies of foreground text can be stored in background image and the data is dispersed, in present scenario wear-and-tear effects are not expected to affect the performance significantly.

Application of HD-DataStripe in educational certificates would allow to biologically lock the document to its intended user so that the document cannot be misused. This can be achieved by using HD-DataStripe to store fingerprints of intended document holder along with other document contents. Consequently, each time certificate is submitted, the certificate holder would be asked for the fingerprints. For verification the document would be sent to the issuing authorities along with the fingerprints to verify: the contents integrity, counterfeiting and its intended user. Furthermore, data hiding technology for constant background grayscale images can be applied against data-tampering attacks, which would further increase the robustness against wear-and-tear effects. This new approach would eliminate the need for expensive content securing techniques, resulting in less-expensive and more efficient contents protection technology.

Another new application of HD-DataStripe and the data hiding technique for superposed background images would allow to transmit the exact copy of the fax documents by transmitting only the HD-DataStripe or digital contents recovered from it. This would decrease transmission time and communication cost, while offering *exact quality* as the original document does. The techniques given in this research would be even more useful in future with further advancements in printing and scanning technology, which would obviously offer superior quality.

One promising direction for future work is the investigation of printing technologies being used for security printing. As the security printing devices offer much higher resolution as compared with the office printing devices and such devices are especially designed for printing micro patterns, this fact consequently encourages to consider such technology to further increase the performance (capacity) of HD-DataStripe. Similarly, the data-reading can also be extended to color DataStripes, which would further increase the capacity. The color DataStripes could be especially beneficial for copy detection technique as it further increases the entropy of the CDP pattern. The data-reading technique is general and can be extended to other printing inks (magnetic, fluorescence, ultraviolet, infrared etc.) for highly sensitive security documents, increasing their strength and decreasing the dependence on expensive analog content protection technologies.

Finally, the findings of this research have potential usage in all existing applications of hardcopy documents that are prone to counterfeiting and data-tampering attacks. They can decrease dependence on: 1) the expensive storage media (e.g. optical memory stripe, IC-chips, magnetic stripe), and 2) analog document protection technologies intended for second/third-line identity verification.

Bibliography

[AlA04] A. M. Alattar, and O. M. Alattar, “Watermarking electronic text documents containing justified paragraphs and irregular line spacing,” *Proc. SPIE Conf. on Security and Watermarking of Multimedia Contents VI,* Vol. 5306, Jan. 2004**.**

[AnK97] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. *Int. Workshop on Security Protocols*, vol.1361, pp.125–136, 1997.

[Art04] Alessandro Artusi, “Real Time Tone Mapping,” *Ph.D. Dissertation, eingereicht an der Technischen Universität Wien*, 2004.

[Asb02] A. Hovstø, “Requirements Specifications: Visual ID on smart card used as a travel document,” *Contribution to Pan-European Electronic Identity White Paper*, version 1.1, 2002.

[Ami02] Isaac Amidror, “New print-based security strategy for the protection of valuable documents and products using moiré intensity profiles,” *Proc. SPIE Conf. on Optical Security and Counterfeit Deterrence Techniques IV*, Vol. 4677, Jan. 2002.

[BBG01] Bern, M. W. Breidenbach, J. A. Goldberg D., “Trustworthy paper documents,” *Information Hiding Workshop,* Apr. 2001, pp. 25-27; Pittsburgh, PA.

[BLM+95] J. T. Brassil, S. Low, N. F. Maxemchuk, and L. O’Gorman, “Electronic marking and identification techniques to discourage document copying,” *IEEE Journal on Selected Areas in Communication*, vol. 13, no. 8, pp. 1495–1504, Oct. 1995.

[BLM99] J. T. Brassil, S. Low, and N. F. Maxemchuk, “Copyright protection for the electronic distribution of text documents,” *Proc. of the IEEE*, vol. 87, no. 7, Jul. 1999, pp. 1181–1196.

[CBN] Canadian Bank Note Company Limited, “Machine readable visas, passports, identification cards,” http://www.cbnco.com/id/idproducts.html.

[CKL+97] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[CMB+01] I. Cox, M. Miller, J. Bloom, M. Miller **“**Digital Watermarking: Principles & Practice**”,** *Publisher: Morgan Kaufmann 2001*, ISBN: 1558607145

[Cryp] “Cryptoglyphs Technology Overview”, www.alpvision.com.

[DFV01] J. Dittmann, L. C. Ferri, C. Vielhauer: “Hologram Watermarks for Document Authentications,” Int. Symposium on Information Technology (ITCC 2001), Apr. 2001.

[DiC] "ARE YOUR IDS SECURE ENOUGH?" *Annual report Digimarc corporation*: www.digimarc.com.

[DMB04] IDAutomation.com, "Data Matrix Barcode FAQ & Tutorial." http://idautomation.com/datamatrixfaq.html. Available by Nov. 30th, 2004.

[DStr] Datastrip applications, http://www.findbiometrics.com/Pages/2dbarcodes/2dbar code_2.htm.

[DP03] Norberto Degara-Quintela, Fernando Perez-Gonzalez, "Visible encryption: Using paper as a secure channel", *Proc. of SPIE Conf. on Security and Watermarking of Multimedia Contents* V, volume 5020, Jan. 2003.

[Ditt01] J. Dittmann, "Content-fragile watermarking for image authentication", *Proc. of SPIE Conf. on Security and Watermarking of Multimedia Contents* III, Vol. 4314, Jan. 2001.

[Durr87] H. J. Durrett, "Color and computer", Academic Press Inc.,U.S. 1987, ISBN: 0122252101.

[DSF02] J. Dittmann, M. Steinebach, L. C. Ferri, "Watermarking protocols for authentication and ownership protection based on timestamps and holograms", *Proc. of* SPIE *Security and Watermarking of Multimedia Contents IV*, Vol. 4675, Jan. 2002.

[FDG01] Lefèbvre Frédéric, Delannay Damien, Gueluy A., Macq Benoit, "A print and scan optimized watermarking scheme", *IEEE Fourth Workshop on Multimedia Signal Processing, Cannes, France, October 3-5, 2001,* Proc., pp. 511-516, 2001.

[FMF+02] L. C. Ferri, M. Frank, C. Vielhauer, R. Steinmetz: "Biometric authentication for ID cards with hologram watermarks", *Proc. of SPIE Conf. Security and Watermarking of Multimedia Contents IV*, Vol. 4675, Jan. 2002.

[FPR+99] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn. Information hiding – a survey. *Proc. of I.E.E.E.*, 87(7):1062–1078, Jul. 1999.

[FuA01] M.S. Fu, O.C. Au, "Halftone Image Data Hiding with Intensity Selection and Connection Selection", *Signal Processing: Image Communication*, Vol. 16, No. 10, pp. 909 – 930, Aug. 2001.

[FuA02] M.S. Fu, O.C. Au, "Data Hiding Watermarking for Halftone Images*", IEEE Trans. On Image Processing*, Vol. 11, No. 4, Apr. 2002.

[Goo01] S. Gooran, "High Quality Frequency Modulated Halftoning," *Ph.D. Dissertation, Linköping Studies in Science and Technology Sweden*, Jan. 2001, ISBN 91-7219-913 X.

[GR98] L. O'Gorman and I. Rabinovich. Secure identification documents via pattern recognition and public-key crypto. *PAMI*, pp.1097–102, 1998.

[Hec94] D. Hecht, "Embedded Data Glyph Technology for Hardcopy Digital Documents," *Proc. of SPIE Color Hard Copy and Graphic Arts III,* Vol. 2171, Feb. 1994.

[HeO00] Hagit Z. Hel-Or, "Watermarking and Copyright Labeling of Printed Images", *Proc. of IEEE Int. Conf. on Image Processing (ICIP) 2000.*

[Her04] A. Herrigel, "Smart ID A new Approach for the Integrity Verification of Analog and Digital Documents", *Proc. of SPIE Conf. on Optical Security and Counterfeit Deterrence Techniques V*, vol. 5310, Jan. 2004.

[HoJ99] L. Hong and A. K. Jain, "Multimodal biometrics," *BIOMETRICS: Personal Identification in Networked society*, pp.327-344, 1999. ISBN: 0792383451

[HVH99] A.Herrigel, S.Voloshynovskiy and Z. Hrytskiv, "Optical/digital identification/verification system based on digital watermarking technology," *SPIE Int. Workshop on Optoelectronic and Hybrid Optical/Digital Systems for Image/Signal Processing ODS'99*, Lviv Ukraine, Sep. 1999.

[JBP99] A.K. Jain, R. Bolle and S. Pankanti (Eds.), "BIOMETRICS: Personal Identification in Networked society, Kluwer Academic Publishers, 1999. ISBN: 0792383451

[JRP04] A. K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, Vol. 14, No. 1, pp. 4-20, Jan. 2004.

[JRU05] A. K. Jain, A. Ross, and U. Uludag, "Biometric Template Security: Challenges and Solutions", *Proc. of EUSIPCO*, Sep. 2005.

[Kan99] H. R. Kang, **"**Digital Color Halftoning**",** *Publisher John Wiley & Sons*. 1999 ISBN: 0780347412.

[Kim05] H. Y. Kim, "A public-key authentication watermarking for binary document images resistant to parity attacks", *IEEE Int. Conf. on Image Processing*, vol. 2, pp. 1074-1077, 2005.

[KJJ04] D. Kirovski, N. Jojic, and G. Jancke, "Tamper-Resistant Biometric IDs," *Information Security Solutions Europe, (Berlin, Germany),* Sep. 28-30 2004.

[LCD] LaserCard Data Storage Capacity Comparison, available on the Web at: http://www.lasercard.com/tech/technology4.htm.

[LoM00] S. H. Low and N. F. Maxemchuk, "Capacity of text marking channel," *IEEE Signal Processing Letters*, vol. 7, no. 12, pp. 345–347, Dec. 2000.

[LoM98] S. H. Low and N. F. Maxemchuk, "Performance comparison of two text marking methods," *IEEE Transaction on Selected Areas in Communication*, 1998.

[LN05] D. Lopresti, G. Nagy, "Chipless ID for paper documents," *Document Recognition and Retrieval XII, Proc. of SPIE-IS&T Electronic Imaging*, Vol. 5676, Jan. 2005.

[MAC+04] K. Mikkilineni, G.N. Ali, P. Chiang, G.T.C. Chiu, J.P. Allebach, and E.J. Delp, "Signature-Embedding in Printed Documents for Security and Forensic Applications," *Proc. of the SPIE Conf. on Security, Steganography and Watermarking of Multimedia Contents*, San Jose, CA, Vol. 5306, Jan. 2004,

[MBB04] Motwani, R.; Breidenbach, J. A.; Black, J. "Collocated Dataglyphs for Large Message Storage and Retrieval", *Proc. of SPIE Conf. Security, Steganography and Watermarking of Multimedia Contents VI*, Vol. 5306, Jan. 2004.

[MoS98] P. Moulin, J. O'Sullivan, "Information-theoretic analysis of information hiding," *IEEE Int. Symposium on Information Theory*, Boston, MA, Aug. 1998.

[MOV96] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. Handbook of Applied Cryptography. *CRC Press*, 1996.

[MWM01] Q. Mei, E. Wong and N. Memon, "Data Hiding in Binary Text Documents," *Proc. of SPIE Conf. Security and Watermarking of Multimedia Contents III*, Vol. 4314, Jan. 2001.

[Pic04] J. Picard, "Digital authentication with copy-detection patterns," *Proc. of SPIE Conf. on Optical Security and Counterfeit Deterrence Techniques V*, San Jose, CA USA, Vol. 5310, Jun. 2004

[Phil00] G. Phillips, "Combining thermochromics and conventional inks to deter document fraud," *Proc. of SPIE Conf. on Optical Security and Counterfeit Deterrence Techniques III*, vol. 3973, Apr. 2000.

[Phil02] G. Phillips**,** "Combining nanocharacter printing, digital watermarking, and UV-coded taggents for optimal machine-readable security," *Proc. of SPIE Conf. on Optical Security and Counterfeit Deterrence Techniques IV,* Vol. 4677, Apr. 2002**.**

[Phil04] G. Phillips**,** "New digital anti-copy/scan and verification technologies," *Proc. of SPIE Conf. on Optical Security and Counterfeit Deterrence Techniques V*, Vol. 5310, Jun. 2004.

[PNW+04] Sharron G. Penn, Scott M. Norton, Ian D. Walton, Richard Freeman, and Glenn Davis “Nanobarcodes particles as covert security tags for documents and product security” *Proc. of SPIE Conf. on Optical Security and Counterfeit Deterrence Techniques V*, Vol. 5310, Jun. 2004.

[PVT04] J. Picard, C. Vielhauler and N. Thorwirth, “A Fraud-Proof ID document based on multiple data hiding technologies and biometrics”, *Proc. of SPIE Conf. Security and Watermarking of Multimedia Contents* VI, Vol. 5306, Jan. 2004.

[Ren98] Rudolf L. van Renesse, "Optical Document Security", *Second Edition, Artech House, Boston, London*, 1998. ISBN: 0890069824

[Ren05] Rudolf L. van Renesse, "Optical Document Security", *Third Edition, Artech House, Publishers*, 2005. ISBN: 1580532586

[ShT97] G. Sharma and H. J. Trussell, “Digital color imaging,” *IEEE Trans. Image Proc.*, vol. 6, no. 7, pp. 901-932, Jul. 1997.

[ShW04] G. Sharma and S. Wang, “Show-through watermarking of duplex printed documents,” *Proc. of SPIE Conf. on Security, Steganography and Watermarking of Multimedia Contents* VI, Vol. 5306, Jan. 2004.

[SCO] Smart Card Overview, available on the Web at: http://java.sun.com/ products/ javacard/smartcards.html.

[SMS03] M. Suzaki, Y. Mitsui, and M. Suto, “New alteration detecting technique for printed documents using dot pattern watermarking”, *Proc. SPIE Conf. on Security and Watermarking of Multimedia Contents V,*Vol. 5020, Jan. 2003.

[SRS+] C. Soutar, D. Roberge, A. Stoianov, R. Gilory, and B.V.K.V. Kumar, “Biometric Encryption”, www.bioscrypt.com.

[SSC05] G. S. Spagnolo, C. Simonetti and L. Cozzella, “Content fragile watermarking based on a computer generated hologram coding technique”, *J. Opt. A: Pure Appl. Opt.* **7** 333-342, 2005.

[ST] Symbol Technologies Inc. The PDF417 Barcode. Details available from: http://www.pdf417.com.

[Tia04] J. Tian, “Digital authentication with digital and analog documents”, *Digimarc Corporation*, US Patent Appl. No. 20040264732, Dec. 2004.

[Tch04] J. Tchan, “The development of an image analysis system that can detect fraudulent alterations made to printed images,” *Proc. of SPIE Conf. Optical Security and Counterfeit Deterrence Techniques V*, Vol. 5310, Jan. 2004.

[UPP+04] U. Uludag, S. Pananti, S. Prabhakar, and A. K. Jain, “Biometric Cryptosystem: Issues and Challenges”, *Proc. IEEE* Vol. 92, No. 6, Jun. 2004.

[VKD04] S. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun, “Visual communications with side information via distributed printing channels: extended multimedia and security perspectives,” *Proc. of SPIE Conf. on Security, Steganography, and Watermarking of Multimedia Contents VI*, Vol. 5306, Jan. 2004.

[VVK+05] R. Villán, S. Voloshynovskiy, O. Koval and Thierry Pun, “Multilevel 2D Bar Codes: Towards High Capacity Storage Modules for Multimedia Security and Management,” *Proc. of SPIE Conf. on Security, Steganography, and Watermarking of Multimedia Contents VII*, Vol. 5661, Jan. 2005.

[Wan01] H.C. Wang (2001), “Data Hiding Techniques for Printed Binary Images,” *Proc. of IEEE International Conference on Information Technology: Coding and Computing (ITCC-2001)*, pp 55-59, Las Vegas, Nevada, Apr. 2001.

[WLH99] H.C. Wang, C. Y. Lin, C. C. Huang, (1999), Data Hiding in a binary image by the modified digital halftoning techniques, *Proc., of Conference on Computer Vision, Graphics and Image Processing (CVGIP)*, pp. 183-190, Taipei, Taiwan, Aug. 1999.

[WoM01] P. W. Wong, N. Memon, “Secret and public key image watermarking schemes for image authentication ownership verification”, *IEEE Trans. on Image Processing*, Vol. 10, No. 10, Oct. 2001.

[Wu01] M. Wu, Multimedia Data Hiding, *Ph.D. thesis, Princeton University*, 2001.

[WuL04] M. Wu, and B. Liu, “Data Hiding in Binary Image for Authentication and Annotation,” *IEEE Trans. on Multimedia, Vol. 6, No. 4*, Aug. 2004.

[Zha04] J. Zhao, “Digital authentication with digital and analog documents” *MediaSec Technologies GmbH (DE)*, US Patent No. 6,751,336, Jun. 2004.

[ZPT04] J. Zhao, J. Picard, N. Thorwirth, “Apparatus and methods for improving detection of watermarks in content that has undergone a lossy transformation,” *MediaSec Technologies, GmbH (DE)*, US Patent No. 6,782,116, Aug. 2004.

Appendix-A:

In another scenario corresponding to the black dot, having immediate top, bottom and right dots as white ones and left one black dot is considered here. As mentioned earlier all these dots are the immediate neighbors. Furthermore, corner dots are not taken into account. Also, similar procedure is followed as before; however, some of the equations are modified according to the new scenario.

Filter-5 Case-2:

It starts by computing the statistic, X_1 as follows,

$$X_1 = (-1).\left(\sum_{x=\sigma_1} \sum_{y=y_1+\sigma_2}^{y_2-\sigma_2} (B_{i,j}(x,y) - I_{i,j}(x,y)) \right) \qquad \text{(A-1)}$$

σ_1, σ_2, are integer constants. ***I*** is identity matrix having same size as ***B***. As black and white pixels have values “0” and “1”, respectively, this fact does not allow to count the black pixels, unlike white pixels which can be handled easily by summation operator (as in eq. (3.17)). In eq. (A-4) subtraction and multiplication of value, -1, interchanges the behavior of black and white pixels, and allows easy handling of black pixels otherwise it would have required many changes.

Now, if $1 \le X_1 < T_0$ and $T_1 = 0$, where T_0 and T_1 are given by:

$$T_0 = (-1).\left(\sum_{x=\sigma_1+1} \sum_{y=y_1+\sigma_2}^{y_2-\sigma_2} (B_{i,j}(x,y) - I_{i,j}(x,y)) \right),$$

$$T_1 = (-1).\left(\sum_{x=\sigma_1+4} \sum_{y=y_1+\sigma_2}^{y_2-\sigma_2} (B_{i,j}(x,y) - I_{i,j}(x,y)) \right).$$

Furthermore,

$$\left[\sum_{x=x_1+3}^{x_2-2} \sum_{y=y_1+2}^{y_2-3} (B_{i-1,j}(x,y) - I_{i,j}(x,y)) + \sum_{x=x_1+3}^{x_2-2} \sum_{y=y_1+3}^{y_2-2} (B_{i+1,j}(x,y) - I_{i,j}(x,y)) + \right.$$

$$\left. \sum_{x=x_1+2}^{x_2-2} \sum_{y=y_1+2}^{y_2-2} (B_{i,j+1}(x,y) - I_{i,j}(x,y)) \right] = 0 \quad \ldots\text{(A-2)}$$

It is to be noted that in eq. (A-2) dot gain/loss effects has to be taken into account. When all the above conditions are satisfied, only then the submatrix can be considered *as possible candidate* and it proceeds as follows:

$$X_2 = (-1).\left(\sum_{x=\sigma_1}^{\alpha} \sum_{y=\sigma_2}^{y-\sigma_2} (B_{i,j}(x,y) - I_{i,j}(x,y)) \right)$$

(A-3)

Where value of α is computed from the following relation,

$$\arg\max_{\alpha \in X} \left\{ \sum_{X} \sum_{y=\sigma_1}^{y_2-\sigma_1} B_{i,j}(x,y) = 1, \quad X \in [\sigma_1, \ldots, \sigma_1 + 4] \right\}, \tag{A-4}$$

If $X_2 \geq T_2$ (T_2 is an integer constant) then compute X_3, X_4, X_5 as follows:

$$X_3 = (-1) \cdot \left[\sum_{x=\alpha} \sum_{y=y_1}^{y_2} (B_{i,j}(x,y) - I_{i,j}(x,y)) + \sum_{x=\alpha} \sum_{y=y_m}^{y_2} (B_{i-1,j}(x,y) - I_{i,j}(x,y)) \right.$$
$$\left. + \sum_{x=\alpha} \sum_{y=y_m}^{y_2} (B_{i+1,j}(x,y) - I_{i,j}(x,y)) \right] \tag{A-5}$$

$$X_4 = (-1) \cdot \left[\sum_{x=\alpha-1} \sum_{y=y_1}^{y_2} (B_{i,j}(x,y) - I_{i,j}(x,y)) + \sum_{x=\alpha-1} \sum_{y=y_m}^{y_2} (B_{i-1,j}(x,y) - I_{i,j}(x,y)) \right.$$
$$\left. + \sum_{x=\alpha-1} \sum_{y=y_m}^{y_2} (B_{i+1,j}(x,y) - I_{i,j}(x,y)) \right] \tag{A-6}$$

Similarly, X_5 can be computed from (A-5) or (A-6) by substituting $x = \alpha - 2$, and it is given by:

$$X_5 = (-1) \cdot \left[\sum_{x=\alpha-2} \sum_{y=y_1}^{y_2} (B_{i,j}(x,y) - I_{i,j}(x,y)) + \sum_{x=\alpha-2} \sum_{y=y_m}^{y_2} (B_{i-1,j}(x,y) - I_{i,j}(x,y)) \right.$$
$$\left. + \sum_{x=\alpha-2} \sum_{y=y_m}^{y_2} (B_{i+1,j}(x,y) - I_{i,j}(x,y)) \right] \tag{A-7}$$

where $x_m = \left\lfloor \frac{x_1 + x_2}{2} \right\rfloor, \qquad y_m = \left\lfloor \frac{y_1 + y_2}{2} \right\rfloor$

Using eqs. (A-5) and (A-7) another statistic X_6 is computed as

$$X_6 = \begin{cases} (X_3 + X_4) & X_3 \geq T_3 \\ (X_4 + X_5) & X_3 < T_3 \end{cases} \quad ; T_3 \text{ is a known integer constant.}$$

Finally, X_7 is computed as

$$X_7 = (-1)\left(\sum_{x=\alpha-1}^{\alpha} \sum_{y=y_m}^{y_2} (B_{i-1,j}(x,y) - I_{i,j}(x,y)) + \sum_{x=\alpha-1}^{\alpha} \sum_{y=y_1}^{y_m} (B_{i+1,j}(x,y) - I_{i,j}(x,y)) \right)$$

(A-8)

Now, if $X_6 \leq T_4$, and $X_7 \leq T_5$, where T_4, T_5 are known constants and take same value as before, then $X_{i,j}$ is marked as *black dot*, means binary “0” is detected as recovered bit.

Appendix B:

Table B1: Number of errors encountered in recovered data for the novel HD-DataStripe.

Exp. no	1	2	3	4	5	6	7
Errors	6	12	9	17	5	17	15
Exp. no	8	9	10	11	12	13	14
Errors	7	24	24	18	23	40	9
Exp. no	15	16	17	18	19	20	21
Errors	18	18	19	9	20	22	28

Table B2: Number of errors encountered in recovered data for various printing devices using unoptimized set of parameters.

Printer	**HP4050**	**HP4600**	**HP8150**	**HP8000**	**HP4100**	**HP2200**	**HP2100**
Test1	95	147	47	154	261	233	237
Test2	116	153	164	237	326	326	300
Test3	146	160	19	**494**	284	360	197
Test4	147	129	108	256	289	343	255
Test5	152	192	32	211	361	308	375
Test6	94	189	**350**	329	325	375	268
Test7	198	**806**	92	136	298	**510**	**721**
Mean	**135**	**253**	**116**	**259**	**307**	**350**	**336**

Table B3: Number of errors encountered in recovered data for various printing devices using optimized set of parameters.

Scanner	HP8250	HP5550	HP8250	HP8250	HP8250	HP8250	HP8250
Printer	**HP8150**	**HP4600**	**HP4050**	**HP8000**	**HP2100**	**HP4100**	**HP2200**
Test1	25	100	95	162	142	261	233
Test2	42	90	116	188	150	326	326
Test3	83	89	146	133	170	284	360
Test4	29	86	147	199	141	289	343
Test5	48	90	152	211	142	361	308
Test6	50	114	94	347	150	325	375
Test7	93	198	198	108	274	298	510
Mean	**53**	**109**	**135**	**193**	**167**	**307**	**350**

Table B 4: Performance comparison of two scanners HP5550c and HP8250 for three printing devices.

Printer	**HP8150**	**HP8150**	**HP4600**	**HP4600**	**HP8000**	**HP8000**
Test1	25	48	197	100	162	133
Test2	42	112	211	90	188	50
Test3	83	35	244	89	133	29
Test4	29	102	234	86	199	180
Test5	48	67	237	90	211	186
Test6	50	126	210	114	347	309
Test7	93	171	285	198	108	324
Scanner	**HP8250**	**HP5550**	**HP8250**	**HP5550**	**HP8250**	**HP5550**
Mean	**53**	**94**	**231**	**198**	**193**	**173**

Table B5: Performance comparison for two different RM-patterns considering three different printing devices.

Scanner	HP8250	HP8250	HP8250	HP8250	HP8250	HP8250
Printer	**HP8150***	**HP8150**	**HP2100***	**HP2100**	**HP4100***	**HP4100**
Test1	25	120	142	207	261	255
Test2	42	95	150	169	326	274
Test3	83	125	170	191	284	275
Test4	29	140	141	178	289	253
Test5	48	97	142	190	361	**514**
Test6	50	105	150	227	325	284
Test7	93	144	274	**629**	298	**502**
Mean	**93**	**118**	**167**	**256**	**307**	**337**

* MRM-Pattern

Table B6: Robustness of data-reading technique against 10% contrast as well as luminance reduction noise.

	10% LR	**10% CR**	**10% LR**	**10% CR**	**10% LR**	**10% CR**
Printer	**HP8150**	**HP8150**	**HP4600**	**HP4600**	**HP4050**	**HP4050**
Test1	37	38	141	140	144	132
Test2	42	67	149	134	163	147
Test3	69	120	166	142	127	185
Test4	33	36	130	148	161	167
Test5	66	59	201	172	162	204
Test6	79	67	147	116	91	126
Test7	45	203	287	232	83	246
Mean	**53**	**84**	**174**	**155**	**133**	**172**

Table B7: Time profile (in seconds) of some computationally most expensive parts (filters, routines) of data-reading techniques.

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
Test1-A1	127.3	54.3	46.0	15.2	7.8	1.9	2.1	10.3	288	220
Test1-A2	139.9	57.0	45.6	15.1	7.8	1.8	1.9	10.3	303	240
Test1-A3	126.0	55.6	46.0	15.3	7.9	1.9	0.7	10.5	288	220

A1, A2 and A3 represent HP8150, HP4050 and HP2100 printing devices, respectively. Test1 is HD-DataStripe consisting of real-data.

A …is the computational time taken by the adaptive binarization technique.

B …computational time taken by the Filters: 3-5,

C … computational time taken by the Filters: 5-6,

D-J ... computational time taken by the Filter-2, Filter-1, RM-pattern identification, template drawn, image reading, total computational time including profile generation, and data-reading time with profile-generation option deactivated.

Table B8: Optimal performance obtained with modified priority.

Scanner	HP8250	HP5550	HP8250	HP8250	HP8250	HP8250	HP8250
Printer	**HP8150**	**HP4600**	**HP4050**	**HP8000**	**HP2100**	**HP4100**	**HP2200**
Test1	21	135	112	177	167	263	234
Test2	35	94	128	206	157	326	293
Test3	52	99	119	141	181	278	345
Test4	39	97	122	226	159	276	334
Test5	47	138	139	207	165	345	309
Test6	54	101	83	393	218	279	335
Test7	39	204	124	97	201	282	408
Mean	**41**	**124**	**118**	**207**	**178**	**293**	**323**

Table B9: Empty toner performance (errors in recovered data) of a printing device. (Printer: HP8000, Scanner: HP8250c, Optimized scenario without modified priority, * real data without superposed noise)

Test	1	2	3	4	5	6	7*	**Mean**
Errors	112	81	107	91	135	86	94	101

Table B10-1: Comparison of the existing binarization techniques using new RM-pattern. Printer HP8150 and Scanner HP8250

	Novel	MW	Wang	Fu	MW*	Wang*	Fu*
Test1	25	1232	920	5373	2035	2094	6809
Test2	42	1441	1235	5593	2361	2699	7109
Test3	83	1247	851	5807	1920	2054	7254
Test4	29	1320	944	5351	2118	2200	6790
Test5	48	1848	1389	5813	2685	2633	7130
Test6	50	2230	1342	6115	3099	2508	7460
Test7	93	1488	1128	5331	2189	2191	6318
Mean	**53**	**1543**	**1115**	**5626**	**2343**	**2340**	**6981**

* By shifting the sampling point (region) by one pixel in a random order.

Table B10-2: Comparison of the existing binarization techniques using new RM-pattern. Printer HP8000 and Scanner HP8250

	Novel	MW	Wang	Fu	MW*	Wang*	Fu*
Test1	162	3348	2739	8031	4607	4185	9423
Test2	188	3433	3186	8592	4659	4446	9882
Test3	133	3162	2952	7980	4218	4165	9181
Test4	199	3331	2696	7867	4325	3812	9192
Test5	211	3278	2850	8101	4391	4149	9281
Test6	347	3859	3367	8676	5008	4585	9813
Test7	108	2639	2373	7174	3591	3458	8014
Mean	**193**	**3293**	**2880**	**8117**	**4400**	**4115**	**9255**

* By shifting the sampling point (region) by one pixel in a random order.

Table B10-3: Comparison of the existing binarization techniques using new RM-pattern. Printer HP2100 and Scanner HP8250

	Novel	MW	Wang	Fu	MW*	Wang*	Fu*
Test1	142	3336	3107	8642	5023	4647	9819
Test2	150	3171	3103	8623	4745	4530	9835
Test3	170	3349	3253	8465	4925	4621	9671
Test4	141	2913	3175	8212	4349	4420	9458
Test5	142	3249	3321	8391	4561	4680	9559
Test6	150	3976	3447	9009	5538	4988	10115
Test7	274	2784	2633	7263	4115	3799	8234
Mean	**167**	**3254**	**3148**	**8372**	**4750**	**4526**	**9527**

* By shifting the sampling point (region) by one pixel in a random order.

Appendix-C

C-1: Parameters for Various Filters

Filter-2: $\omega_1 = 1, \omega_2 = 2$ and $\alpha = 1$.

Filter-5: $\sigma_1 = 2, \sigma_2 = 3$, $T_2 = 2$, $T_3 = 5$, $T_4 = 16$ and $T_5 = 1$.

Filter-6: $\varepsilon_1 = 0.5 \cdot \textit{total numer of elements in the submatrix}$, and $\varepsilon_2 = 1$.

C-2: Filter parameters used to obtain optimal performance (Table-B3)

Adaptive Binarization Technique parameters that need to be modified.

ML: Mean luminance value is obtained using criteria discussed in section 3.8.1. In this research T_1 is obtained by adding a value ~10 in ML; except HP8000 and HP2100, which suffer from dot loss effects and 20-30 value is added. Note: usually a deviation ±5 in T_1 does not affect the performance significantly.

Printer	HP8150	HP4600	HP4050	HP8000	HP2100	HP4100	HP2200
ML	120	110	117	110	130	115	120
T_1	128	120	128	135	150	120	128
T_3	5	10	5	5	5	5	5
T_4	15	20	15	15	15	15	15

C-3: Scanning Process Parameters

	Highlights	Shadows	Midtones	Resolution	Color
HP8250	247	6	2.20	2400	Grayscale
HP5550c	247	6	2.20	2400	Grayscale

All other parameters have been used as the default settings.

C-4: Second Order Polynomial Fitting

According to this approach a fixed number of points at the center of HD-DataStripe are used to find the location of the center points needed to approximate second order polynomial. Initially all center points are chosen as an average value of the center points and template is drawn using 2nd order approximation. Next, the isolated points (black dots surrounded by all white ones) are identified using the technique discussed in RM-pattern recognition to precisely recognize these isolated dots. As the isolated dots, dots at predefined locations at central region can be used.

Next, the error is computed objectively between template drawn using 2nd order approximation and isolated dots as follows:

$$E = \sum_{i=1}^{n} abs(y_i' - y_i'')$$

y_i', y_i'', are upper y-coordinates of the top-side of isolated dot i and of the template at that location, respectively and n is the desired number of isolated points. Then the initial center point is shifted slightly and whole process is repeated by shifting ±1, ±2 the initial center points. Finally, the template resulting in minimum error is considered as the correct one and is utilized by the data reading technique afterwards.

Above approach requires dots modification in original HD-DataStripe and avoidance in data recovery process. Another approach that avoids contents modification could be to search for fixed number of isolated dots, starting from center region, in its neighborhood. The former approach is expected to result in less computational time, whereas the latter one does not require contents modifications as it utilizes the exiting contents to as the isolated dots. The feedback error control can also be added to 2nd order polynomial approximation by checking the number of errors encountered in recovered data. In this case, predetermined *small* critical region (e.g. small central region) can be used by the data-reading technique to find the number of errors encountered in recovered data for template modifications as a feedback error. It is to be mentioned that this technique is not yet implemented.

Appendix-D

Figures D-1 and D-2 shown on the following pages, are printed again without size reduction to illustrate the true quality of constant background grayscale images with and without superposed text (previously shown in Figure 6.8-6.9).

Chapter 6 Data Hiding in Background Images

Recently a watermarking technique for hardcopy documents such a Cinema tickets, contracts etc,. is given in [1] by Suzaki et al. This technique allows to encode *Hidden Message* in a *Constant Greyscale Background Image* (CGBI) and claims higher capacity for the hidden/watermark data as compared with the previous techniques given for similar applications. In this research we have found that by using our ideas, discussed in Chapter 3 for data recovery from hardcopy documents e.g. High-Density Bar Codes (HDBC), a further improvement in the capacity offered by the existing technique [1] can be achieved. With this objective we have given an improved technique which is described and discussed in this Chapter. The new technique uses CGBI of the same quality as in [1] to encode contents integrity related data. However, it offers much stronger methods for contents integrity verification and this is due to the fact the novel technique offers sufficient capacity to encode both contents integrity related extracted features as well as the full contents of the document, providing additional benefits. The novel technique uses different data encoding method, but still results in same quality of the background image. The data-reading method given in this work, enables to recover the encoded information from more noisy environment as compared with the existing technique. The robustness of the new technique against rotational distortion is checked by using two different methods, whereas one of the methods does not depend on the rotated image. The suggestion made in the existing work [1] to use ECC to overcome errors due to character overlapping is not found very promising for final applications and a different approach is used for such scenarios. For performance evaluation of the new technique more than one printers are used. Finally, in the existing technique no results are reported for practical applications, whereas in the novel technique issues related to the practical applications are considered as well.

6.1 Brief Review of Existing Work

To encode hidden data in hardcopy text documents different techniques have been proposed. In [2] data is encoded by slightly shifting up-down, left-right a group of characters (word). Whereas in another technique [3] interline space is varied by one pixel to encode a single bit of information. There are techniques in which pattern of

Appendix-E

Potential Counterfeiting Threats Against the Cryptoglyph^{TM} Technology

In this section on abstract level the strength of cryptoglyph against active counterfeiting attack is assessed based the underlying mechanism used in the technology. In this research a counterfeiting attack is characterized as *active* if noise behavior is analyzed scientifically and the appropriate filters (e.g. techniques given in chapter 3 and 6) are developed and used to recover the original signal (to be used as counterfeit). In *passive attacks* either the signal (printed mark) is copied using a high-quality copying device or scanned at sufficiently higher resolution using high quality scanner and printed as counterfeit. In [Cryp] it is mentioned that anti-counterfeiting technology works with conventional printing (e.g. inkjet, laser printers) and scanning devices (flatbed scanners, digital cameras, mobile phone cameras), given that a device offers resolution 600 dpi or higher. The strength of the printed cryptogyph mark is attributed to invisibility (smaller dot size) and *randomly spread* (missing synchronization marks) dots of size 1/600 of an inch or less. For present discussion mark generation process (encoded information, data redundancy and data encryption technique) is irrelevant and what concern here is the randomly spread tiny printed dots that needs to be recovered from the digitized image to find the actually printed cryptoglyph mark. Once the originally printed mark is recovered with *high accuracy* this can be used to counterfeit the genuine application. Next, it comes to show the possibility to recover the originally printed mark and is the objective of following discussion.

A Potential Counterfeiting Attack

While considering *invisibility* of cryptoglyph mark, clearly it does not contribute to the strength, as it pose no challenge (against active counterfeiting attacks) for an expert due to the fact that mark can be visualized from the scanned image. Of course the printed mark has to be digitized at sufficient higher over-sampling rate and visualized using some image processing software.

Next, it comes to recover the original cryptoglyph mark (randomly spread pixels) from the digitized image. This scenario is similar to HD-DataStripe or CDP in which dots are randomly spread, so broadly speaking similar approach as the one used for data-reading technique in chapter-3 can be used. In present scenario there are some additional challenges arising from the missing registration marks patterns (needed to generate the sampling point array) and unknown size (resolution) of the actually printed dots. The 600 dpi constraint for printing device does not guarantee that this resolution has actually been used to print the mark and any resolution resulting in *almost invisible* printed dots might have been used. At this stage some crucial decisions have to be made.

Scenario-I: Cryptoglyph Mark Printed at Full Resolution

In this research it is found (see chapter-3) that if the mark is printed at 600 dpi then inter-symbol interference gets very strong and consequently makes the exact *printed* signal recovery impossible (Fig. 3.4 pp. 41). This is true for both inkjet as well as laser technologies. However, for inkjet technology such behavior starts at much lower data encoding rate (i.e. larger symbol size or lower resolution). This means that if the mark is printed at full resolution then only those symbols, which are not affected by inter-symbol interference noise, can be used. Such symbols could consist of either single or group of *black* pixels put together (like AM halftoning Fig 2.8 pp. 18), given that symbol size grows within invisible range. It is mentionable that it has been shown in chapter-6 that invisible printed dots measuring 1/600 of an inch have sufficient energy and allow the original signal to be recovered, given that mark does not suffer from inter-symbol interference. If this is the case then the original cryptoglyph mark can be recovered with the help of *superposed RM-pattern* discussed afterwards. Apart from the above discussion, it seems that in reality mark is unlikely to be printed at full resolution because the constraint on imaging device cannot allow digitizing the image at higher over-sampling rate.

Scenario-2: Cryptoglyph Mark Printed at One Half of Full-Resolution

Invisibility can also be achieved at 300 dpi, where an isolated printed dot is *almost invisible* (as claimed in [Cryp]). However, at 300 dpi signal strength gets higher as compared with 600 dpi, making it easier to recover the mark. Furthermore, it has been shown in this research that for laser printing technology at 300 dpi inter-symbol interference does not distort the signal beyond recovery. Digitization process remains within the constraint imposed by device and minimum over-sampling factor. One constraint that cannot be fulfilled is unavoidable inter-symbol interference for inkjet technology at this resolution. This consequently implies that only isolated black symbols can be used and invisibility is further controlled by decreasing the ratio of black dots per unit area. If this is the case, which seems to be very likely then the original cryptoglyph mark recovery is guaranteed as shown in chapter-3. Here the absence of inter-symbol interference makes original signal recovery much more easier. In order to recover the randomly spread mark, RM-pattern is to be superposed as mentioned above and then mark can be recovered.

Scenario-3: Cryptoglyph Mark With Unknown Symbol Size

In general dot (or symbol) size could be any integer divisor of full-resolution (600 dpi) that results in zero remainder and additionally satisfies the invisibility constraint as well. With above constraints, the following set of values Dot-Size=[200, 300, 600] could be the possible candidates for print resolution. Another possibility could be to form a template of *isolated dots* consisting of continuously (at small step-size) increasing dot sizes that are almost invisible and then digitizing this printed template at sufficiently high over-sampling rate. The invisible cryptoglyph mark can be digitized at same over-sampling rate that is used in template digitization and the match for the smallest dot found in cryptoglyph can be searched in the template to estimate the print resolution used in cryptoglyph mark printing. This process might need to be repeated several times for different or same cryptoglyph mark using same printer. It is not difficult to find the actual printer used to print the cryptoglyph mark and same device can be used by the person intending repudiation attack. By taking into account the commitment and available print/scan and computational facilities the above scenario should not be considered very complex for a skilled counterfeiter.

Registration Mark Pattern

Given that print resolution (size of the smallest printed dot visible in digitized image) used to print the mark is known, then sampling point array can be obtained by printing a pattern in which only isolated black dots are separated suitably so that there is no inter-symbol interference. The pattern needs to be scanned at appropriate over-sampling rate and from the resulting pattern center points of the isolated pixels can be found using the technique given chapters 3 and 6 for RM-pattern identification. From the identified central points remaining points can be estimated. This would result in a sampling point array. By superposing scanned RM-pattern on the cryptoglyph mark and after careful alignment, the cryptoglyph mark can be sampled to recover the actually printed cryptoglyph mark.

Finally, the fact that digital cameras and mobile phones cameras, which unlike scanners cannot be in close contact with the crpytoglyph mark, can be used for counterfeiting detection shows that printed signal has enough engery and this energy can be exploited to launch active counterfeiting attack.