

**A
DISSERTATION
ON
WATERMARKING TECHNIQUE FOR
DIGITAL IMAGES (Using SVD)**

Submitted In Partial Fulfillment of the Requirement for the
Award of the Degree of

**MASTER OF ENGINEERING
(COMPUTER TECHNOLOGY & APPLICATION)**

SUBMITTED BY:
JITENDRA SINGH KUSHWAH

COLLEGES ROLL NO: 09/CTA/09
UNIVERSITY ROLL NO. 8548

Under the esteemed Guidance of:
MR. MANOJ KUMAR
(ASSISTANT PROFESSOR, COMPUTER ENGINEERING)



**DEPARTMENT OF COMPUTER ENGINEERING
DELHI COLLEGE OF ENGINEERING
UNIVERSITY OF DELHI
2009-2011**

CERTIFICATE



DELHI COLLEGE OF ENGINEERING
(Govt. of National Capital Territory of Delhi)
BAWANA ROAD, DELHI – 110042

Date: _____

This is certified that the major project report entitled “**WATERMARKING TECHNIC FOR DIGITAL IMAGES (Using SVD)**” is a work of **Jitendra Singh Kushwah** (College Roll No 09/CTA/09 & University Roll No- 8548) is a student of Delhi College of Engineering. This work is completed under my direct supervision and guidance and forms a part of master of engineering (Computer Technology and Application) course and curriculum. He has completed his work with utmost sincerity and diligence.

The work embodied in this major project has not been submitted for the award of any other degree to the best of my knowledge.

MR MANOJ KUMAR

Assistant Professor and Project Guide
Department of Computer Engineering
Delhi College of Engineering,
University of Delhi, India

ACKNOWLEDGEMENT

It is distinct pleasure to express my deep sense of gratitude and indebtedness to my learned supervisor **Mr. Manoj Kumar** Assistant Professor, Department of Computer Engineering, Delhi College of Engineering, for his invaluable guidance, encouragement and patient reviews. His continuous inspiration only has made me complete this dissertation. Without his help and guidance, this dissertation would have been impossible. He remained a pillar of help throughout the project.

I am extremely thankful to **Dr. Daya Gupta**, Head of the Department, Computer Engineering, Delhi College of Engineering, Delhi, for the motivation and inspiration. I would like to take this opportunity to present my sincere regards to my teachers **Mrs. Rajni Jindal, Mr. Vinod Kumar, Dr. S. K. Saxena, Mr. Manoj Sethi, Mrs. Akshi Kumar, Mr. Shailendra Singh, Mr. R. P. Yadav**. I am also thankful to all teaching and non-teaching staff of Computer Engineering Department for providing me unconditional and any time access to the resources and guidance.

I am grateful to my parents for their moral support all the time; they have been always around to cheer me up, in the odd times of this work. I am also thankful to my classmates for their unconditional support and motivation during this work. Last but not least, I special thanks to the crowd who are active in the field of Image Watermarking issues.

JITENDRA SINGH KUSHWAH

Master of Engineering
(Computer Technology & Application)
College Roll No. - 09/CTA/09
University Roll No. - 8548
Department of Computer Engineering
Delhi College of Engineering, Delhi-110042

ABSTRACT

Digital watermarking addresses the growing concerns of theft and tampering of digital media through the use of advanced signal processing strategies to embed copyright and authentication information within media content., since it makes possible to identify the author, owner, distributor or authorized consumer of a document. In case of any dispute, one can prove their identity by decoding the watermark. This thesis aims to develop and implement Robust and secure watermarking technique for digital images. Two most important prerequisites for an efficient watermarking scheme are robustness and invisibility. After embedding the watermark, perceptual quality of the digital content should not be degraded and watermark must be recoverable from the watermarked image even if it is altered or processed by one or more image processing attacks such as compression, filtering, geometric distortions, resizing etc.

In my research work, I have proposed a blind watermarking scheme based on the discrete wavelet transformation (DWT) and theory of linear algebra called “singular value decomposition (SVD)” to digital image watermarking..SVD method can transform A into product of USV , which allow us to refactoring a digital image in three matrixes. The using of singular values of such refactoring allows us to represent the image in the small set of values, which can preserve useful features of the original image, but use less storage space in the memory and achieve a image watermarking process. In this scheme, Singular Values (SV's) were embedded in the HH band of the watermark for perceptual transparency and robustness. Although the scheme proves to be robust however it is insecure. An authentication mechanism is proposed at the decoder for security enhancement. It is implemented by using a signature based authentication mechanism. Finally the resulting water- marking scheme is secure and robust.

TABLE OF CONTENTS

Certificate	2
Acknowledgement.....	3
Abstract	4
Table of Contents.....	5
Notations.....	8
Tables	8
List of Figures.....	9
1 INTORDUCTION.....	10
1.1 Introduction	10
1.2 Hiding Information Digitally.....	11
1.3 History of Watermarking.....	13
1.4 Objectives of this thesis	15
1.5 Organization of Dissertation.....	16
2 DIGITAL IMAGE WATERMARKING.....	18
2.1 Introduction	18
2.2 Structure of a watermarking system	20
2.3 Characteristic features of watermarking.....	24
2.3.1: Imperceptibility.....	24
2.3.2: Robustness	24
2.3.3: Security	26
2.4 Types of digital watermarking System.....	26
2.4.1 Private watermarking.....	27
2.4.2 Semiprivate Watermarking.....	27
2.4.3 Public Watermarking.....	27
2.4.4 Asymmetric & symmetric watermarking	28
2.4.5 Blind Watermarking	28

2.4.6	Steganographic & non-Steganographic watermarking	28
2.5	Distortions and attacks.....	29
2.5.1	Additive Noise.....	30
2.5.2	Filtering	30
2.5.3	Cropping.....	30
2.5.4	Compression.....	30
2.5.5	Rotation and Scaling	31
2.5.6	Statistical Averaging.....	31
2.5.7	Multiple Watermarking.....	32
2.5.8	Wiener Attack.....	32
2.5.9	Attacks at Other Levels.....	33
2.6:	Applications of digital watermarking.....	33
2.6.1	Video Watermarking	33
2.6.2	Audio watermarking.....	34
2.6.3	Hardware/software watermarking	34
2.6.4	Text watermarking.....	34
2.6.5	Executable watermarks.....	35
2.6.6	Labeling	35
2.6.7	Fingerprinting	35
2.6.8	Authentication	35
2.6.9	Copy and playback control.....	36
2.6.10.	Signaling.....	36
3	BACK GROUND STUDY	37
3.1	Wavelet Watermarking Techniques	37
3.1.1:	Continues wavelet transform.....	39
3.1.2	Discrete wavelet Transform.....	41
3.1.3:	Mother Wavelet.....	43
3.1.4:	Comparison with Fourier transform.....	44
3.2	Single Value Decomposition.....	44
3.3	Watermarking Schemes Based On SVD	47

3.2.1 Pure SVD Based Schemes	47
3.2.2 Hybrid SVD Based Schemes	48
4. PROPOSED WATERMARKING SCHEME	49
4.1 Motivation for Proposed Scheme	49
4.2 Proposed Watermarking Scheme	50
4.2.1 Watermark Embedding Algorithm	50
4.2.2 Watermark Extraction Algorithm	51
4.3 Authentication Issues in the Proposed Scheme	51
4.3.1 Generation of Signature	53
4.3.2 Proposed Authentication Scheme	53
5. EXPERIMENTAL RESULTS	56
5.1 Experimental Setup	56
5.1.1 Tools and Software Used	58
5.2 Experiments	58
5.2.1 To Check Perceptual Quality	59
5.2.2 To Check Robustness	59
5.2.2.1 JPEG Compression.	60
5.2.2.2 Median Filtering.	61
5.2.2.3 Histogram Equalization.	62
5.2.2.4 Noise Addition.	62
5.2.2.5 Rotation.	63
5.2.2.6 Scaling.	64
5.2.2.7 Cropping.	65
5.2.2.8 Print & Scan Attack.	66
5.2.3 To Check Authenticity	67
5.3 Comparison with Existing Approaches	68
6 Conclusions and Future Work	74
7. BIBLIOGRAPHY.	75

NOTATIONS USED

SVD: Single Value Decomposition

DWT: Discrete Wavelet Transform

HH,LL : Higher frequency band and low frequency band

HL,LH: Middle Frequency Band

TABLES

Table 3.1 Various attacks on Lena image, its singular values

Table 4.1: Singular Values of HH Frequency Band of Different Test Images

Table 5.1: PSNR of Watermarked Test Images Image PSNR(in dB)

Table 5.2: Recovered Signature Bits

Table 5.3: Comparison Between Proposed & Existing Scheme

Table 5.4: Recovered Watermark and Correlation Coefficient with Original Watermark

LIST OF FIGURES

- Figure 1.1- Information hiding technique
- Figure 2.1 - Illustration of a Stenographic System
- Figure 2.2 - Block diagram of a watermarking system
- Figure 2.3: Watermark insertion unit
- Figure 2.4: Original 'Lena' image and Perceptual Mask of the image
- Figure 2.5: Watermark detection and extraction unit
- Figure 2.6 Types of watermarking
- Figure 3.1 Types of wavelets
- Figure 3.2 D4 wavelet
- Figure 4.1: Embedding of Watermark
- Figure 4.2: Extraction of Watermark
- Figure 5.1: Gray Scale Test Images (512X512)
- Figure 5.2: Sample Gray Scale Watermark (256X256)
- Figure 5.3: Performance Comparison Among different H/W Operating Environment
- Figure 5.4: Original & Watermarked Cameraman Image with PSNR=43.3374dB
- Figure 5.5: Result of JPEG Compression(90%)
- Figure 5.6 Result of JPEG Compression (50%)
- Figure 5.7 Result of JPEG Compression(1%)
- Figure 5.8: Result of Median Filtering
- Figure 5.9: Result of Histogram Equalization
- Figure 5.10: Result of Adding Gaussian Noise(Mean=0 & Var=0.01)
- Figure 5.11: Result of Adding Salt & Pepper Noise(Mean=0 & Var=0.01)
- Figure 5.12: Result of Rotating Watermarked Image with 15°
- Figure 5.13: Result of Rotating Watermarked Image with 5°
- Figure 5.14: Result of Scale-down Watermarked Image by 50% Figure
- Figure 5.15: Result of Scale-up Watermarked Image by 200%
- Figure 5.14: Result of Cropping
- Figure 5.15: Result of Print & Scan Attack

Chapter 1

INTRODUCTION

1.1 INTRODUCTION

Fast growth of digital technologies has enhanced the ways of access to digital information. These new technologies allow us to store, transfer and processing of digital content with fewer time complexities and additional efficiency. Along with the fiery enlargement of the Internet not only attractive new possibilities - like publicly obtainable access to information databases around the world, distributed project work crosswise different countries, or quick and reliable means of electronic communication emerged, but the easiness of digital media can be duplicated and modified, or the truth that legislation is seemingly powerless to cope with its fast rate of change makes it also extremely attractive to people with dishonorable motives.

Digital watermarking exploits the limitation of the human visual system (HVS). Digital watermarking includes many techniques that are used to imperceptibly communicate information by embedding it into the cover data. With these advantages it also leads to illegal reproduction and distribution of digital content. Now a days Internet is the best way, to flow illegal or unauthenticated digital content without disclosing the identity.

It increases the risk of violating the copyrights of the real holder and authenticity of any digital content. One way to protect digital content against illegal reproduction and distribution is to embed some additional information called digital signature or copyright label or watermark without affecting the perceptual quality of the digital content. This information should embed into the digital content in such a way that no malicious or unauthorized person can decode or use it. Encryption alone often is not sufficient to protect digital content, since unconsidered and erroneous usage by human operators often renders it useless. The most basic forms of information hiding can actually be considered to be highly crude forms of private-key cryptography; the “key” in this case being the knowledge of the method being employed (security through

obscurity). The use of an open medium like Internet increase to concerns about protection and enforcement of intellectual property rights of the digital content used in the transaction.

In addition, unauthorized replication and manipulation of digital content is relatively trivial and can be done using inexpensive tools, unlike the traditional analog multimedia content. The protection and enforcement of intellectual property rights for digital media has become an important issue. In recent years, the research community has seen much activity in the area of digital watermarking as an additional tool in protecting digital content. Watermarking refers to the embedding of an indiscernible ID in the data which identifies the owner or the recipient of the data.

Fingerprinting does not mean cryptographically hashing the data into a signature that can be used to identify the data uniquely. The embedded ID can be detected and decoded from a fingerprinted data whenever and wherever the data is encountered. This process can be achieved through the use of digital watermarking techniques. This becomes particularly important as the technological disparity between individuals and organizations grows. Governments and businesses typically have access to more powerful systems and better encryption algorithms than individuals. Hence, the chance of individual's messages being broken increases which each passing year. Reducing the number of messages intercepted by the organizations as suspect will certainly help to improve privacy.

1.2 Hiding Information Digitally

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. This situation is, however, changing rapidly and the first academic conference on this topic was organized in 1996.

The main driving force is concern over protecting copyright; as audio, video and other works become available in digital form, the ease with which perfect copies can be made may lead to large-scale unauthorized copying, and this is of great concern to the music, film, book and software publishing industries. At the same time, moves by various

governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

The general model of hiding data in other data can be described as follows. The embedded data is the message that one wishes to send secretly. It is usually hidden in an innocuous message referred to as a cover-text, or cover- image or cover-audio as appropriate, producing the stego-text or other stego-object. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data to parties who know it (or who know some derived key value).

As the purpose of steganography is having a covert communication between two parties whose existence is unknown to a possible attacker, a successful attack consists in detecting the existence of this communication. Copyright marking, as opposed to steganography, has the additional requirement of robustness against possible attacks. In this context, the term 'robustness' is still not very clear; it mainly depends on the application. Copyright marks do not always need to be hidden, as some systems use visible digital watermarks, but most of the literature has focused on invisible (or transparent) digital watermarks which have wider applications.

Visible digital watermarks are strongly linked to the original paper watermarks which appeared at the modern visible watermarks may be visual patterns (e.g., a company logo or copyright sign) overlaid on digital images. In the literature on digital marking, the stego-object is usually referred to as the marked object rather than stego-object. We may also qualify marks depending on the application.

Fragile watermarks are destroyed as soon as the object is modified too much. This can be used to prove that an object has not been 'doctored' and might be useful if digital images are used as evidence in court. Robust marks have the property that it is infeasible to remove them or make them useless without destroying the object at the same time. This usually means that the mark should be embedded in the most perceptually significant components of the object. Authors also make the distinction between various types of robust marks. Fingerprints (also called labels by some authors) are like hidden serial numbers which enable the intellectual property owner to identify which customer

broke his license agreement by supplying the property to third parties. Watermarks tell us who the owner of the object is.

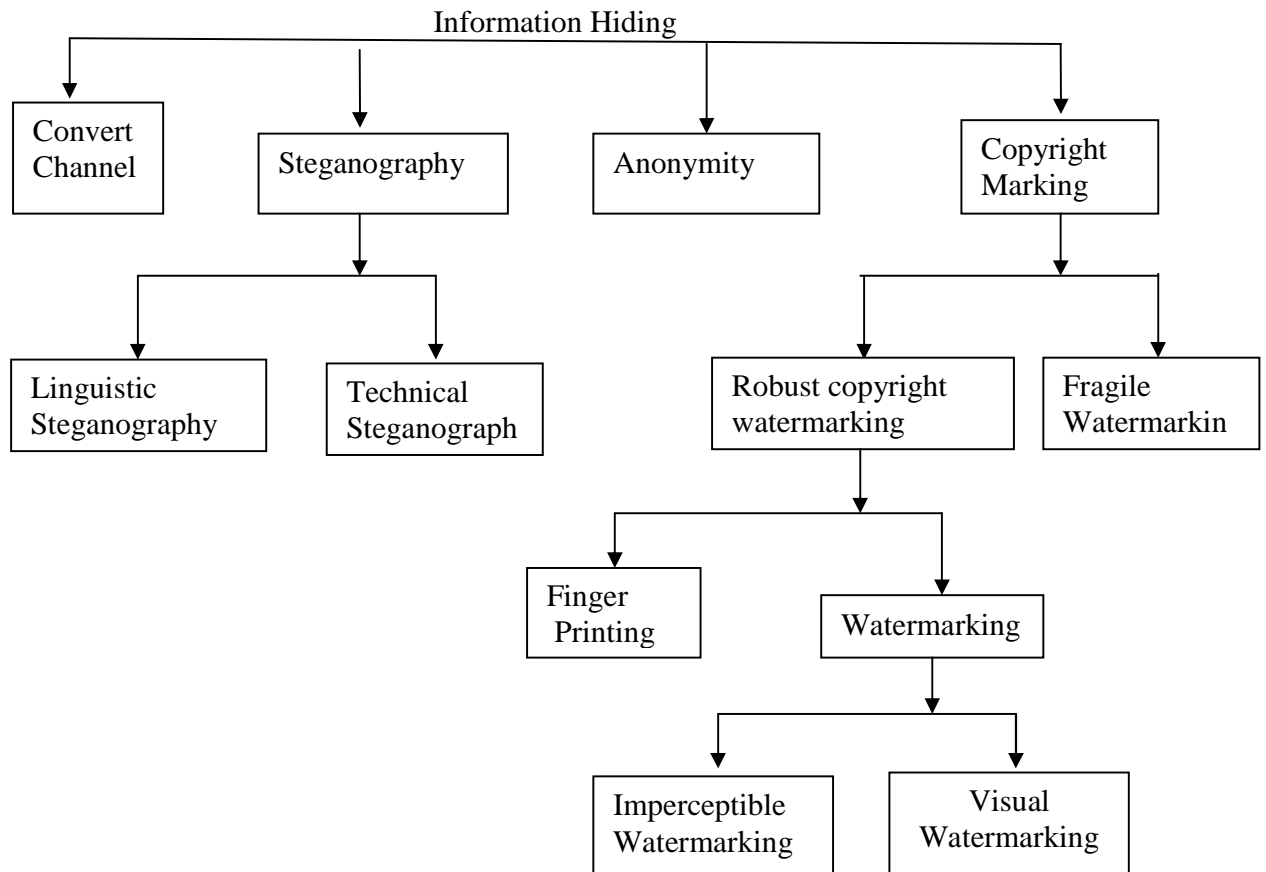


Figure 1.1 Types of Information Hiding

1.3 HISTORY OF WATERMARKING

The core principles of watermarking and data hiding can be traced back approximately 4,000 years to Egypt and Greece. At this time, hidden packets of information had been transferred by special character adjustments or mutations (Hanjalic et al., 2000). Herodotus, the great Greek storyteller, often refers to the hidden information methodology transferred on wax tablets or smuggling secret messages tattooed on the skull of human messengers (Cox et al., 2002).

In Roman times a slave would have his head shaved, then tattooed with an important message, and as the hair began growing, he made his way as instructed through enemy lines and indifferent countries, across water and inhospitable terrain, sleet and snow, mountain ranges, etc. Finally reaching the reader who immediately had the head shaved, and eagerly scanned the message.

The art of papermaking was invented in China over one thousand years earlier, paper watermarks did not appear until about 1282, in Italy. The marks were made by adding thin wire patterns to the paper molds. The paper would be slightly thinner where the wire was and hence more transparent. The meaning and purpose of the earliest watermarks are uncertain. They may have been used for practical functions such as identifying the molds on which sheets of papers were made, or as trademarks to identify the papermaker. On the other hand, they may have represented mystical signs, or might simply have served as decoration.

The United States Constitution states that “The Congress shall have Power to promote the progress of Science and useful Arts, by securing for limited times to Authors and Inventors the exclusive right to their respective writings and discoveries.” The origin of this concept, but not of the noble sentiment of promoting progress in the arts and sciences, in the Anglo-American legal system (similar restrictions also existed in France) stems from a royal charter granted by Mary Tudor, Queen of England, to the Stationer’s Company in 1557.

This charter limited the right to print books to the members of the company. The intent behind this privilege was primarily to exert censorship, the commercial interests of the publishers were of secondary interest only. Even after the repealing of the 1662 Licensing Act in 1681, the Stationer’s Company retained control over the printing trade through the use of a bylaw establishing rights of ownership for books registered to its members. This common law mechanism was supplanted in 1710 by the Statute of Anne enacted in 1709. The Act of Parliament granted authors copyright over their work initially for 14 years and was the first copyright legislation in the current sense, in most European states the rights of the authors were recognized only partially until the French Revolution. Cryptography and

steganography have been used throughout history as means to add secrecy to communications especially during the times of war and peace.

Some of the early methods to hide information include text written on wax-covered tablets, invisible writing using invisible ink. In World War II null ciphers were used in which the secret was camouflaged in an innocent sounding message as in the example below. Apparently neutral's protest is thoroughly discounted and ignored. Islam hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suet and vegetable oils.

Taking the second letter in each word the following message emerges:

Pershing sails from NY June 1

As technology developed and detection methods improved, more effective methods of hiding information were developed. The Germans invented microdot technology for covert communication in 1941. In microdots, the messages were neither hidden nor encrypted but their size was too small to be seen by the naked eye. Advances in microdot technology still continue to this day, the latest development being the embedding of a message in a strand of DNA by the use of the technique of genomic steganography.

With the advent of the internet, steganography has found new applications. But, at the same time it is also vulnerable to more powerful attacks since the medium is relatively insecure. To overcome this limitation, watermarking comes into picture. The main difference between the two techniques is the superior robustness capability of watermarking schemes.

This will be clearer in the following sections which explain the basic concepts of cryptography, steganography and watermarking. It also lists some of the most common applications of watermarking in today's world

1.4 Objectives of this thesis

The Objectives of this thesis are as follows:

- To develop an image watermarking scheme which must be robust against different type of image processing attacks such as compression filtering,

histogram equalization and geometrical attacks but the main emphasis is to make the scheme resilient against Print & Scan attack.

- To develop a secure image watermarking scheme against unauthorized watermark detection.
- To develop a blind image watermarking scheme in nature. It should not require original content for watermark detection at receiver side.

1.5 Organization of Dissertation

This report will begin with a quick background on cryptography and steganography, which form the basis for a large number of digital watermarking concepts. Then we move on to concept of discrete wavelet transformation (DWT) and theory of linear algebra called “singular value decomposition (SVD)” to digital image watermarking.

Chapter 1 gives the introduction about the digital image watermarking; it explains the basic watermarking related to this project. This chapter gives the history of watermarking, information hiding, and stenography. This chapter explains about the different techniques of information hiding. The last part gives the objective of this thesis and structure of report.

Chapter 2 is concerned about the review of the related literature required for the project. This chapter gives the Structure of a watermarking system, Characteristic features of watermarking, Types of digital watermarking System, Distortions and attacks. The last part of the Chapter 2 gives an overview of applications of the digital watermarking techniques.

Chapter 3 gives the basic idea about watermarking techniques purpose and attribute of watermark image. It includes spatial, frequency and wavelet domain watermarking techniques. The next part of the Chapter 3 gives the basic idea of theory of linear algebra technique called “singular value decomposition (SVD)” for digital image watermarking.

Chapter 4 It explain the .proposed watermarking scheme and method for the authentication for the proposed scheme based on SVD (Single Value Decomposition) and Wavelet transform of digital images.

Chapter 5 shows the different experimental result after applying the proposed technique. It also compares this technique with the other proposed technique using experimental results. These different results are processed by MATLAB software programming.

Chapter 6 discusses about the conclusion and future directions in this project.

Chapter 7 shows the Bibliography which is used for making this report.

Chapter 2

DIGITAL IMAGE WATERMARKING

2.1 INTRODUCTION

Digital watermarking technique is one of most important methods in information hiding and IPR (Intelligence Properties Right) protection and authentication. It is the process of embedding information into a digital signal *in a way that is difficult to remove*. The process of embedding a certain piece of information (technically known as watermark) into multimedia content including text documents, images, audio or video streams, such that the watermark can be detected or extracted later to make an assertion about the data

In *visible* digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark.

In *invisible* digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal).

Information hiding (or data hiding) is a general term encircling a wide range of problems beyond the embedding messages in content. The term hiding can refer to either for information imperceptibility (watermarking) or information secrecy (steganography). Watermarking and steganography are two important sub disciplines of information hiding that are closely related to each other and may be coincide but with different underlying properties, requirements and designs, thus result in different technical solutions . Steganography is a term derived from the Greek words steganos, which means “covered,” and graphia, which means “writing.” It is the art of concealed communication.

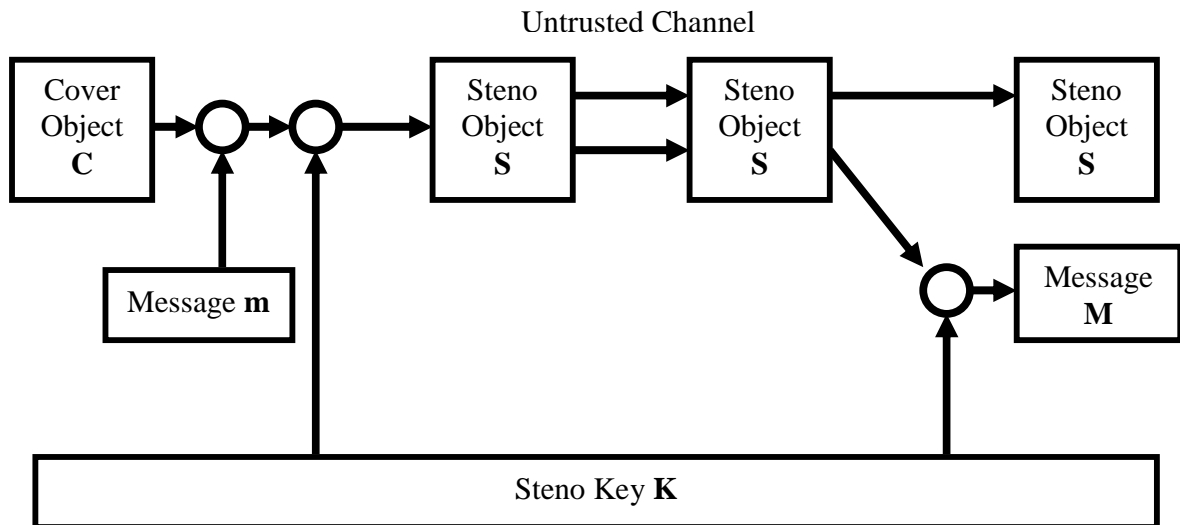


Figure 2.1- Illustration of a Stenographic System

The existence of a message is secret. Watermarking was once considered to be a promising solution however; the techniques are still far from practical. It is difficult to make it commercial in the near future as although many watermarking companies exist at present, none of them seem profitable for the moment. It is worth to mention that the author observes different opinions and beliefs of predicting the future trends of digital watermarking field. However, the author believes that digital watermarking is a potential multi-discipline field that opens up more opportunities in parallel with the technology advancement. This is due to reasons listed below:

- There are always trade-offs between security, robustness and economic constraints in designing digital watermarking systems.
- Digital watermarking needs collective concepts from fields like computer science, signal processing and communications along with human psycho-visual analysis, multimedia and computer graphics.
- Digital watermarking is distinctive based upon its applications, requirements, techniques implemented and attacks applied on them.
- Due to both business and academic interests, digital watermarking serves as a ground for commercial solutions and collective research and discovery.

- Considerable progress includes perceptual modeling, implementations, security threats and countermeasures gives possibilities for further research, with new requirements and future challenges.

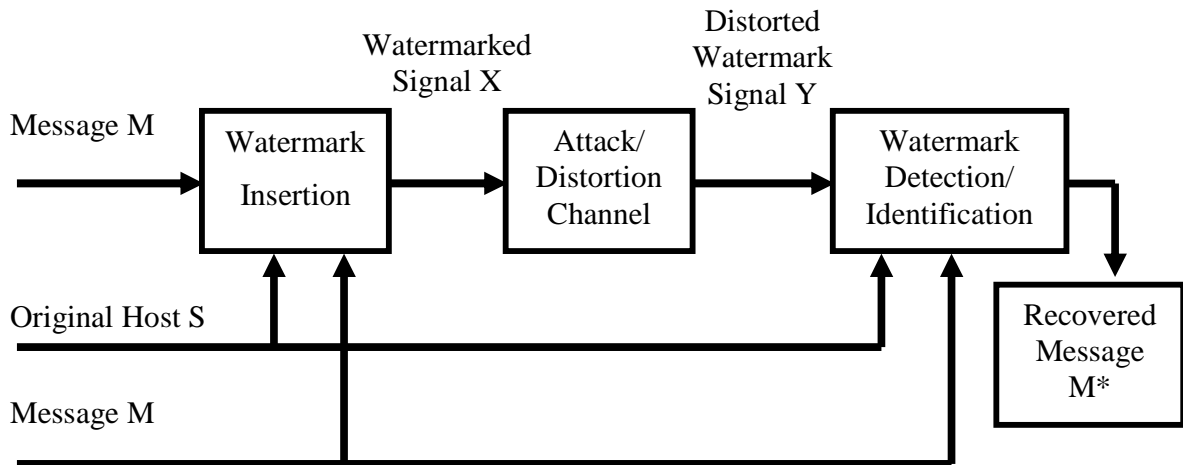


Figure 2.2 - Block diagram of a watermarking system

Watermarking is defined as the practice of imperceptibly altering a Work to embed a message about that Work and Steganography is defined as the practice of undetectably altering a Work to embed a secret message. Figure 2.2 shows the basic block diagram of a watermarking system.

2.2: STRUCTURE OF A WATERMARKING SYSTEM

Every watermarking system consists at least of two different parts: watermark embedding unit and watermark detection and extraction unit. Figure 2.3 shows an example of embedding unit for still images. The unmarked image is passed through a perceptual analysis block that determines how much a certain pixel can be altered so that the resulting watermarked image is indistinguishable from the original. This takes into account the human eye sensitivity to changes in flat areas and its relatively high tolerance to small changes in edges. After this so-called perceptual-mask has been computed, the information to be hidden is shaped by this mask and spread all over the original image.

This spreading technique is similar to the interleaving used in other applications involving coding, such as compact disc storage, to prevent damage of the information caused by scratches or dust. In our case, the main reason for this spreading is to ensure that the hidden information survives cropping of the image. Moreover, the way this spreading is performed depends on the secret key, so it is difficult to recover the hidden information if one is not in possession of this key. Additional key-dependent uncertainty can be introduced in pixel amplitudes (recall that the perceptual mask imposes only an upper limit). Finally, watermark is added to the original image.

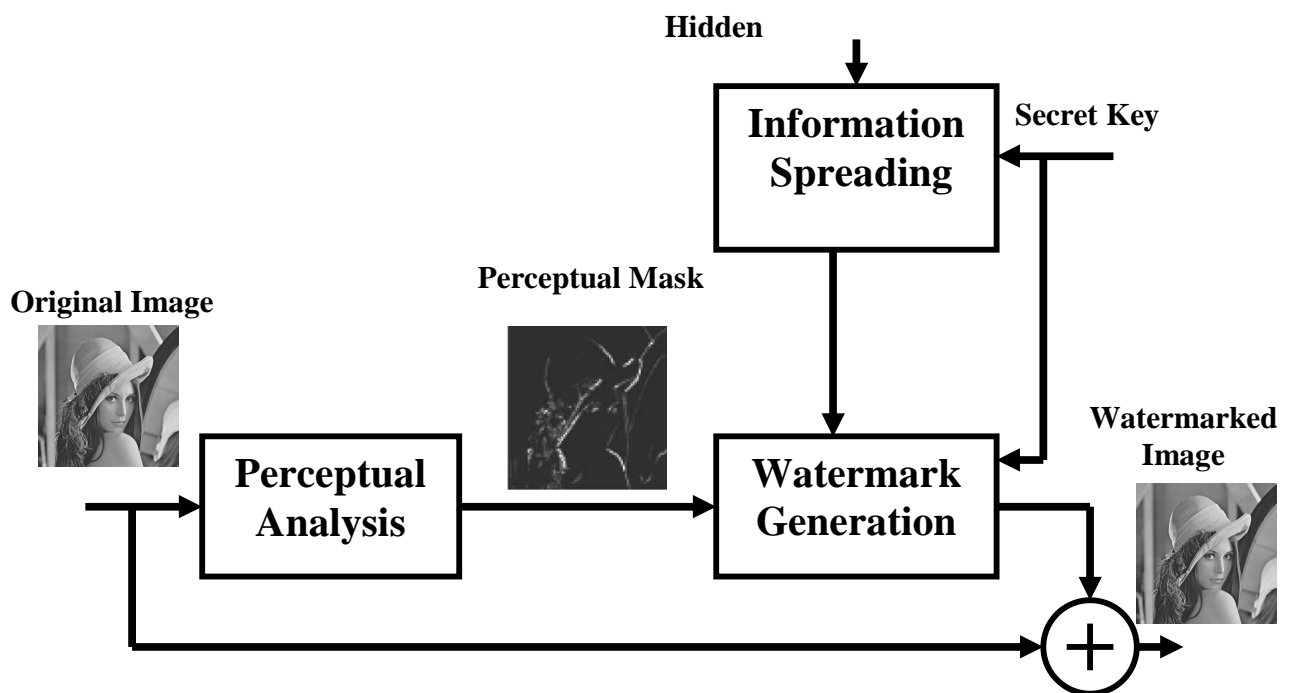


Figure 2.3: Watermark insertion unit

Figure 2.4 represents the perceptual mask that results after analyzing the image presented in Figure 2.4. Higher intensity (i.e., whiter) levels imply that higher perturbations can be made at those pixels without perceptible distortion. Thus, the higher capacity areas for hiding information correspond to edges.



Figure 2.4: Original 'Lena' image and Perceptual Mask of the image

These masks are computed by using some known results on how the human eye works in the spatial domain. Different results are obtained when working on other domains, such as the DCT (Discrete Cosine Transform) or Wavelet transform. In fact, when working on the DCT coefficients domain one may take advantage of the relative independence between the maximum allowable perturbations at every coefficient. This is useful when dealing with the mask for watermarking purposes.

Above, Figure 2.5 shows the typical configuration of a watermark detection and extraction unit. Watermark detection involves deciding whether a certain image has been watermarked with a given key. Note then that a watermark detector produces a binary output. Important considerations here are the probability of correct detection PD (i.e., the probability of correctly deciding that a watermark is present) and the probability of false alarm PF (i.e., the probability of incorrectly deciding that an image has been watermarked with a certain key). These two measures allow us to compare different watermarking schemes: One method will be superior if achieves a higher PD for a fixed PF. Note also that for a watermarking algorithm to be useful it must work with extremely low probabilities of false alarm.

Watermark detection is usually done by correlating the watermarked image with a locally generated version of the watermark at the receiver side. This correlation yields a high value when the watermark has been obtained with the proper key. It is possible to

improve the performance of the detector by eliminating original image-induced noise with signal processing. It is worthy of remark that some authors, like Cox I.J. in [1], propose using the original image in the detection process.

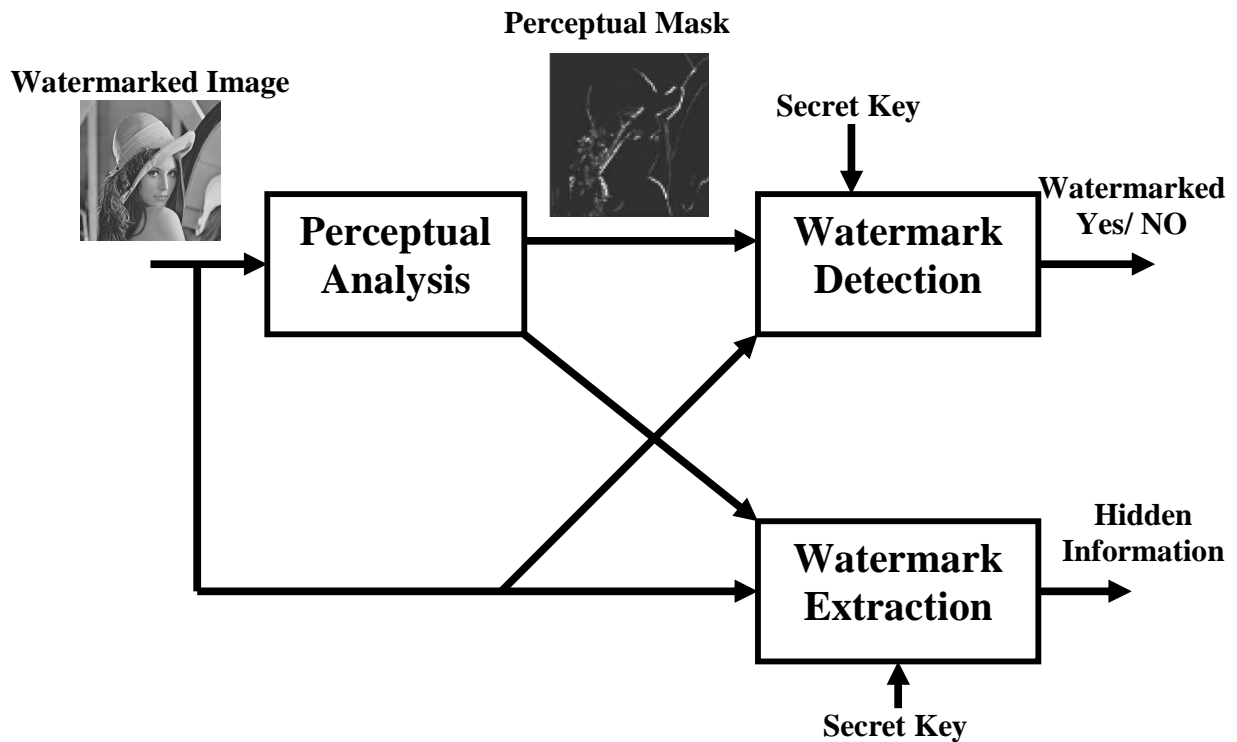


Figure 2.5: Watermark detection and extraction unit

Once the presence of the watermark has been correctly detected, it is possible to extract the hidden information. The procedure is also generally done by means of a cross-correlation but in this case, an independent decision has to be taken for every information bit with a sign slicer. In fact, I.J. Cox et al. [1] have also shown that this correlation structure has not been well-founded and significant improvements are achievable when image statistics are available. For instance, the widely-used DCT coefficients used in the JPEG and MPEG-2 standards are well approximated by generalized Gaussian probability density functions that yield a considerably different extraction scheme. Obviously, when extracting the information the most adequate parameter for comparison purposes is the probability of bit error P_b , identical to that used in digital communications. This is not

surprising because watermarking creates a hidden (also called steganographic) channel on which information is conveyed.

2.3 CHARACTERISTIC FEATURES OF WATERMARKING

As mentioned earlier, digital watermarking techniques are useful for embedding metadata in multimedia content. There are alternate mechanisms like using the header of a digital file to store meta-information. However, for inserting visible marks in images & video and for adding information about audio at the beginning or end of the audio clip etc. the digital watermarking technique is appealing, since it provides following main features and does not require out-of-band data as in other mechanisms.

2.3.1 Imperceptibility:

The embedded watermarks are imperceptible both perceptually as well as statistically and do not alter the aesthetics of the multimedia content that is watermarked. The watermarks do not create visible artifacts in still images, alter the bit-rate of video or introduce audible frequencies in audio signals. The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.

2.3.2 Robustness:

Depending on the application, the digital watermarking technique can support different levels of robustness against changes made to the watermarked content. If digital watermarking is used for ownership identification, then the watermark has to be robust against any modifications. The watermarks should not get degraded or destroyed as a result of unintentional or malicious signal and geometric distortions like analog-to-digital conversion, digital-to-analog conversion, cropping, re-sampling, rotation, dithering, quantization, scaling and compression of the content. On the other hand, if digital watermarking is used for content authentication, the watermarks should be fragile, i.e., the watermarks should get destroyed whenever the content is modified.

The watermark must be difficult (hopefully impossible) to remove. If only partial knowledge is available (for example, the exact location of the watermark in an image is unknown), then attempts to remove or destroy a watermark should result in severe degradation in fidelity before the watermark is lost. In particular, the watermark should be robust in the following areas:

- **Inseparability** - After the digital content is embedded with watermark, separating the content from the watermark to retrieve the original content is not possible.
- **Common Signal Processing** - The watermark should still be retrievable even if common signal processing operations are applied to the data. These include, digital-to-analog and analog-to-digital conversion, re-sampling, re-quantization (including dithering and recompression), and common signal enhancements to image contrast and color, or audio bass and treble, for example.
- **Common Geometric Distortions** - Watermarks in image and video data should also be immune from geometric image operations such as rotation, translation, cropping and scaling.
- **Subterfuge Attacks (Collusion and Forgery)** - In addition, the watermark should be robust to collusion by multiple individuals who each possess a watermarked copy of the data. That is, the watermark should be robust to combining copies of the same data set to destroy the watermarks. Further, if a digital watermark is to be used in litigation, it must be impossible for colluders to combine their images to generate a different valid watermark with the intention of framing a third party.
- **Universality** - The same digital watermarking algorithm should apply to all three media under consideration. This is potentially helpful in the watermarking of multimedia products. Also, this feature is conducive to implementation of audio and image/video watermarking algorithms on common hardware.

- **Unambiguousness** - Retrieval of the watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification should degrade gracefully in the face of attack.

2.3.3 Security:

The digital watermarking techniques prevent unauthorized users from detecting and modifying the watermark embedded in the cover signal. Watermark keys ensure that only authorized users are able to detect/modify the watermark. Finally, the watermark should withstand multiple watermarking to facilitate traitor tracing.

In general, a digital watermark should have several different properties. The most important are imperceptibility, robustness and security. Imperceptibility means that the watermarked data should be perceptually equivalent to the original, un-watermarked data. In some applications, the watermark may be perceptible as long as it is not annoying or obtrusive; however, many applications require that the watermark be imperceptible. Security means that unauthorized parties should not be able to detect or manipulate the watermark. Cryptographic methods are typically employed to make watermarks secure. Finally, robustness means that, given the watermarked data, one should not be able to make the watermark undetectable without also destroying the value or usefulness of the data.

Another characteristic of a watermarking scheme is whether or not the original data is available during detection. In some schemes [1], the watermark detector has access to the original data. Hence, interference from the original can presumably be eliminated. Blind schemes do not have the luxury of using the original during watermark detection. They typically apply some pre-processing to the received data to suppress interference from the original.

2.4 TYPES OF WATERMARKING

There are several types of robust copyright marking systems. They are defined by their inputs and outputs:

2.4.1 Private watermarking

Private watermarking systems are also called non-blind watermarking. In this watermarking system, the original image is required during detection. There are two types of systems i.e. Type I and Type II. In type I systems the mark M is extracted from the possibly distorted image Y and use the original image as a hint to find where the mark could be in Y ($Y * I * K \rightarrow W$). Type II systems also require a copy of the embedded mark for extraction and just yield a 'yes' or 'no' answer to the question: does Y contain the mark M ? ($Y * I * K * W \rightarrow \{0,1\}$). It is expected that this kind of scheme will be more robust than the others since it conveys very little information and requires access to secret material.

2.4.2 Semiprivate Watermarking

In semi-private watermarking does not use the original image for detection ($Y * I * K * W \rightarrow \{0,1\}$) but answers the same question. The main uses of private and semi-private marking seem to be evidence in court to prove ownership and copy control in applications such as DVD where the reader needs to know whether it is allowed to play the content or not. Many of the currently proposed schemes fall in this category.

2.4.3 Public Watermarking

This scheme is also known as blind watermarking. In this case, the detection process (and in particular the detection key) is fully known to anyone as opposed to private watermarking where a secret key is required. So here, only a public key is needed for verification and a private key (secret) is required for embedding. The knowledge of the public key does not help to compute the private key (at least in reasonable time), it does not either allow removal of the mark nor it allows an attacker to forge a mark. Indeed such systems really extract n bits of information (the mark) from the marked image: ($Y * I * K \rightarrow W$)

2.4.4 Asymmetric & symmetric watermarking

Asymmetric watermarking (also called asymmetric key watermarking) is a technique where different keys are used for embedding and detecting the watermark. It should have the property that any user can read the mark, without being able to remove it. In symmetric watermarking (or symmetric key watermarking), the same keys are used for embedding and detecting watermarks.

2.4.5 Blind Watermarking

Blind watermarking techniques can perform verification of the mark without use of the original image. Other techniques rely on the original to detect the watermark. Many applications require blind schemes; these techniques are often less robust than non blind algorithms.

2.4.6 Steganographic & non-Steganographic watermarking

Steganographic watermarking is a technique where content users are unaware that a watermark is present. In non-steganographic watermarking, the users are aware of the presence of a images are required but one also wants to protect these images after they are resample and used watermark. Steganographic watermarking is used in fingerprinting applications while non- steganographic watermarking techniques can be used to deter piracy.

Another classification of watermarking technique (Yusnita Yusof and Othman O. Khalifa [19]) as shown in figure 2.6.

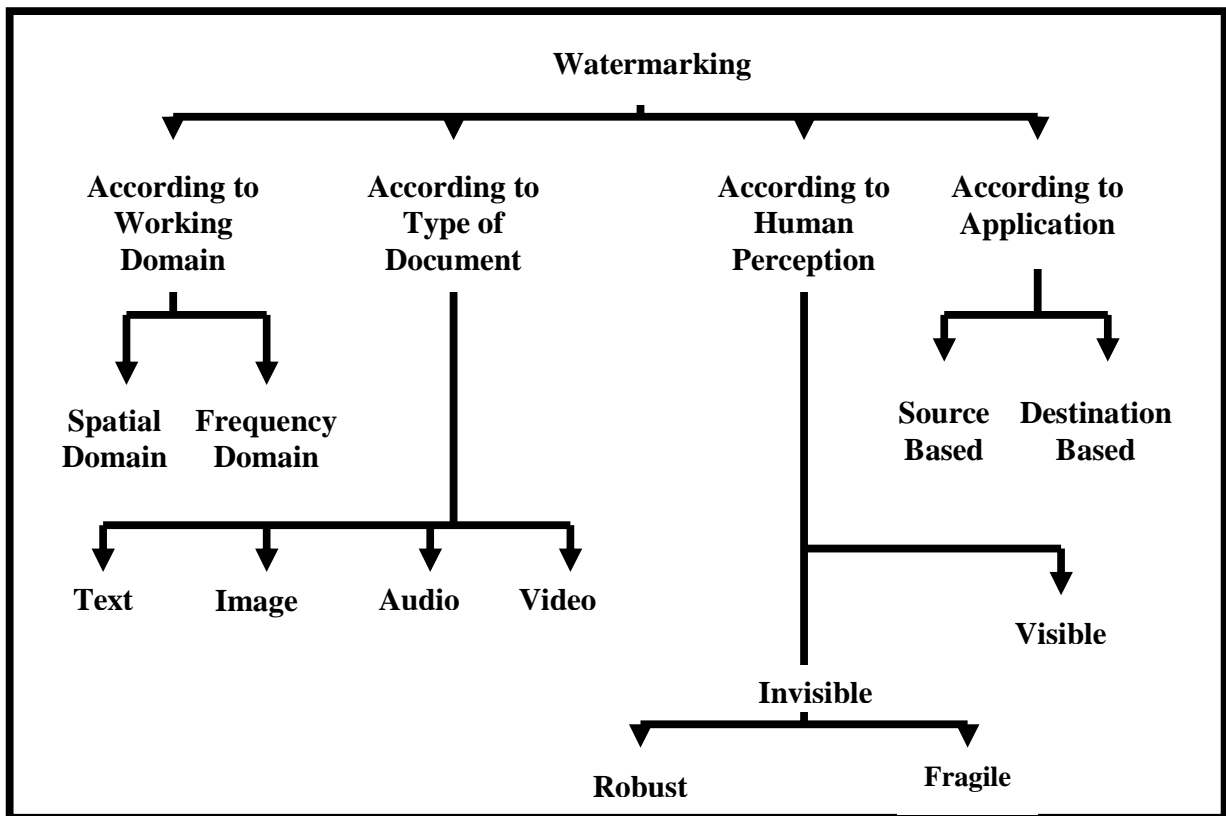


Figure 2.6 Types of watermarking.

2.5 DISTORTIONS AND ATTACKS:

In practice, a watermarked object may be altered either on purpose or accidentally, so the watermarking system should still be able to detect and extract the watermark. Obviously, the distortions are limited to those that do not produce excessive degradations, since otherwise the transformed object would be unusable. These distortions also introduce degradation on the performance of the system. For intentional attacks, the goal of the attacker is to maximize the reduction in these probabilities while minimizing the impact that his/her transformation produces on the object; this has to be done without knowing the value of the secret key used in the watermarking insertion process, which is where all the security of the algorithm lies. Next, we introduce some of

the best known attacks. Some of them may be intentional or unintentional, depending on the application:

2.5.1 Additive Noise:

This may stem in certain applications from the use of D/A and A/D converters or from transmission errors. However, an attacker may introduce perceptually shaped noise (thus, imperceptible) with the maximum unnoticeable power. This will typically force to increase the threshold at which the correlation detector works.

2.5.2 Filtering:

Low-pass filtering, for instance, does not introduce considerable degradation in watermarked images or audio, but can dramatically affect the performance, since spread-spectrum-like watermarks have non negligible high-frequency spectral contents.

2.5.3 Cropping:

This is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of a video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place.

2.5.4 Compression:

This is generally an unintentional attack which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed via Internet have been compressed. If the watermark is required to resist different levels of compression, it is usually advisable to perform the watermark insertion task in the same domain where the compression takes place. For instance, DCT domain

image watermarking is more robust to JPEG compression than spatial-domain watermarking.

2.5.5 Rotation and Scaling:

This has been the true battle horse of digital watermarking, especially because of its success with still images. Correlation based detection and extraction fail when rotation or scaling is performed on the watermarked image because the embedded watermark and the locally generated version do not share the same spatial pattern anymore. Obviously, it would be possible to do exhaustive search on different rotation angles and scaling factors until a correlation peak is found, but this is prohibitively complex. Note that estimating the two parameters become simple when the original image is present, but we have argument against this possibility in previous sections. In [10] the authors have shown that although the problem resembles synchronization for digital communications, the techniques applied there fail loudly. Some authors have recently proposed the use of rotation and scaling-invariant transforms (such as the Fourier-Mellin) but this dramatically reduces the capacity for message hiding. In any case, publicly available programs like Strirmark break the uniform axes transformation by creating an imperceptible non-linear resampling of the image [9] that renders invariant transforms unusable. In audio watermarking it is also quite simple to perform a non-linear transformation of the time axis that considerably difficult watermark detection.

2.5.6 Statistical Averaging:

An attacker may try to estimate the watermark and then ‘unwatermark’ the object by subtracting the estimate. This is dangerous if the watermark does not depend substantially on the data. Note that with different watermarked objects it would be possible to improve the estimate by simple averaging. This is a good reason for using perceptual masks to create the watermark.

2.5.7 Multiple Watermarking:

An attacker may watermark an already watermarked object and later make claims of ownership. The easiest solution is to timestamp the hidden information by a certification authority.

2.5.8 Wiener Attack:

Wiener2 low pass filters a grayscale image that has been degraded by constant power additive noise. Wiener2 uses a pixel wise adaptive Wiener method based on statistics estimated from a local neighborhood of each pixel.

$J = \text{Wiener2}(I, [m\ n], \text{noise})$ filters the image I using pixel wise adaptive Wiener filtering, using neighborhoods of size m -by- n to estimate the local image mean and standard deviation. If you omit the $[m\ n]$ argument, m and n default to 3. The additive noise (Gaussian white noise) power is assumed to be noise.

$[J, \text{noise}] = \text{wiener2}(I, [m\ n])$ also estimates the additive noise power before doing the filtering. Wiener2 returns this estimate in noise.

Wiener2 estimates the local mean and variance around each pixel.

$$\mu = \frac{1}{NM} \sum_{n_1, n_2 \in \eta} a(n_1, n_2)$$

and

$$\sigma^2 = \frac{1}{NM} \sum_{n_1, n_2 \in \eta} a^2(n_1, n_2) - \mu^2$$

Where η the N -by- M local neighborhood of each pixel is in the image A . Wiener2 then creates a pixel wise Wiener filter using these estimates,

$$b(n_1, n_2) = \mu + \frac{\sigma^2 - v^2}{\sigma^2} (a(n_1, n_2) - \mu)$$

Where v^2 is the noise variance. If the noise variance is not given, Wiener2 uses the average of all the local estimated variances.

2.5.9 Attacks at Other Levels:

There are a number of attacks that are directed to the way the watermark is manipulated. For instance, it is possible to circumvent copy control mechanisms discussed below by super scrambling data so that the watermark is lost or to deceive web crawlers searching for certain watermarks by creating a presentation layer that alters the way data are ordered. The latter is sometimes called ‘mosaic attack’.

2.6 APPLICATIONS OF DIGITAL WATERMARKING:

In this section we discuss some of the scenarios where watermarking is being already used as well as other potential applications. The list given here is by no means complete and intends to give a perspective of the broad range of business possibilities that digital watermarking opens.

2.6.1 Video Watermarking:

In this case, most considerations made in previous sections hold. However, now the temporal axis can be exploited to increase the redundancy of the watermark. As in the still images case, watermarks can be created either in the spatial or in the DCT domains. In the latter, the results can be directly extrapolated to MPEG-2 sequences, although different actions must be taken for I, P and B frames. Note that perhaps the set of attacks that can be performed intentionally is not smaller but definitely more expensive than for still images.

2.6.2 Audio Watermarking:

Again, previous considerations are valid. In this case, time and frequency masking properties of the human ear are used to conceal the watermark and make it inaudible. The greatest difficulty lies in synchronizing the watermark and the watermarked audio file, but techniques that overcome this problem have been proposed.

2.6.3 Hardware/Software Watermarking:

This is a good paradigm that allows us to understand how almost every kind of data can be copyright protected. If one is able to find two different ways of expressing the same information, then one bit of information can be concealed, something that can be easily generalized to any number of bits. This is why it is generally said that a perfect compression scheme does not leave room for watermarking. In the hardware context, Boolean equivalences can be exploited to yield instances that use different types of gates and that can be addressed by the hidden information bits. Software can be also protected not only by finding equivalences between instructions, variable names, or memory addresses, but also by altering the order of non-critical instructions. All this can be accomplished at compiler level.

2.6.4 Text Watermarking:

This problem, which in fact was one of the first that was studied within the information hiding area, can be solved at two levels. At the printout level, information can be encoded in the way the text lines or words are separated (this facilitates the survival of the watermark even to photocopying). At the semantic level (necessary when raw text files are provided), equivalences between words or expressions can be used, although special care has to be taken not to destruct the possible intention of the author.

2.6.5 Executable Watermarks:

Once the hidden channel has been created it is possible to include even executable contents, provided that the corresponding applet is running on the end user side.

2.6.6 Labeling:

The hidden message could also contain labels that allow for example to annotate images or audio. Of course, the annotation may also be included in a separate file, but with watermarking it results more difficult to destroy or loose this label, since it becomes closely tied to the object that annotates. This is especially useful in medical applications since it prevents dangerous errors.

2.6.7 Fingerprinting:

This is similar to the previous application and allows acquisition devices (such as video cameras, audio recorders, etc) to insert information about the specific device (e.g., an ID number) and date of creation. This can also be done with conventional digital signature techniques but with watermarking it becomes considerably more difficult to excise or alter the signature. Some digital cameras already include this feature.

2.6.8 Authentication:

This is a variant of the previous application, in an area where cryptographic techniques have already made their way. However, are two significant benefits that arise from using watermarking: first, as in the previous case, the signature becomes embedded in the message, second, it is possible to create 'soft authentication' algorithms that offer a multi-valued 'perceptual closeness' measure that accounts for different unintentional transformations that the data may have suffered (an example is image compression with different levels), instead of the classical yes/no answer given by cryptography-based authentication. Unfortunately, the major drawback of watermarking-based authentication

is the lack of public key algorithms that force either to put secret keys in risk or to resort to trusted parties.

2.6.9 Copy and Playback Control:

The message carried by the watermark may also contain information regarding copy and display permissions. Then, a secure module can be added in copy or playback equipment to automatically extract this permission information and block further processing if required. In order to be effective, this protection approach requires agreements between content providers and consumer electronics manufacturers to introduce compliant watermark detectors in their video players and recorders. This approach is being taken in Digital Video Disc (DVD).

2.6.10 Signaling:

The imperceptibility constraint is helpful when transmitting signaling information in the hidden channel. The advantage of using this channel is that no bandwidth increase is required. An interesting application in broadcasting consists in watermarking commercials with signaling information that permits an automatic counting device to assess the number of times that the commercial has been broadcast during a certain period. An alternative to this would require complex recognition software.

Chapter 3

BACK GROUND STUDY

3.1 Wavelet Watermarking Techniques

A wavelet is a wave-like oscillation with an amplitude that starts out at zero, increases, and then decreases back to zero. It can typically be visualized as a "brief oscillation" like one might see recorded by a seismograph or heart monitor. Generally, wavelets are purposefully crafted to have specific properties that make them useful for signal processing. Wavelets can be combined, using a "shift, multiply and sum" technique called convolution, with portions of an unknown signal to extract information from the unknown signal.

As wavelets are a mathematical tool they can be used to extract information from many different kinds of data, including - but certainly not limited to - audio signals and images. Sets of wavelets are generally needed to analyze data fully. A set of "complementary" wavelets will deconstruct data without gaps or overlap so that the deconstruction process is mathematically reversible. Thus, sets of complementary wavelets are useful in wavelet based compression/decompression algorithms where it is desirable to recover the original information with minimal loss.

In formal terms, this representation is a wavelet series representation of a square-integrable function with respect to either a complete, orthonormal set of basis functions, or an over complete set or Frame of a vector space, for the Hilbert space of square integrable functions.

Wavelet theory is applicable to several subjects. All wavelet transforms may be considered forms of time-frequency representation for continuous-time (analog) signals and so are related to harmonic analysis. Almost all practically useful discrete wavelet transforms use discrete-time filterbanks. These filter banks are called the wavelet and scaling coefficients in wavelets nomenclature. These filterbanks may contain either finite impulse response (FIR) or infinite impulse response (IIR) filters. The wavelets forming a continuous wavelet transform (CWT) are subject to the uncertainty principle of Fourier

analysis respective sampling theory: Given a signal with some event in it, one cannot assign simultaneously an exact time and frequency response scale to that event. The product of the uncertainties of time and frequency response scale has a lower bound. Thus, in the scaleogram of a continuous wavelet transform of this signal, such an event marks an entire region in the time-scale plane, instead of just one point. Also, discrete wavelet bases may be considered in the context of other forms of the uncertainty principle.

Wavelets are mathematical functions that cut up data into different frequency components, and then study each component with a resolution matched to its scale. They have advantages over traditional Fourier methods in analyzing physical situations where the signal contains discontinuities and sharp spikes. Wavelets were developed independently in the fields of mathematics, quantum physics, electrical engineering, and seismic geology. Interchanges between these fields during the last ten years have led to many new wavelet applications such as image compression, turbulence, human vision, radar, and earthquake prediction

The development of wavelets can be linked to several separate trains of thought, starting with Haar's work in the early 20th century. Later work by Dennis Gabor yielded Gabor atoms (1946), which are constructed similarly to wavelets, and applied to similar purposes. Notable contributions to wavelet theory can be attributed to Zweig's discovery of the continuous wavelet transform in 1975 (originally called the cochlear transform and discovered while studying the reaction of the ear to sound),^[4] Pierre Goupillaud, Grossmann and Morlet's formulation of what is now known as the CWT (1982), Jan-Olov Strömberg's early work on discrete wavelets (1983), Daubechies' orthogonal wavelets with compact support (1988), Mallat's multiresolution framework (1989), Nathalie Delprat's time-frequency interpretation of the CWT (1991), Newland's Harmonic wavelet transform (1993) and many others since.

DWT is used for data compression if signal is already sampled, and the CWT for signal analysis. Thus, DWT approximation is commonly used in engineering and computer science, and the CWT in scientific research. Wavelet transforms are now being adopted for a vast number of applications, often replacing the conventional Fourier Transform. Many areas of physics have seen this paradigm shift, including molecular

dynamics, ab initio calculations, astrophysics, density-matrix localization, seismology, optics, turbulence and quantum mechanics. This change has also occurred in image processing, blood-pressure, heart-rate and ECG analyses, DNA analysis, protein analysis, climatology, general signal processing, speech recognition, computer graphics and multiracial analysis. In computer vision and image processing, the notion of scale-space representation and Gaussian derivative operators is regarded as a canonical multi-scale representation.

One use of wavelet approximation is in data compression. Like some other transforms, wavelet transforms can be used to transform data, then encode the transformed data, resulting in effective compression. For example, JPEG 2000 is an image compression standard that uses biorthogonal wavelets. This means that although the frame is over complete, it is a *tight frame* (see types of Frame of a vector space), and the same frame functions (except for conjugation in the case of complex wavelets) are used for both analysis and synthesis, i.e., in both the forward and inverse transform. For details see wavelet compression.

A related use is that of smoothing/denoising data based on wavelet coefficient thresholding, also called wavelet shrinkage. By adaptively thresholding the wavelet coefficients that correspond to undesired frequency components smoothing and/or denoising operations can be performed.

Wavelet transforms are also starting to be used for communication applications. Wavelet OFDM is the basic modulation scheme used in HD-PLC (a powerline communications technology developed by Panasonic), and in one of the optional modes included in the IEEE P1901 draft standard. The advantage of Wavelet OFDM over traditional FFT OFDM systems is that Wavelet can achieve deeper notches and that it does not require a Guard Interval (which usually represents significant overhead in FFT OFDM systems).

3.1.1 Continuous wavelet transform:

In continuous wavelet transforms, a given signal of finite energy is projected on a continuous family of frequency bands (or similar subspaces of the L^p function space

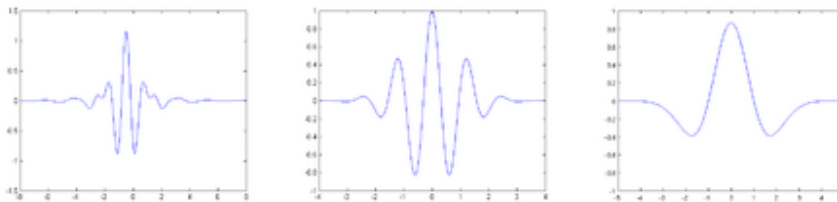
$L^2(\mathbb{R})$). For instance the signal may be represented on every frequency band of the form $[f, 2f]$ for all positive frequencies $f > 0$. Then, the original signal can be reconstructed by a suitable integration over all the resulting frequency components.

The frequency bands or subspaces (sub-bands) are scaled versions of a subspace at scale 1 . This subspace in turn is in most situations generated by the shifts of one generating function $\psi \in L^2(\mathbb{R})$, the *mother wavelet*. For the example of the scale one frequency band $[1, 2]$ this function is

$$\psi(t) = 2 \operatorname{sinc}(2t) - \operatorname{sinc}(t) = \frac{\sin(2\pi t) - \sin(\pi t)}{\pi t}$$

with the (normalized) sinc function. Other example mother wavelets are:

Figure 3.1 Types of wavelets



Meyer

Morlet

Mexican Hat

The subspace of scale a or frequency band $[1/a, 2/a]$ is generated by the functions (sometimes called *child wavelets*)

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}} \psi\left(\frac{t-b}{a}\right),$$

where a is positive and defines the scale and b is any real number and defines the shift.

The pair (a, b) defines a point in the right halfplane $\mathbb{R}_+ \times \mathbb{R}$.

The projection of a function x onto the subspace of scale a then has the form

$$x_a(t) = \int_{\mathbb{R}} WT_{\psi}\{x\}(a, b) \cdot \psi_{a,b}(t) db$$

with *wavelet coefficients*

$$WT_{\psi}\{x\}(a, b) = \langle x, \psi_{a,b} \rangle = \int_{\mathbb{R}} x(t) \overline{\psi_{a,b}(t)} dt$$

See a list of some Continuous wavelets.

For the analysis of the signal x , one can assemble the wavelet coefficients into a scaleogram of the signal.

3.1.2 Discrete wavelet Transform

It is computationally impossible to analyze a signal using all wavelet coefficients, so one may wonder if it is sufficient to pick a discrete subset of the upper halfplane to be able to reconstruct a signal from the corresponding wavelet coefficients. One such system is the affine system for some real parameters $a > 1$, $b > 0$. The corresponding discrete subset of the halfplane consists of all the points $(a^m, n a^m b)$ with integers $m, n \in \mathbb{Z}$. The corresponding *baby wavelets* are now given as

$$\psi_{m,n}(t) = a^{-m/2} \psi(a^{-m}t - nb).$$

A sufficient condition for the reconstruction of any signal x of finite energy by the formula

$$x(t) = \sum_{m \in \mathbb{Z}} \sum_{n \in \mathbb{Z}} \langle x, \psi_{m,n} \rangle \cdot \psi_{m,n}(t)$$

is that the functions $\{\psi_{m,n} : m, n \in \mathbb{Z}\}$ form a tight frame of $L^2(\mathbb{R})$.

Multiresolution discrete wavelet transforms

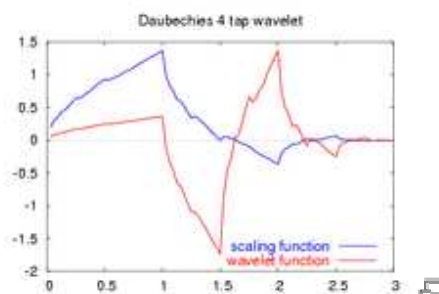


Figure 3.2 D4 wavelet

In any discretised wavelet transform, there are only a finite number of wavelet coefficients for each bounded rectangular region in the upper halfplane. Still, each coefficient requires the evaluation of an integral. To avoid this numerical complexity, one needs one auxiliary function, the *father wavelet* $\phi \in L^2(\mathbb{R})$. Further, one has to restrict a to be an integer. A typical choice is $a=2$ and $b=1$. The most famous pair of father and mother wavelets is the Daubechies 4 tap wavelet.

From the mother and father wavelets one constructs the subspaces

$$V_m = \text{span}(\phi_{m,n} : n \in \mathbb{Z}), \text{ where } \phi_{m,n}(t) = 2^{-m/2}\phi(2^{-m}t - n)$$

and

$$W_m = \text{span}(\psi_{m,n} : n \in \mathbb{Z}), \text{ where } \psi_{m,n}(t) = 2^{-m/2}\psi(2^{-m}t - n).$$

From these one requires that the sequence

$$\{0\} \subset \dots \subset V_1 \subset V_0 \subset V_{-1} \subset \dots \subset L^2(\mathbb{R})$$

forms a multiresolution analysis of $L^2(\mathbb{R})$ and that the subspaces $\dots, W_1, W_0, W_{-1}, \dots$ are the orthogonal "differences" of the above sequence, that is, W_m is the orthogonal complement of V_m inside the subspace V_{m-1} . In analogy to the sampling theorem one may conclude that the space V_m with sampling distance 2^m more or less covers the frequency baseband from 0 to 2^{-m-1} . As orthogonal complement, W_m roughly covers the band $[2^{-m-1}, 2^{-m}]$.

From those inclusions and orthogonality relations follows the existence of sequences $h = \{h_n\}_{n \in \mathbb{Z}}$ and $g = \{g_n\}_{n \in \mathbb{Z}}$ that satisfy the identities

$$h_n = \langle \phi_{0,0}, \phi_{-1,n} \rangle \text{ and } \phi(t) = \sqrt{2} \sum_{n \in \mathbb{Z}} h_n \phi(2t - n)$$

and

$$g_n = \langle \psi_{0,0}, \phi_{-1,n} \rangle \text{ and } \psi(t) = \sqrt{2} \sum_{n \in \mathbb{Z}} g_n \phi(2t - n)$$

The second identity of the first pair is a refinement equation for the father wavelet ϕ . Both pairs of identities form the basis for the algorithm of the fast wavelet transform.

3.1.3 Mother Wavelet

For practical applications, and for efficiency reasons, one prefers continuously differentiable functions with compact support as mother (prototype) wavelet (functions). However, to satisfy analytical requirements (in the continuous WT) and in general for theoretical reasons, one chooses the wavelet functions from a subspace of the space $L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. This is the space of measurable functions that are absolutely and square integrable:

$$\int_{-\infty}^{\infty} |\psi(t)| dt < \infty \quad \text{And} \quad \int_{-\infty}^{\infty} |\psi(t)|^2 dt < \infty.$$

Being in this space ensures that one can formulate the conditions of zero mean and square norm one:

$$\int_{-\infty}^{\infty} \psi(t) dt = 0 \quad \text{is the condition for zero mean, and}$$

$$\int_{-\infty}^{\infty} |\psi(t)|^2 dt = 1 \quad \text{is the condition for square norm one.}$$

For ψ to be a wavelet for the continuous wavelet transform (see there for exact statement), the mother wavelet must satisfy an admissibility criterion (loosely speaking, a kind of half-differentiability) in order to get a stably invertible transform.

For the discrete wavelet transform, one needs at least the condition that the wavelet series is a representation of the identity in the space $L^2(\mathbb{R})$. Most constructions of discrete WT make use of the multiresolution analysis, which defines the wavelet by a scaling function. This scaling function itself is solution to a functional equation.

In most situations it is useful to restrict ψ to be a continuous function with a higher number M of vanishing moments, i.e. for all integer $m < M$

$$\int_{-\infty}^{\infty} t^m \psi(t) dt = 0.$$

The mother wavelet is scaled (or dilated) by a factor of a and translated (or shifted) by a factor of b to give (under Morlet's original formulation):

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}} \psi \left(\frac{t-b}{a} \right).$$

For the continuous WT, the pair (a,b) varies over the full half-plane $\mathbb{R}_+ \times \mathbb{R}$; for the discrete WT this pair varies over a discrete subset of it, which is also called *affine group*. These functions are often incorrectly referred to as the basis functions of the (continuous) transform. In fact, as in the continuous Fourier transform, there is no basis in the continuous wavelet transform. Time-frequency interpretation uses a subtly different formulation

3.1.4 Comparison with Fourier transforms:

The wavelet transform is often compared with the Fourier transform, in which signals are represented as a sum of sinusoids. The main difference is that wavelets are localized in both time and frequency whereas the standard Fourier transform is only localized in frequency. The Short-time Fourier transform (STFT) is more similar to the wavelet transform, in that it is also time and frequency localized, but there are issues with the frequency/time resolution trade-off. Wavelets often give a better signal representation using Multiresolution analysis, with balanced resolution at any time and frequency.

The discrete wavelet transform is also less computationally complex, taking $O(N)$ time as compared to $O(N \log N)$ for the fast Fourier transform. This computational advantage is not inherent to the transform, but reflects the choice of a logarithmic division of frequency, in contrast to the equally spaced frequency divisions of the FFT(Fast Fourier Transform). It is also important to note that this complexity only applies when the filter size has no relation to the signal size. A wavelet without compact support such as the Shannon wavelet would require $O(N^2)$. (For instance, a logarithmic Fourier Transform also exists with $O(N)$ complexity, but the original signal must be sampled logarithmically in time, which is only useful for certain types of signals.

3.2 SINGLE VALUE DECOMPOSITION:

In recent years Singular Value Decomposition (SVD) become very popular in watermarking schemes due to its simplicity in implementation and some attractive mathematical features of SVD. In this section, a brief description of SVD And its role in

the watermarking field have been discussed. SVD for square matrices was discovered by Beltrami in 1873 and Jordan in 1874, and extended to rectangular matrices by Eckart and Young in the 1930s. It was not used as a computational tool until the 1960s because of the need for sophisticated numerical techniques. In later years, Gene Golub demonstrated its usefulness and feasibility as a tool in a variety of applications. SVD is one of the most useful tools of linear algebra with several applications in image compression, watermarking, and other signal processing areas. In linear algebra, the singular value decomposition (SVD) is a factorization of a real or complex matrix, with many useful applications in signal processing and statistics.

Singular Value Decomposition (SVD) is to be a significant topic in linear algebra by many renowned mathematicians. SVD has any practical and theoretical values; special feature of SVD is that it can be performed on any real (m, n) matrix. Let's say we have a matrix with m rows and n columns, with rank r and $r \leq n \leq m$. Then the A can be factorized into three Matrices.

If A is an $m \times n$ matrix, then SVD of matrix A can be defined as :

$$A = U * S * V^T$$

where U and V are the orthogonal matrices and S is a diagonal matrix as:

$$S = \begin{bmatrix} \sigma_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \sigma_{r+1} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & \sigma_n \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix}$$

Here diagonal elements i.e. σ_i s are singular values and satisfy the following property:

$$\sigma_1 \geq \sigma_2 \dots \geq \sigma_n$$

SVD is popular for the watermarking because:

SVD represent maximum signal energy into as few coefficient as possible.

SVD can be applied to square as well as rectangular images.

The SV's (Singular Values) of an image have very good stability, i.e. SV's do not change rapidly when a small perturbation is added to an image intensity values.

SV's represent algebraic properties which are intrinsic and not visual.

To check the stability of the singular values, an experiment was conducted on 8 bit gray scale 512X 512 Lena image. In this experiment original singular values were compared with singular values after applying various attacks on it. Table 2.1 shows first four singular values of original image and modified image after applying various attacks.

Table 3.1 Various attacks on Lena image, its singular values

Image	S1	S2	S3	S4
Original Image	151.5234	42.2745	36.1516	27.9067
JPEG Compression(Q=20)	151.6007	42.2129	36.0787	27.6894
Rotation(15 Degree)	144.1636	48.0665	39.9409	28.7351
Scaling (512-256-512)	152.1418	42.1731	36.0141	27.7552
Scaling (512-1024-512)	152.7299	42.2633	36.1170	27.8758
Gaussian Noise (M=0, V= 0.01)	158.5279	40.7767	35.4015	27.3755
Salt & Paper Noise (M=0 V=0.01)	152.3987	41.9533	35.8831	27.7077
Median Filter {3X3}	151.2235	42.2745	36.1516	27.9067
Histogram Equalization	151.5234	42.2745	36.1516	27.9067

Table 3.1 shows that after applying various attacks on Lena image, its singular values do not change very much. Because of the stability of singular values, SVD become a popular tool to develop watermarking schemes.

3.3 Watermarking Scheme Based on SVD:

In recent few years several watermarking algorithms have been proposed based on SVD. The main idea of these approaches is to find the SVD of a cover image and then modify its singular values to embed the watermark. Some SVD-based algorithms are purely SVD-based in a sense that only SVD domain is used to embed watermark into image. Recently some hybrid SVD-based algorithms have been proposed where different types of transforms domain including DCT, DWT, etc. have been used with SVD to embed watermark into the cover image. In the following subsection, some of the popular SVD based schemes are discussed with their approaches and results.

3.3.1 Pure SVD Based Schemes:

Many of the earlier algorithms, based on SVD, used to embed the watermark directly into the SVD domain. Liu and Tan[2] proposed an algorithm where the watermark is embedded directly in the SVD domain. This scheme is blind in nature. Results show that this scheme is resilient against compression filtering, cropping but not good against rotation, scaling and print-scan attacks. Instead of applying SVD to the whole image, authors in [3] divided the whole image into the non overlapping blocks and then SVD applied to these blocks. Singular values of these blocks are used to embed the watermark. This scheme gives good result against compression Filtering, noise addition but not good against cropping and geometric attacks.

To make more robust watermarking scheme authors in [4] used spread spectrum technique (SST) with SVD. Authors used two watermarks, one is embedded by spread spectrum technique and second one is embedded by pure SVD based technique. Here SST technique gives Good robustness against compression, rotation, filtering, scaling, print-scan attack and on the other side SVD gives good robustness against noise addition and histogram equalization. Hence here these two techniques become complementary of each other and covered wide range of attacks. This scheme is non-blind in nature.

3.3.2 Hybrid SVD Based Scheme:

The schemes which are applied with or after cascading of any transform domain are called hybrid SVD based schemes. DCT, DWT, FFT are few most popular frequency domains which used with SVD to make watermarking schemes more robust. A hybrid method based on DCT and SVD has been proposed by Liu Quan and Ai Qingson. Authors applied the DCT to the whole cover image and after that DCT coefficient are mapped to the four quadrants using the zig zag sequence. These four quadrants actually represent frequency bands from the lowest to the highest. After this SVD was applied to each quadrant. Singular values of the DCT-transformed visual watermark are then used to modify the singular values of each quadrant of the cover image. Results of this approach are good for compression, filtering, cropping but not very good against geometrical attacks, print-scan attack. This scheme is also computationally very costly as in this scheme DCT coefficient has to rearrange in to the 4 different bands to embed the watermark. This scheme is also on-blind in nature.

A SVD based algorithm using DWT has been presented by Ganic and Eskicioglu which is very similar to the algorithm of Liu Quan and Ai Qingson discussed previously. The cover image is first decomposed by using DWT into four sub bands and SVD is applied to each sub band image. SVD is then applied on the watermark image and the singular values of the cover image are modified with the singular values of the watermark image for embedding process. This scheme gives comparatively good results against all the schemes discussed so far. The only limitation of this scheme is its non-blind detection.

SVD for the development of watermarking schemes is discussed and some of the popular schemes are discussed with their approaches and results. There are many other schemes exists which are based on SVD and they have their own advantages and limitations. Study in this chapter shows that robustness of SVD based watermarking schemes is reasonably good but can be improved further. Robustness can be increased by using suitable combination of the transform domain and SVD. In the next chapter, proposed scheme will be discussed which is based on the SVD.

Chapter 4

PROPOSED WATERMARKING SCHEME

Proposed Watermarking Scheme In this chapter, proposed watermarking scheme is discussed. First, short background of the proposed scheme has been presented and then the detailed algorithm has been described. To make the scheme more reliable and secure, a signature based authentication mechanism is also proposed in the last of this chapter.

4.1: Motivation for Proposed Scheme:

Proposed scheme is based on the cascading of DWT and SVD. DWT will decompose the image into four different frequency bands: LL, HL, LH, and HH band. Here LL band represents low frequency band, HL & LH represent middle frequency bands and HH represents high frequency band respectively. In this scheme HH frequency band is selected to embed the watermark because it contains the finer details of the image and HH band contributes very low energy in the image. Hence human vision system (HVS) can not differentiate the changes made in this band.

The proposed scheme is based on the replacement of singular values of the HH band with the singular values of the watermark. In table 3.1, singular values of the HH band of different test images are given. It is observed that singular values lie between 84 to 173 approximately. If a watermark is selected by the user having singular values within the given range then the energy of the singular values of watermark will be approximately equal to the energy of the singular values of the HH band. Hence the replacement of the singular values will not be effect the perceptual quality of image as the replaced energy is approximately equal to the original energy.

Preprocessing of the watermark can be done by using any image processing tool before embedding the watermark. Watermark used for experimentation in this scheme, having singular values within the range of 150 to 0 and not having much variation with the singular values of the given test images. Watermark size should be equal to the size of

the HH band because this will generate the same number of singular values for replacement.

Table 4.1: Singular Values of HH Frequency Band of Different Test Images

Image	Max	Min
Lenna	142.6490	0
Bubble	84.7352	0
Building	173.2125	0
Cameraman	109.2292	0

4.2: Proposed Watermarking Scheme :

In this section, proposed algorithm for watermark embedding and extraction into the cover image, are presented which are follows:

4.2.1: Watermark Embedding Algorithm:

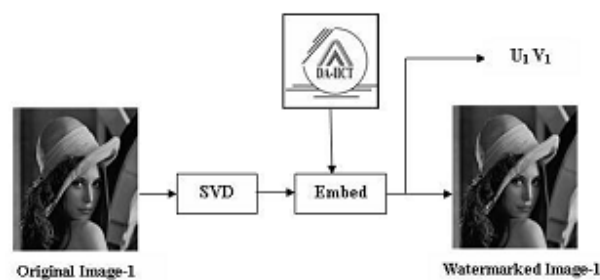
- Read the watermark and apply SVD to it.
- Read the cover image. 3. Using DWT, decompose the cover image into 4 sub-bands:
- LL, HL, LH, and HH with help of Haar Filter
- Apply SVD to HH band.
- Replace the singular values of the HH band with the singular values of the watermark.
- Obtain the modified HH band using inverse SVD.
- Apply the inverse DWT using the modified HH band Coefficient to produce the watermarked cover image.

4.2.2: Watermark Extraction Algorithm:

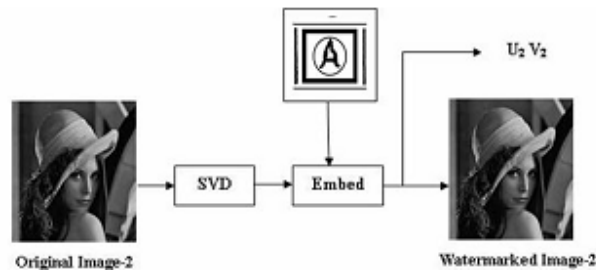
- Read the watermarked image.
- Using DWT, decompose the watermarked image into 4 sub-bands: LL, HL, LH, and HH with help of Haar filter
- Apply SVD to HH band.
- Extract the singular values from HH band.
- Construct the watermark using the extracted singular values of HH band with orthogonal matrices (U and V) from SVD of original watermark.

4.3: Authentication Issues in the proposed Scheme:

Xiao-Ping Zhang and Kan Li [6] observed an authentication issue in the SVD based approaches proposed by the authors in [2,3,5]. Proposed scheme in this chapter is also suffered with the same problem. This section describes the problem of SVD based schemes and a solution to this problem is also proposed in the section. To demonstrate the problem, authors in setup a experiment in which they took two Lena images and two different watermarks as shown in figure. They embedded the watermarks by modifying the singular values of Lena image with the singular values of the watermark respectively.



(a) Case-1



(b)Case-2

Figure 4.1: Embedding of Watermark

Figure 4.1 shows that decoder extracted the SV's from watermarked image-2 and used the orthogonal matrices (U_1 and V_1) of watermark-1. In result, watermark-1 is recovered after applying the inverse SVD. This result shows the contradiction with the expected output.

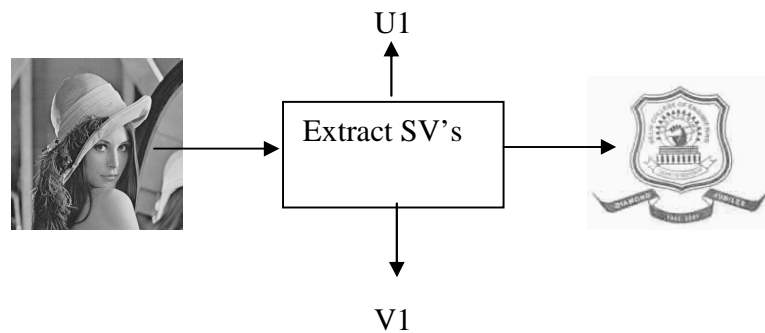


Figure 4.2: Extraction of Watermark

Figure 4.2: Extraction of Watermark Author in [5] explained that the orthogonal matrices preserve the major information of the given matrix as they are the column matrix of eigen vectors of the respective singular values. When inverse SVD is applied, eigen vector matrices plays an important role to construct the original matrix. Hence if wrong singular matrix is applied with orthogonal matrices then it will generate the correlated output matrix instead of the actual output matrix and this correlation will be high if the wrong singular values will be approximately nearly equal to the original singular values. So this problem can be viewed as the false-positive detection of the watermark.

To remove this drawback, a signature based authentication mechanism is proposed in this section. In this orthogonal matrices will be authenticated before applying

to the singular matrix. To implement this a unique signature will be generated for them and embedded with the watermark. Decode will extract the signature first and authenticate the orthogonal matrices before applying to extract the watermark.

This section also presents a algorithm to generate the signature with embedding and extraction algorithm.

4.3.1: Generate Signature:

Digital Signature of the orthogonal matrices is a unique binary string generated through a specified c function. In addition, the digital signature must be secure, so that an attacker cannot predict the signature of given orthogonal matrices. To generate the digital signature for the given matrices, following algorithm is proposed.

Proposed Algorithm

- Sum the column of matrices and stored into a 1-D array.
- Based on the threshold value convert the array values into binary digits.
- By apply XORing we can generate the signature for the given matrices of the desired length. Here threshold value plays an important role for the conversion of decimal values into the binary bits. This threshold value can be kept secret to make this process more secure and reliable.

Proposed Authentication Scheme

To embed the signature, cover image was decomposed into four different frequency bands(LL,LH,HL & HH) by using DWT. LL band represents the maximum energy of any image hence LL band coefficient are very large in magnitude and robust in comparison of other band's coefficient. To get more robust coefficient, LL band is further subdivided up to 4th level by using DWT but these coefficient are perceptually very significant as They can not be modified much otherwise change will reflect in the cover image. Hence the length of the signature is kept very small so that it should not degrade the perceptual quality of the image. LL4 band coefficient shows good robustness against

compression, filtering and geometrical attacks and HH4 band coefficient shows good robustness against histogram equalization and noise addition.

Hence one set of signature bits is embedded into LL4 and another set is embedded into HH4 band to ensure the recovery from at least one band. The algorithm for embedding and extracting the signature is as follows:

4.3.1: Signature Embedding

- Generate the signature for the U and V matrices of watermark of N bits respectively.
- Read the cover image.
- Using DWT, decompose the cover image into 4 sub-bands: LL, HL, LH, and HH with help of Haar filter and further subdivide LL band up to 4th level decomposition.
- Select N random coefficient from LL4 and HH4 band with the help of secret key and convert the integer part into the binary code of L bits.
- Replace the nth bit of the coefficient with signature bit and then convert the binary code into the decimal.
- Apply the inverse DWT using modified LL4 and HH4 band coefficients to embed the signature.

4.3.2 Signature Extraction:

- Read the watermarked image.
- Haar Using DWT, decompose the cover image into 4 sub-bands: LL, HL, LH, and HH with help of Haar filter and further subdivide LL band up to 4th level decomposition.
- Select N random coefficient from LL4 and HH4 band with the help of secret key and convert the integer part into the binary code of L bits.
- Extract the nth bit from the coefficient
- Match the extracted bit pattern with signature of the U and V matrices of the original watermark.

This authentication mechanism is implemented in parallel with the proposed watermarking scheme. The encoder will embed the watermark according to the proposed scheme and also generate the signature for the orthogonal matrices to embed it with the watermark. At receiver side decoder first extracts the signature and match with the original signature. If it satisfies the matching criteria then only decoder decode the watermark according to the proposed algorithm. In the next chapter, experimental results of the proposed scheme are given which will prove its robustness and authenticity.

Chapter 5

EXPERIMENTAL RESULTS

The scheme proposed in chapter 3 is secure and robust against given set of image processing attacks on watermarked image. The correctness and effectiveness of the proposed scheme is verified by using set of experiments. The experimental setup for the proposed scheme and its results with their analysis are presented in this chapter. In the last, results of the proposed scheme are compared with the results of the existing scheme.

5.1 Experimental setup:

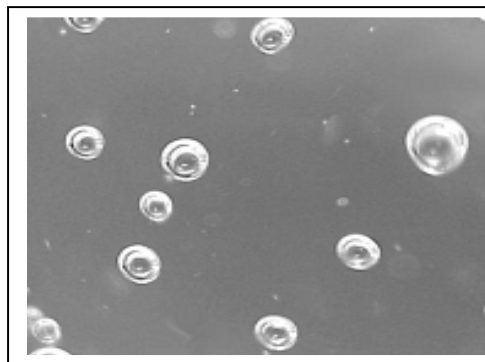
It is important to test an image watermarking scheme on many different images and for fair comparison the same set of sample images should always be used. They should also cover a broad range of contents and types. In our experiments 512X512 8 bit gray scale Lena, Bubble, Cameraman and Building test images were used as a cover image shown in figure 5.1. All the images have different intensity variations and background. We used 256X256 gray scale DA-IICT sample logo as watermark shown in figure5.2. The watermarked images were subjected to various attacks to test the robustness of embedded watermark and the method performance was also compared with the scheme proposed by Ganic and Eskicioglu. Correlation coefficient between recovered and original watermark, was used as a metric for performance evaluation of these methods. The value of correlation coefficient for two images lies between -1 to +1. If two images are absolutely identical then its value will be +1, if they are completely anti correlated (i.e. one image is the negative of other image) then its value will be -1 and its value will be 0 if both the images are totally uncorrelated. The correlation coefficient value in between 0.4 to 0.9 will give the significant similarity between two images.



(a) Building



(b) Lenna



(b) Bubble



(d)Cameraman

Figure 5.1: Gray Scale Test Images(512X512)



Figure 5.2: Sample Gray Scale Watermark (256X256)

5.1.1 Tools and Organization of Dissertation:

All the experimentation and testing performed on Windows-XP platform. MATLAB version-7.7 is used for the implementation of the proposed algorithm.

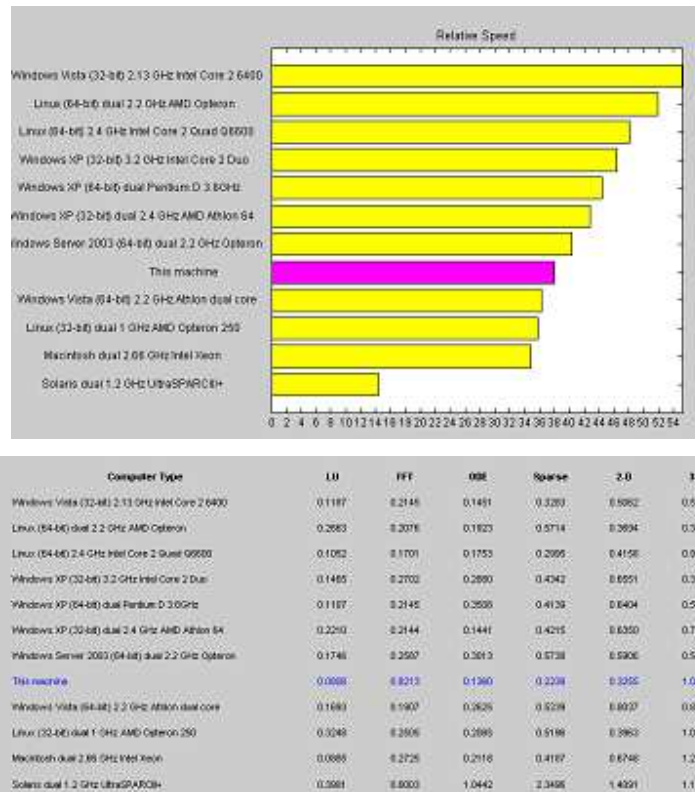


Figure 5.3: Performance Comparison Among different H/W Operating Environment

Figure 5.3 shows the computational speed different among different computer. By this one can have an idea about the platform, which is used to develop and test the proposed watermarking scheme. These statistics are generated in MATLAB by using a inbuilt function “BENCH”.

5.2 Experiments:

To check the perceptual quality, robustness and authenticity of the proposed watermarking scheme, following experiments were executed. Their results and analysis are as follows:

5.2.1 To check Perceptual Quality:

In order to check the perceptual similarity between original and watermarked image, peak-signal-to-noise ratio(PSNR) is used as a metric. Table 4.1 shows the PSNR(in dB) of the watermarked images after embedding the watermark into the given test image given in figure4.1 by the proposed watermarking scheme. In watermarking

Image	PSNR (db)
Lenna	43.3374
Building	50.6747
Cameraman	45.7734
Bubble	47.6209

Table 5.1: PSNR of Watermarked Test Images Image PSNR(in dB)

literatures, PSNR above 40dB is considered as an acceptable level which indicates the good perceptual similarity between the watermarked and original image. Here it can be observed that PSNR for the different test images is above 40 dB which shows the effectiveness of the proposed scheme.

5.2.2 To check robustness:

After embedding the watermark into the cover image, a given set of attacks was applied on the watermarked image to check the robustness of the scheme. Here cameraman image was taken for the experimentation and figure 4.4 shows the original and watermarked image. Correlation Coefficient was used to check the robustness of the extracted watermark. Attacks performed on the watermarked image are as follows:



(a) Original Image

(b) Watermarked Image

Figure 5.4: Original & Watermarked Cameraman Image with PSNR=43.3374dB

5.2.2.1 JPEG Compression:

JPEG compression is one of the most popular image processing attack and generally used to reduce the payload for storage and transmission on the network. The quality of the compression is the amount of distortion to be applied to reduce the size of the image. The quality parameter ranges between 0 to 100 where 0 refers to the maximum reduction in size which results the worst perceptual quality. Figure 5.5 shows the watermarked image compressed with 90% quality factor and the extracted watermark with correlation coefficient value = 0.5057.



Figure 5.5: Result of JPEG Compression (90%)



Figure 5.6 Result of JPEG Compression (50%)



Figure 5.7 Result of JPEG Compression(1%)

5.2.4 Median Filtering:

Median Filtering is one kind of smoothing technique and all the smoothing techniques are effective at removing noise but adversely affect the edges. A 3x3 median filter is used to the Watermarked image Figure 4.6 shows the median filtered watermarked image and the extracted watermark with correlation coefficient value = 0.6173.



Figure 5.8: Result of Median Filtering

5.2.5 Histogram Equalization :

Histogram equalization is a contrast enhancement technique to obtain a new enhanced image with an uniform histogram. This can be achieved by using the normalized cumulative histogram as the gray scale mapping function. Figure 4.7 shows the histogram equalized watermarked image and the extracted watermark with correlation coefficient value = 0.7962.



Figure 5.7: Result of Histogram Equalization

5.2.6 Noise Addition:

Generally image noise is described as an undesirable by-product of image capture or some distortion caused communication channel in transmission. Here gaussian and salt & pepper noise (with mean = 0 and variance=0.01) is added to the watermarked image to

test the robustness of the proposed scheme. Figure 5.8 & 5.9 show the watermarked images after noise addition and the extracted watermarks with correlation coefficient value = 0.4772 & 0.4986 respectively.



Figure 5.8: Result of Adding Gaussian Noise(Mean=0 & Var=0.01)



Figure 5.9: Result of Adding Salt & Pepper Noise(Mean=0 & Var=0.01)

5.2.7 Rotation:

To check robustness against rotation attack, watermarked image was rotated at 15° and 5° using bicubic interpolation. Modified image was cropped to obtain the same size as the unrotated image. Figure 5.10 & 5.11 show the watermarked image after noise addition and the extracted watermark with correlation coefficient value = 0.5207 & 0.5756 respectively.



Figure 5.10: Result of Rotating Watermarked Image with 15°



Figure 5.11: Result of Rotating Watermarked Image with 5°

5.2.7 Scaling:

Scaling is another critical and common geometrical attack in image processing. The size of the watermarked image was reduced by 50% and increased by 200% by using bicubic interpolation. In bicubic interpolation the output pixel value is a weighted average of pixels in the nearest 4-by-4 neighborhood. Figure 4.12 & 4.13 show the scaled watermarked images and the extracted watermark with correlation coefficient value = 0.4418 & 0.7253 respectively.



Figure 5.12: Result of Scale-down Watermarked Image by 50% Figure



Figure 5.13: Result of Scale-up Watermarked Image by 200%

5.2.8 Cropping:

Cropping is also the most popular attack on the image to alter them. Here 35% of image was cropped to test embedding efficiency. Figure 5.14 shows the cropped watermarked image and the extracted watermark with correlation coefficient value = 0.8333.



Figure 5.14: Result of Cropping

5.2.9 Print & Scan Attack:

Print & Scan is the most severe attack on the images. In this attack, first image is printed and then scanned with the help of scanner to convert into the digital format again. This process heavily distorts the image. Lots of noise added into the image during the conversion and scanning process distort the geometrical parameters also. In this attack, image is printed with actual size and scanned at 100 dpi(dots per inches). Figure 5.15 shows the print-scanned watermarked image and the extracted watermark with correlation coefficient value = 0.5995.



Figure 5.15: Result of Print & Scan Attack

These results show that the proposed watermarking scheme is robust against given set of attacks especially against geometrical and print-scan attacks. At receiver side

decoder does not require any information of the original image which proves that the proposed scheme is blind in nature.

5.2. To Check Authenticity:

For the authentication of U and V matrices of watermark, a signature of 8 bit length is generated. Cover image was decomposed into 4 different bands using DWT and low frequency band is further decomposed up to 4-level. LL4 and HH4 band coefficient are used to embed the signature bits. Selected coefficients were converted into 16 bit binary number. For embedding, 10th bit position from MSB was replaced with signature bits respectively. For some attacks like compression, filtering and geometric attacks LL4 band coefficients give good recovery whereas for attacks like histogram equalization, Gaussian noise and print-scan HH4 band coefficients give the ne recovery of the signature bits. Cameraman image was used to test the proposed method and table 4.2 shows the results.

Attack	Cameraman	
	LL4 Band	HH4 Band
JPEG Compression(QF=20)	8	8
Rotation (15 degree)	8	8
Rotation (5 degree)	8	8
Median Filtering	8	7
Salt and Pepper Noise (M=0,Var=0.01)	8	8
Scaling (512-256-512)	8	7


























Scaling (512-1024-512)	8	6
Cropping	8	8
Gaussian Noise (M=0,Var=0.01)	3	6
Histogram Equalization	4	6
Print-Scan	5	7

Table 5.2: Recovered Signature Bits

At the receiver side, decoder first extract the signature of the U & V matrices, then it will match the extracted signature with the original signature. If extracted signature satisfies the matching criteria then it will indicate the authentication of the given matrices. Here Table 5.2 shows exact recovery of the signature for most of the attacks but attacks like Gaussian noise, histogram equalization and print-scan 6 bits are recovered. This can be serving as a threshold for the matching criteria.

5.3 Comparison with Existing Approaches:

Table 5.3 shows the comparison between the proposed watermarking scheme and the existing scheme presented by Ganic, Emir and Eskicioglu, Ahmet M.[17]. Scheme proposed by Ganic, Emir and Eskicioglu, Ahmet M. is non-blind watermarking scheme and 4 watermarks are embedded into four different frequency bands of the cover image after applying DWT on it. The authors motivation behind multiple watermarks is to ensure that at least watermark will survive from any of the band against different types of attacks. Here correlation coefficient is used as metric to check the robustness of the recovered watermark.

Attack	Proposed Scheme	E. Ganic & Ahmet M.[17]				
Types of Attack	Correlation Coefficient					
	HH Band	LL Band	LH Band	HL Band	HH Band	
JPEG Compression (Q=20)						
	0.5057	0.9014	0.0635	0.3440	0.5106	
Median Filtering						
	0.6173	0.2422	0.6471	0.5230	0.0110	
Histogram Equalization						
	0.7962	0.9003	0.8323	0.8048	0.7006	
Gaussian Noise (M=0 & Var=0.01)						
	0.4772	0.2087	0.3188	0.2978	0.4535	
Salt & Pepper Noise (M=0 & Var=0.01)						
	-0.4986	0.1585	0.2997	0.2978	0.4773	

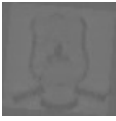











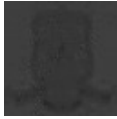









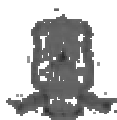



Rotation (15degree)					
	0.5207	0.0959	-0.0157	0.3259	-0.1543
Rotation(5 degree)					
	0.5756	0.0778	-0.0715	-0.2327	-0.6567
Scaling (50% of original image)					
	0.4418	0.0244	-0.6580	-0.5930	-0.6030
Scaling (150% of original image)					
	0.7253	0.2733	-0.6404	-0.5663	-0.6776
Cropping (35%)					
	0.5231	-0.3030	0.2637	0.2994	0.1695
Print-Scan		Not Shown			
	0.5231				

Table 5.3: Comparison Between Proposed & Existing Scheme

Results in table 5.3 show that the proposed scheme is showing comparatively good robustness against all the given attacks, where as scheme given by Ganic, Emir and Eskicioglu, Ahmet M.[6]is not very robust against cropping, rotation and scaling. For JPEG compression(Q=20) and histogram equalization existing scheme gives slightly good recovery of the watermark but results of the proposed scheme for these attacks are also reasonably fair. Proposed scheme is also resilient against the print & scan attack where as existing schemes shows no result for this attack. Existing scheme also suffers from authentication law which is discussed in chapter 3. Proposed scheme is blind in nature where as existing scheme is non-blind.





















My actual contribution is a modification in an already existing watermarking scheme proposed by E. Ganic & Ahmet M. [17]. This scheme is not robust against rotation, scaling and cropping attack and especially against print & scan attack, which are considered very significant attacks against any image.

























Results in chapter 4 show that the proposed scheme showing comparatively good robustness against compression, filtering and geometrical attacks and its also shows comparatively good robustness against print & scan attack. To overcome these attacks SVD works as a complement with DWT. So cascading of DWT and SVD enhance the robustness of the whole scheme. Various test image were used to test the effectiveness of the proposed watermarking scheme. Table 5.4 shows the recovered watermark from various watermarked test images and correlation coefficient was used to measure the robustness of the recovered watermark.

This table shows that the proposed scheme has equally good robustness with various real life test images. Proposed scheme is totally blind in nature as decoder does not require any information of cover or host image for decoding the watermark at receiver side. It uses single watermark for all types of attacks with less embedding time complexity. The results of the proposed scheme were compared with the existing proposed by E. Ganic & Ahmet M. [17]. Table 5.3 shows the comparison between the two approaches and results shows the proposed scheme is providing more robustness than the existing scheme against the given set of attacks. Proposed scheme does not require original content to decode the watermark at receiver side hence it blind in nature whereas approach used in [17] is non-blind in nature. Except this use of signature based authentication mechanism

proposed in chapter 3 made the proposed scheme more secure and reliable. Table 5.3 shows the recovery of the significant bits for the authentication purpose.

Table 5.4: Recovered Watermark and Correlation Coefficient with Original Watermark

Attack	Lenna	Building	Cameraman	Bubble
JPEG Compression (Q=20)				
	0.5057	0.9014	0.0635	0.3440
Median Filtering				
	0.6173	0.2422	0.6471	0.5230
Histogram Equalization				
	0.7962	0.9003	0.8323	0.8048
Gaussian Noise (M=0 & Var=0.01)				
	0.4772	0.2087	0.3188	0.2978
Salt & Pepper Noise (M=0 & Var =0.01)				
	-0.4986	0.1585	0.2997	0.2978

Attack	Lenna	Building	Cameraman	Bubble
Rotation (15degree)				
	0.5207	0.0959	-0.0157	0.3259
Rotation(5 degree)				
	0.5756	0.0778	-0.0715	-0.2327
Scaling (50% of original image)				
	0.4418	0.0244	-0.6580	-0.5930
Scaling (150% of original image)				
	0.7253	0.2733	-0.6404	-0.5663
Cropping (35%)				
Print-Scan				
	0.5231	-0.3030	0.2637	0.2994

Chapter 6

CONCLUSIONS AND FUTURE DIRECTIONS

As electronic distribution of copyright material becomes more prevalent a need for digital watermarking rises. In this project, the basic characteristics of a digital watermark are outlined; mainly including: fidelity preservation, robustness to common signal and geometric processing operations, robustness to attacks applicability to digital images.

To meet these requirements, I proposed algorithm of watermarking technique of digital image using SVD. It is only limited to watermarking of still gray scale images. Further research can be Done for developing the same concept for color images, audio and video filter. Recovery of the signature is not good for Gaussian noise, histogram equalization & print-scan. To provide more reliability in signature based authentication, error control code can be used with signature at the time of embedding which can ensure the exact recovery of the signature bits. Also can added cryptography technique to make it more robust and secure.

Chapter 7

BIBLIOGRAPHY

- [1] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoan, "Secure spread-spectrum watermarking for multimedia," *IEEE Trans. On Image Processing*, Vol. 6, No. 12, December 1997.
- [2] R. Liu; T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership", *IEEE Transactions on Multimedia*, vol.4, no.1, pp.121-128, Mar.2002.
- [3] Ghazy R.A.; El-Fishawy N.A.; Hadhoud M.M.; Dessouky M.I.; El-Samie F.E.A./"An A Efficient Block-by-Block SVD-Based Image Watermarking Scheme", *Radio Science Conference, NRSC 2007*, pp.1-9, 13-15 Mar. 2007.
- [4] Kunal Bhandari, Suman K. Mitra; Ashish Jadhav, "A Hybrid Approach to Digital Image Watermarking Using Singular Value Decomposition and Spread Spectrum", S. K. Pal et al. (Eds.): *PreMI, LNCS 3776*, pp.272-275, Oct. 2005.
- [5] Xiao-Ping Zhang; Kan Li, "Comments on-An SVD-based watermarking scheme for protecting rightful Ownership", *Multimedia, IEEE Transactions on*, vol.7, no.3, pp.593-594, Jun. 2005.
- [6] Emir Ganic; Ahmet M. Eskicioglu, "Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies", *Proceedings of the workshop on Multimedia and security, Magdeburg, Germany*, pp. 166-174, Sep. 2004.
- [7] Stefan Katzenbeisser and Fabien A. Petitcolas, editors. "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, Inc., Norwood, MA, USA, 2000.
- [8] Sin-Joo Lee; Sung-Hwan Jung, "A Survey of Watermarking Techniques Applied to Multimedia", *In Industrial Electronics, 2001. Proceedings. ISIE 2001.IEEE International Symposium on*, vol.1, pp.272-277, Jul. 2001.
- [9] Podilchuk C.I.; Delp E.J., "Digital watermarking: Algorithms and Applications", *Signal Processing Magazine, IEEE*, vol.18, no.4, pp.33-46, Jul 2001.
- [10] Yusof Y.; Khalifa O.O., "Digital Watermarking for Digital Images Using Wavelet Transform", *Telecommunications and Malaysia International Conference on*

Communications, 2007. ICT-MICC 2007. IEEE International Conference on, pp.665-669, May 2007.

[11] Cox I.J.; Miller M.L.; Bloom, J.A., "Watermarking Applications and Their Properties", Information Technology: Coding and Computing, 2000. Proceedings. International Conference on, pp.6-10, Sep. 2000.

[12] Wan Adnan W.A.; Hitam S.; Abdul-Karim S.; Tamjis M.R., "A Review of Image Watermarking", Research and Development, 2003. SCORED 2003. Proceedings. Student Conference on, pp.381- 384, Aug. 2003.

[13] Raval M.S.; Rege P.P., "Discrete Wavelet Transform Based Multiple Watermarking Scheme", TENCON 2003. Conference on Convergent Technologies for Asia-Pacifc Region, vol.3, pp.935-938, Oct. 2003.

[14] Kasmani S.A.; Naghsh-Nilchi A., "A New Robust Digital Image Watermarking Technique Based on Joint DWT-DCT Transformation", Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference on, vol.2, pp.539-544, Nov. 2008.

[15] A DWT Domain Visible Watermarking Techniques for Digital Images 2010 International Conference on Electronics and Information Engineering (ICEIE 2010)

[16] H. C. Andrews; C. L. Patterson, "Singular Value Decomposition (SVD) image coding", IEEE Transactions on Communication, vol.24, no.4, pp.425-432, Apr. 1976.

[17] B. Zhou; J. Chen, "A Geometric Distortion Resilient Image Watermarking Algorithm Based on SVD", Chinese Journal of Image and Graphics, vol.9, pp.506-512, Apr. 2004.

[18] Liu Quan; Ai Qingsong, "A Combination of DCT-based and SVD-based Watermarking Scheme", Signal Processing, 2004. Proceedings. ICSP '04. 2004 7th International Conference on, vol.1, pp.873- 876, Sept. 2004.

[19] Manuscript received January 30, 2007, revised April 14, 2007. Y. Yusof is with the Centre of Postgraduate Studies, Kulliyah of Engineering, International Islamic University Malaysia, Gombak, Kuala Lumpur. O. O. Khalifa is with the Kulliyah of Engineering, International Islamic University Malaysia, Gombak, Kuala Lumpur.