



**Ministry of Higher Education and Scientific
Research**

**KASDI MERBAH OUARGLA
UNIVERSITY**

**Faculty of New Information and
Communication Technologies**

**Department of Electronic and Telecommunication
Specialty: TELECOMMUNICATION SYSTEMS**



PROFESSIONAL MASTER MEMORY

LMD

Dissertation

For the Master Degree In Telecommunication Systems

Title:

**WATERMARKING ALGORITHM BASED ON
IMAGE PROJECTION AND ROTATION VIEW**

Presented by:

**ELKHALILI ADEL
DARI MOHAMED ELHADI**

Jury members:

Dr. MOAD SAYAH	University of KASDI MERBAH OUARGLA	Jury-header
Dr. HACHEMI CHENINA	University of KASDI MERBAH OUARGLA	Examiner
Dr. BELKEBIR DJALILA	University of KASDI MERBAH OUARGLA	Supervisor

Academic Year 2021-2022

Dedication

To those who have reached the message and to whom brings us the burdens of doing good and avoiding evil and He has advised the nation to the Prophet of mercy and light of the worlds Prophet Muhammad, peace be upon him.

To what God gives him prestige and dignity, to those who taught me tender without waiting, to what I proudly bear his name.

“Dear dad”

the sense of love and the sense of compassion and dedication, to the smile of life and the mystery of existence, to which his prayer is the secret of my success, and affection it is the balm of my wounded

“Dear mom”

To my wonderful wife who has stood faithfully with me and she was the big motivation behind continue my studies, of course don't forget my daughters Cham and Chahd.

“ADEL”

To my colleague and study friend I had the happiest moments of my life and the most wonderful memories.

Acknowledgement

Before presenting this work, we would like to thank "God" almighty, for allowing us to reach this level of study, and also for giving us a lot of patience and courage without forgetting our parents who did not skimp on no problem to give us all the help necessary to reach this level which will allow us to ensure our future.

We would like to thank Mr. DJALILA BELKEBIR, our supervisor for his decision in charge and his good advice, which resulted in the development of a work which we hope will be satisfactory.

We also extend our thanks to the people who have done us the honor of participating in this work, to the juries of this thesis.

Thank you to all those who have contributed directly or indirectly to the accomplishment of this work.

Abstract

The content of this project discussed the watermarking based on a spatial domain technique where the objective was to protect and to introduce more secure communication so that people can exchange data safely.

In this project we focused on watermarking algorithm based on image projection and rotation view. We have treated an image by changing its dimensions through two main factors, the distance (from the observer) and the rotation as the original image is viewed from a position in a perpendicular direction to its center, while its projection is viewed from a tilted position. It is based on projection of each pixel of the original image on another virtual image that appears as a rotated one.

We have also proposed an application which was programmed by us using the previous algorithm that can provide more protection for the information and the ownership right.

This project contains a comparison between our proposed method and the LSB one. (Least Significant Bit) where we proved that our method was more efficient than the latter.

Key words: watermarking, spatial domain, image projection, rotation view, pixel, LSB (Least Significant Bit).

Résumé

Le contenu de ce projet portait sur le tatouage basé sur une technique de domaine spatial où l'objectif était de protéger et d'introduire une communication plus sécurisée afin que les personnes puissent échanger des données en toute sécurité.

Dans ce projet, nous nous sommes concentrés sur l'algorithme de tatouage basé sur la projection d'image et la vue en rotation. Nous avons traité une image en changeant ses dimensions à travers deux facteurs principaux, la distance (de l'observateur) et la rotation lorsque l'image originale est vue depuis une position dans une direction perpendiculaire à son centre, tandis que sa projection est vue depuis une position inclinée. Il est basé sur la projection de chaque pixel de l'image d'origine sur une autre image virtuelle qui apparaît comme une image pivotée.

Nous avons également proposé une application qui a été programmée par nos soins en utilisant l'algorithme précédent qui peut fournir plus de protection pour les informations et le droit de propriété.

Ce projet contient une comparaison entre notre méthode proposée et celle du LSB. (Bit moins significatif) où nous avons prouvé que notre méthode était plus efficace que cette dernière.

Mots clés : tatouage, domaine spatial, projection d'image, vue en rotation, pixel, LSB (Bit moins significatif).

ملخص

يناقش محتوى هذا المشروع العلامة المائية على أساس تقنية المجال المكاني حيث أن الهدف هو حماية وتقديم اتصالات أكثر أماناً حتى يتمكن الأشخاص من تبادل البيانات بأمان.

ركزنا في هذا المشروع على خوارزمية العلامات المائية بناءً على إسقاط الصورة واستدارتها. لقد تعاملنا مع الصورة من خلال تغيير أبعادها وفق عاملين رئيسيين ، المسافة (من المراقب) والدوران حيث يتم عرض الصورة الأصلية من موضع في اتجاه عمودي إلى مركزها ، بينما يتم عرض إسقاطها من وضع مائل . يعتمد على إسقاط كل بكسل من الصورة الأصلية على صورة افتراضية أخرى تظهر كصورة مستديرة.

لقد اقترحنا أيضاً تطبيقاً تمت برمجته بواسطةنا باستخدام الخوارزمية السابقة التي يمكن أن توفر مزيداً من الحماية للمعلومات وحق الملكية.

يحتوي هذا المشروع على مقارنة بين طريقتنا المقترحة وطريقة LSB. (بت أقل أهمية) حيث أثبتنا أن طريقتنا كانت أكثر كفاءة من الطريقة الأخيرة.

الكلمات المفتاحية : العلامة المائية ، المجال المكاني ، إسقاط الصورة ، الدوران ، البكسل ، LSB (بت أقل أهمية).

Contents

Title:	
Dedication	I
Acknowledgement	II
Abstract.....	III
Résumé.....	IV
ملخص.....	V
Contents... ..	VI
LIST OF TABLES	X
LIST OF FIGURES	XI
LIST OF ABBREVIATIONS.....	XIII
General introduction	1

CHAPTER I: HIDING DATA: STATE OF THE ART

I.1 Introduction.....	2
I.2 What Is Data Hiding?.....	2
I.2.1 History of data hiding	2
I.3 Steganography	3
I.3.1 What Is Steganography?.....	4
I.3.2 Steganography throughout history.....	4
I.3.3 Steganography Types.	7
I.3.3.1 Technical Steganography.....	7
I.3.3.1.A. Invisible Ink.....	7
I.3.3.1.B. Microdots	8
I.3.3.2 Linguistic Steganography.....	8
I.3.3.2.A. Semagrams	8
I.3.3.2.B. Visual Semagrams.....	9
I.3.3.2.C. Text Semagrams.....	9
I.3.3.2.D. Open Codes.....	9
I.3.3.2.E. Misspellings.....	9
I.3.3.2.F. Jargon Code.....	10
I.3.3.2.G. Covered Cipher.....	10
I.3.3.2.H. Null Cipher.....	10

I.3.3.2.I. Grille Cipher.....	11
I.3.3.3 Digital Steganography	11
I.3.3.3.A. Text Steganography.....	11
I.3.3.3.B. Image Steganography.....	12
I.3.3.3.C. Audio/Video Steganography.....	12
I.3.4 Network Steganography	14
I.3.5 Techniques of Steganography.....	14
I.3.5.1 Spatial Domain Methods	14
I.3.5.1.A. LSB.....	15
I.3.5.1.B. Pixel Value Differencing.....	15
I.3.5.1.C. BPC: The Binary Pattern complexity.....	15
I.3.5.2 Transform Domain Steganography....	16
I.3.5.2.A. The Discrete Fourier Transform (DFT)	16
I.3.5.2.B. The Discrete Cosine Transform (DCT)	16
I.3.5.2.C. Discrete Wavelet Transform (DWT)	17
I.3.5.3 Vector Embedding.....	17
I.3.5.4 Spread spectrum.....	18
I.3.5.5 Statistical Technique..	18
I.3.5.6 Distortion Techniques...	18
I.3.5.7 Masking and Filtering.....	18
I.4 Cryptography.....	18
I.4.1 What is cryptography?.....	19
I.4.2 History of Cryptography	19
I.4.2.1 Hieroglyph – The Oldest Cryptographic Technique.....	20
I.4.3 Techniques used in cryptography.....	21
I.4.3.1 Classical cryptography.....	21
I.4.3.1.A. Substitution ciphers.....	21
I.4.3.1.B. Transposition cipher.....	23
I.4.3.1.C. Codebooks.....	24
I.4.3.2 Modern Cryptography.....	24
I.4.3.2.1 Secret-Key (Private) Cryptography	24
I.4.3.2.2 Asymmetric Key (Public) Cryptography.....	25
I.5 Comparatives study between Steganography and Cryptography	26
I.6 Conclusion.....	27

CHAPTER II: WATERMARKING ALGORITHM BASED ON IMAGE PROJECTION AND ROTATION VIEW

II.1 Introduction.....	28
II.2 Watermarking.....	28
II.2.1 Brief History.....	30
II.2.2 Differences between Watermarking and Steganography.....	31
II.2.3 Digital Image Watermarking Working.....	31
II.2.3.1. Embedding Stage.....	33
II.2.3.2. Distortion/Attack Stage	33
II.2.3.3. Detection/Retrieval Stage	33
II.2.4 Digital Watermarking Characteristics.....	33
II.2.4.A. Fidelity.....	33
II.2.4.B. Robustness.....	33
II.2.4.C. Capacity.....	33
II.2.4.D. Security.....	34
II.2.5 Applications of watermarking.....	34
II.2.5.A. Copyright Protection.....	34
II.2.5.B. Content Archiving.....	34
II.2.5.C. Broadcast Monitoring.....	34
II.2.5.D. Tamper Detection.....	34
II.2.5.E. Digital Fingerprinting.....	34
II.2.5.F. Authentication and Integrity Verification.....	34
II.2.6 Digital Watermarks Types.....	34
II.2.6.A. According to type of Document.....	34
II.2.6.B. According to human perception.....	35
II.2.7 Digital Image Watermarking Techniques.....	35
II.2.7.1 Spatial Domain Watermarking.....	36
II.2.7.2 Frequency(transform) Domain Watermarking	37
II.2.7.2.1 Discrete Cosine Transform	37
II.2.7.2.2 Discrete Wavelet Transform.....	38
II.2.7.2.3 Discrete Fourier Transform.....	40
II.2.8 Comparison Between Spatial and Frequency Watermarking Domain	41
II.3 Projection.	41

II.3.1 Directs projection positions	41
II.3.2 The substitution	45
II.3.2.1 Hiding process	45
II.3.2.2 Extraction process	47
II.4 Conclusion	48

CHAPTER III: IMPLEMENTATION AND RESULTS

III.1 Introduction	49
III.2 Materials Used in Development	49
III.3 Image Quality Metrics	49
III.3.1 Mean square error (MSE)	49
III.3.2 Peak Signal to Noise Ratio (PSNR)	50
III.3.3 Average Difference (AD)	50
III.3.4 Maximum Difference (MD)	50
III.3.5 Peak Mean Square Error (PMSE)	50
III.3.6 Normalized Cross-Correlation (NCC)	50
III.3.7 Structural Content (SC)	51
III.3.8 Laplacian Mean Square Error (LMSE)	51
III.3.9 Normalized Absolute Error (NAE)	51
III.3.10 Robustness Test (BER)	51
III.4 Direct Image Projection Analysis	51
III.5 Security Analysis	63
III.6 Integrity Analysis	63
III.7 Conclusion	64
General Conclusion	65
Bibliography	66
Annex	67

LIST OF TABLES

Table 1.1: Comparison of Steganography & Cryptography	27
Table 2.1: Comparison between Watermarking Domains.....	41
Table 3.1: The Relationship Between the Size of the Image and the Corresponding Max Size of the Watermark.....	54
Table 3.2: The effect of the rotation angle on the hiding.	56
Table 3.3: The effect of the distance on the hiding.	57
Table 3.4: Quality Metrics Results.	57
Table 3.5: The Outcomes of Attacking.	63
Table 3.6: Results of transmission stego image through different methods....	63

LIST OF FIGURES

Figure 1.1 Classification of information security techniques.	3
Figure 1.2 The title page of <i>Steganographia</i> by Johannes Trithemius, the inventor of the word “steganography.” Reproduced by kind permission of the Syndics of Cambridge University Library.	6
Figure 1.3. Steganography Process.	6
Figure 1.4 Classification of steganographic methods.	7
Figure 1.5. Example of Image Steganography.	12
Figure 1.6. Example of Audio Steganography.	13
Figure 1.7. Example of Video Steganography.	13
Figure 1.8. Techniques of Steganography.	14
Figure 1.9. Example of LSB Conversion.	15
Figure 1.10. LSB Conversion.	15
Figure 1.11. Process of DCT.	17
Figure 1.12 encryption and decryption	19
Figure 1.13 hieroglyph writing.	20
Figure 1.14 example of encryption.	20
Figure 1.15 Mono-Alphabetic Substitution Cipher.	21
Figure 1.16 Playfair Cipher.	22
Figure 1.17 Vignere Cipher.	24
Figure 1.18 sample columnar transposition.	24
Figure.1.19. Type of keys in encryption and decryption.	25
Figure 1.20 Classification of cryptography methods.	26

Figure 2.1 A paper watermark.	29
Figure 2.2. Watermark Embedding Process.	32
Figure 2.3. Watermark Detection Process...	32
Figure 2.4. Stages in Digital Image Watermarking.	33
Figure 2.5. Digital Image Watermarking.	35
Figure 2.6. Discrete Cosine Transform Region.	38
Figure 2.7. Two Level Decomposition.	39
Figure 2.8. image projection system.	42
Figure 2.9. estimation of a pixel projection position.	43
Figures 2.10. (a) original image, (b) and (c) positions projected from (a).	44
Figure 3.1 Hiding A small watermark in the Cover Image using the Projection method.....	52
Figure 3.2 Hiding A big watermark in the Cover Image using the Projection method.....	53
Figure 3.3 Some outcomes yielded by our proposed technique in different scenarios.....	55
Figure 3.4. Comparison between the proposed and the LSB methods in MSE parameter.....	59
Figure 3.5. Comparison between the proposed and the LSB methods in PSNR parameter....	59
Figure 3.6. Comparison between the proposed and the LSB methods in AD parameter.....	60
Figure 3.7. Comparison between the proposed and the LSB methods in MD parameter.....	60
Figure 3.8. Comparison between the proposed and the LSB methods in PMSE parameter...	61
Figure 3.9. Comparison between the proposed and the LSB methods in SC parameter.....	61
Figure 3.10. Comparison between the proposed and the LSB methods in LMSE parameter..	62
Figure 3.11. Comparison between the proposed and the LSB methods in NAE parameter....	62

LIST OF ABBREVIATIONS

- RGB:** Red-Green-Blue
- JPEG:** Joint Photographic Expert Group
- BER:** Robustness Test
- LSB:** Least Significant Bits
- DFT:** Discrete Fourier Transform
- DCT:** Discrete Cosine Transform
- DWT:** Discrete Wavelet Transform
- PVD:** Pixel Value Differencing
- BPC:** Binary Pattern complexity
- PSNR:** Peak Signal to Noise Ratio
- MSE:** Mean Squared Error
- BPC:** Binary Pattern complexity
- AD:** Average Difference
- MD:** Maximum Difference
- PMSE:** Peak Mean Square Error
- NCC:** Normalized Cross-Correlation
- LMSE:** Laplacian Mean Square Error
- NAE:** Normalized Absolute Error
- SC:** Structural Content



General Introduction

GENERAL INTRODUCTION

Throughout history, humankind always tried to find the best ways to communicate efficiently and securely. data hiding is one of them.

Art of data hiding in digital media, steganography and watermarking, aims to embed secret data into cover with purpose of identification, copyright protection, and annotation. The main constraint factors of this process are message data quantity, necessity of invariability of embedded data under distortions like lossy compression, third party removal, or modification.

Data hiding techniques fall into three categories of cryptography, steganography, and watermarking. Watermarking and particularly steganography tend to conceal presence of hidden data while cryptography makes data gibberish.

In our work we are interested in images, being the most widespread and most traded media on the internet. We are going to create an application that will allow to watermarking based in spatial domain, Once the watermarking is done, this image will be able to circulate from one Internet user to another without any problem since at any time the ownership of this image can be proven by extracting the tattoo hidden in the image

We will propose an invariable method based in method of substitution projection



CHAPTER I :
HIDING DATA :
STATE OF THE ART

I.1 Introduction

The rapidly decreasing cost of processing, storage, and bandwidth has already made digital media increasingly popular over traditional analog media. However, digital media also causes extensive vulnerabilities to mass piracy of copyrighted material. It is, therefore, very important to have the capabilities to detect copyright violations and control access to digital media. Fueled by these concerns, data hiding has evolved as an enabler of potential applications for copyright protection such as access control of digital multimedia (e.g., watermarking), embedded captioning, secret communications (e.g., steganography), tamper detection, and others.

I.2 What Is Data Hiding?

Data hiding is the art of hiding a *message signal* in a *host signal* without any perceptual distortion of the host signal. The composite signal is usually referred to as the *stego* signal. Data hiding is a form of *subliminal* communication.

Any form of communication relies on a channel or medium. Data hiding, or steganographic, communications rely on the channel used to transmit the *host content*. As the stego content moves around the globe, perhaps over the Internet, or by any other means usually deployed for communicating the host signals, so does the *embedded*, covert message signal [1].

I.2.1 History of data hiding

Throughout history, humankind always tried to find the best ways to communicate efficiently and securely. The evolution of communication began with shouting out words, then quickly evolved to the next stage of sophisticated spoken language; however, the carrier (a human) may forget parts of the message or simply forget the message completely when moving from one place to another. A more refined method was needed, such as writing messages on basic materials such as stones. Writing was more efficient and represented a big milestone in human history.

In the Imperial period, the Persian empire was one of the first civilizations to enhance communications routes; roads were built across the entire empire to make sending messages quicker and more efficient.

The wealth and power of the Persian empire allowed it to invade more land outside its borders, which meant sending troops far away from their central capital, hence new requirements

for secure communication emerged. A method for delivering secure messages through cryptographic and message-hiding techniques was devised.

Many sources give credit to Greece for creating the first known hiding technique by humans, as we will see later. Arabs, Chinese, and Romans also created their own methods to communicate securely, especially during war time.

Cryptography is a type of data hiding by obscuring messages. We will be discussing it in the next pages because it is important to understand how old cryptographic techniques work since new methods are mainly based on these principles.

Steganography is the science of hiding data; there are many types and each type have its own techniques in hiding. Combining steganography with encryption to transmit secret messages is the ideal solution to counter today's online risks [2].

The figure 1.1 present the classification of data hiding techniques.

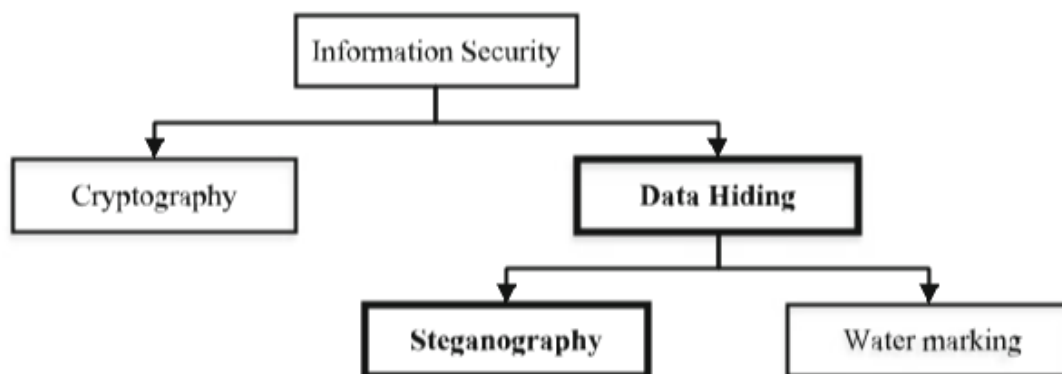


Figure. 1.1 Classification of information security techniques

I.3 Steganography

One of a data hiding techniques is the steganography, we will explain it in this chapter.

I.3.1 What Is Steganography?

Steganography is the science of hiding information. It is among the few disciplines that have the honor to be described as an *art* in addition to being a *science*. Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide data from a third party. Steganography is usually used in conjunction with encryption for additional security of sensitive data. By hiding encrypted data inside an honest-looking carrier, a secret message has less possibility of being discovered by outside parties during information exchange [2].

I.3.2 Steganography throughout history

The word *steganography* is a composite of the Greek words *steganos*, which means “covered,” and *graphia*, which means “writing.” In other words, steganography is the art of concealed communication where the very existence of a message is secret. The term steganography was used for the first time by Johannes Trithemius (1462–1516) in his trilogy *Polygraphia* and in *Steganographia* (see Figure 1.2). While the first two volumes described ancient methods for encoding messages (cryptography), the third volume (1499) appeared to deal with occult powers, black magic, and methods for communication with spirits. The volume was published in Frankfurt in 1606 and in 1609 the Catholic Church put it on the list of “*libri prohibiti*” (forbidden books). Soon, scholars began suspecting that the book was a code and attempted to decipher the mystery. Efforts to decode the book’s secret message came to a successful end in 1996 and 1998 when two researchers independently revealed the hidden messages encoded in numbers through several look-up tables included in the book. The messages turned out to be quite mundane. The first one was the Latin equivalent of “The quick brown fox jumps over the lazy dog,” which is a sentence that contains every letter of the alphabet. The second message was: “The bearer of this letter is a rogue and a thief. Guard yourself against him. He wants to do something to you.” Finally, the third was the start of the 21st Psalm.

The first written evidence about steganography being used to send messages is due to Herodotus, who tells of a slave sent by his master, Histiaëus, to the Ionian city of Miletus with a secret message tattooed on his scalp. After the tattooing of the message, the slave grew his hair back in order to conceal the message. He then traveled to Miletus and, upon arriving, shaved his head to reveal the message to the city’s regent, Aristagoras. The message encouraged Aristagoras to start a revolt against the Persian king.

Herodotus also documented the story of Demeratus, who used steganography to alert Sparta about the planned invasion of Greece by the Persian Great King Xerxes. To conceal his message, Demeratus scraped the wax off the surface of a wooden writing tablet, scratched the message into the wood, and then coated the tablet with a fresh layer of wax to make it appear to be a regular blank writing tablet that could be safely carried to Sparta without arousing suspicion.

Aeneas the Tactician is credited with inventing many ingenious steganographic techniques, such as hiding messages in women's earrings or using pigeons to deliver secret messages. Additionally, he described some simple methods for hiding messages in text by modifying the height of letter strokes or by marking letters in a text using small holes.

Hiding messages in text is called linguistic steganography or acrostics. Acrostics was a very popular ancient steganographic method. To embed a unique "signature" in their work, some poets encoded secret messages as initial letters of sentences or successive tercets in a poem. One of the best-known examples is *Amorosa visione* by Giovanni Boccaccio. Boccaccio encoded three sonnets (more than 1500 letters) into the initial letters of the first verse of each tercet from other poems. The linguistic steganographic scheme described at the beginning of this chapter is an example of Cardan's Grille, which was originally conceived in China and reinvented by Cardan (1501–1576). The letters of the secret message form a random pattern that can be accessed simply by placing a mask over the text. The mask plays the role of a secret stego key that has to be shared between the communicating parties.

Francis Bacon described a precursor of modern steganographic schemes. Bacon realized that by using italic or normal fonts, one could encode binary representation of letters in his works. Five letters of the cover object could hold five bits and thus one letter of the alphabet. The inconsistency of sixteenth century typography made this method relatively inconspicuous.

Brassil described a modern version of this steganographic principle. He described a method for data hiding in text documents by slightly shifting the lines of text up or down by 1/300 of an inch. It turns out that such subtle changes are not visually perceptible, yet they are robust enough to survive photocopying [3]

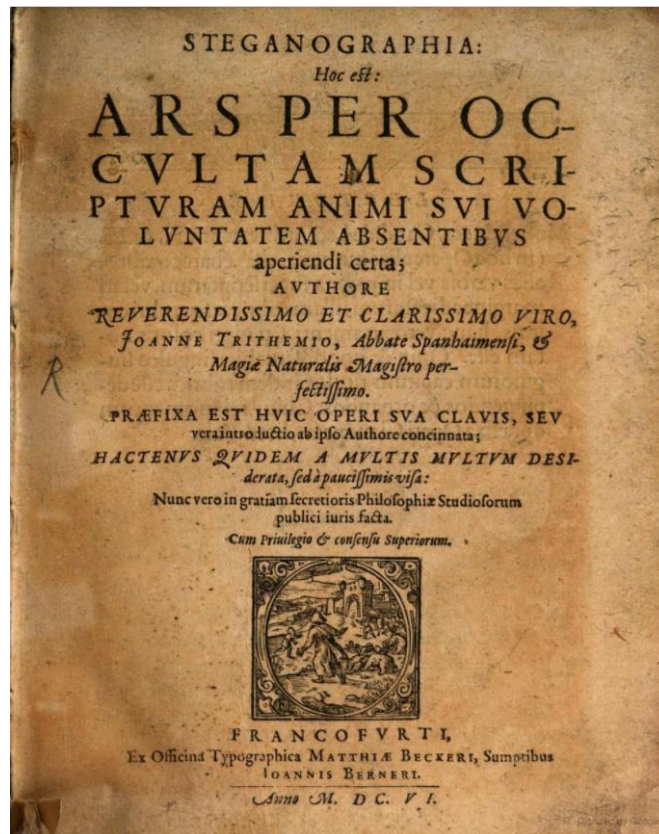


Figure 1.2 The title page of *Steganographia* by Johannes Trithemius, the inventor of the word “steganography.” Reproduced by kind permission of the Syndics of Cambridge University Library.

- The figure 1.3 show the principal elements of steganography process.

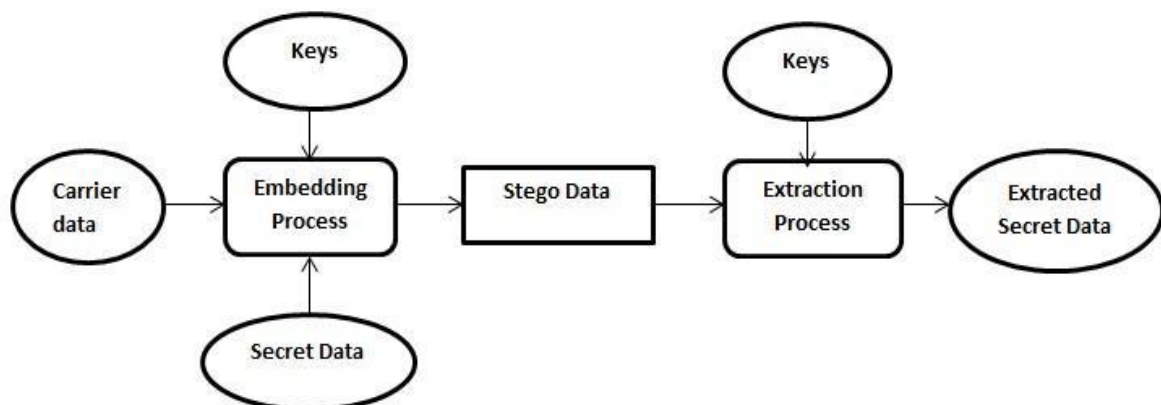


Figure 1.3. Steganography Process

I.3.3 Steganography Types

Steganography can be divided into three types: technical, linguistic, and digital. (Fig. 1.4). Technical steganography applies scientific methods to conceal secret messages, while linguistic steganography uses written natural language. Digital steganography, developed with the advent of computers, employs computer files or digital multimedia data. In this section, we describe each type respectively.

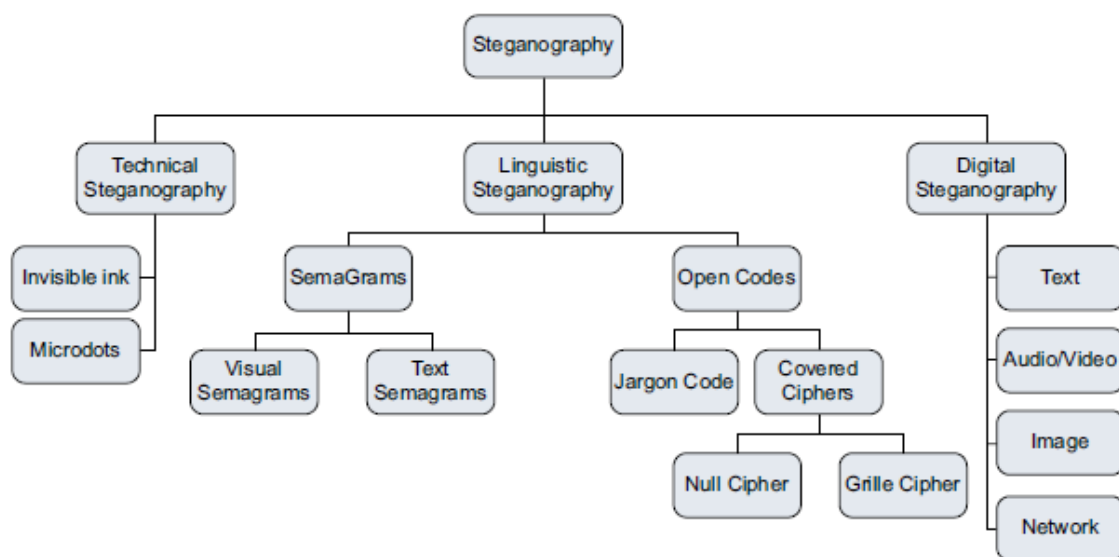


Figure 1.4 Classification of steganographic methods

I.3.3.1 Technical Steganography

Technical steganography uses different scientific methods to obscure messages. We will mention two: invisible ink and microdot.

I.3.3.1.A Invisible Ink

Invisible ink is a colorless ink (such as acid, milk, lemon juice, etc.) that does not visibly appear on paper after writing with it. It requires the use of flame, light, or other chemical material to make the font appear in an attempt to reveal hidden messages.

During the US revolution, both British and American rebels used invisible ink to exchange secret messages. The secret writing was inserted between lines of an ordinary letter. They were

written using a mixture of ferrous sulfate and water. The recipient then put the paper above a candle flame or treated it with a chemical material such as sodium carbonate to reveal the message's hidden contents. You can practice writing a secret message in your home using the following steps:

- Use milk as ink. Use a brush to write your secret message on a piece of paper.
- Let your paper dry once done writing.
- In order to reveal the message, put the paper above a candle flame, or expose the paper to a heat source.

I.3.3.1.B Microdots

Microdots are text or images reduced to a very small size (about 1 mm in diameter) to prevent detection by unintended recipients. This method was used widely during World War II. Microdots have often been about the size and shape of a period or the title of a lowercase i or j.

The Germans often credited the invention of microdots to themselves; however, Alexander Foote, a Soviet agent in World War II, said in his book, *Handbook for Spies*, that the Soviet intelligence service had used this method before World War II. Microdots were used extensively during the war by all parties, especially the French and Germans, by sending their hidden messages across enemy lines by balloons and pigeons. During World War II German spies used to photograph

secret messages and reduce their size to 1 mm (one dot). Then they would insert this dot into another ordinary message. Upon receiving the message, the secret message would be extracted and enlarged again to become readable. The first reported usage of this technique was during the Franco-Prussian War in 1870. It was conducted through shrinking messages to reduce their size during transmission.

I.3.3.2 Linguistic Steganography

Linguistic steganography is the art of using written natural language to hide the presence of secret messages. It is further classified as open codes and semagrams.

I.3.3.2.A Semagrams

Semagrams hide information by the use of symbols or signs. It has two types: visual and text.

I.3.3.2.B Visual Semagrams

A visual semagram uses innocent looking or everyday physical objects to convey a message; for example, a sender can post a picture on his Facebook profile showing a natural landscape at dawn, and this picture may indicate to the recipient a special meaning like Attack at Dawn. Another example is by modifying a website's layout or color, a sender can change the website theme to a different color to communicate a secret message to the recipient. These signs are difficult to detect and have the advantage of normality in an everyday world.

I.3.3.2.C Text Semagrams

A text semagram hides a message by modifying the appearance of the carrier text. Capitalized letters, accentuation, peculiar handwriting, blank spaces in between words, or handwritten text can all be used as signals for a predefined purpose.

I.3.3.2.D Open Codes

In open codes steganography a message is hidden inside a legitimate innocent piece of text that will not draw the attention of a regular observer. Some may argue that this method is not suitable or secure enough for hiding messages; however, the following example will clear this point. A human observer is different from computer surveillance software that is used by many governments to monitor Internet traffic when it comes to steganalysis.

For example, if a political activist wants to send a secret message (email) to someone else in another country by using the open codes technique, he can simply hide his secret message using one of the open code techniques described next and he can almost assure that his message will not draw the attention of any automated monitoring programs that could be used by his government to monitor Internet traffic. This could be achieved by taking advantage of the nonintelligent nature of computer systems. However, this does not mean that it is safe to send top secret messages using an open code technique. A specialist observer can easily extract the hidden message from the regular text if the message was sent for analysis by a human.

I.3.3.2.E Misspellings

Since automated monitoring machines are programmed to track specific keywords, it is difficult for them to know all possible variations of spelling for a specific word. For example, we can misspell the following phrase as follows:

- Regular text: Meet me tomorrow
- Misspelled text: mt m tmrow

You can use this technique to hide only some words that you think the automated machines may be programmed to capture, as it is not practical to hide long messages using this technique.

I.3.3.2.F Jargon Code

Is using a language that is only meaningful for a group of people, the Internet is full of jargon code. These days, for example, many people use specific chat acronyms and text shorthand during online chat like:

- 2BZ4UQT: Too Busy For You Cutey
- 4eva: Forever
- ADBB: All Done Bye Bye

I.3.3.2.G Covered Cipher

Covered Cipher uses a particular method or secret way to hide the classified message inside another innocent looking message. The secret message could only be recovered by the person who knows how it was concealed. It has two types: null and grille.

I.3.3.2.H Null Cipher

Use a set of rules to hide a secret message in an open carrier, like reading the second letter of every word. A famous example of this technique is a message sent by the German Embassy in Washington, DC to the headquarters in Berlin during World War I:

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE.
GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT
FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING
NATIONAL EXCITEMENT IMMENSELY.

If we took the first letter from each word, we will have the following message:

Pershing sails from NY June 1.

The Germans returned another message, apparently as a check on the first:

APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

Taking the second letter in each word the same secret message as the first will emerge:

Pershing sails from NY June 1.

The advantage of this method is that a secret message could be hidden inside another open carrier that contains ordinary text that may not grab the attention of any observer.

I.3.3.2.I Grille Cipher

Grille cipher was invented by Gerolamo Cardano. Grilles are a kind of transposition cipher that can also include aspects of steganography. They are best thought of as pieces of cardboard with holes cut into them in a specific pattern. The secret message is written in the holes, and then the rest of the message is filled in around it. The only way the message is readable is by the recipient who has the correct grille [2]

I.3.3.3 Digital Steganography

The advance of computers and the widespread use of online communication nowadays had allowed us to begin embedding secret messages inside digital files like images and audio files. This could be achieved by adding secret bits or replacing the current bits inside digital files. Such hiding methods are considered difficult to crack and notice for both human observer and automated programs used by governments to monitor online traffic.

We can divide digital steganography according to the host file used (carrier or overt file) as follow:

I.3.3.3.A Text Steganography

Text steganography is a type of steganography that uses text to conceal messages inside it. This could be achieved by changing text formatting or the characteristics of the text. This type is considered impractical, though, because it cannot hide large volumes of data without grabbing someone's attention. Some examples are the hidden text feature in MS Office®, which can be applied by inserting small spaces between words to store bits; white space manipulation to store bits in front of each line or section in the document; shifting lines up or down

to store bits; making text white on a white background; and storing hidden text inside document metadata.

I.3.3.3.B Image Steganography

Image Steganography is a technique that has become more popular in recent years because of the flood of electronic images available online with the advent of digital cameras, smart phones, and high-speed Internet that simplify distribution of large images. In addition to its popularity among users, digital images have more capability to store large amounts of hidden data inside their structure.

Image steganography works by embedding an encrypted message (or the original message without encryption) into a graphic file. This produces what is called a stego-image (see fig 1.5).



Figure 1.5. Example of Image Steganography

This stego-image is then transmitted to the receiver, who then extracts the message from the carrier file using a predefined shared secret between the sender *and* the receiver. During the transmission of the stego-image, unauthenticated persons can only observe the transmission of an image but can't recognize the existence of the hidden message.

I.3.3.3.C Audio/Video Steganography

Audio steganography takes advantage of physical characteristics of the human auditory system. For example, the human ear can listen to noise in the audible frequency range between 20 Hz and 20 kHz. Audio steganography works by embedding a secret message inside a digitized audio signal, which results in changing the binary sequence of the corresponding audio file without any noticeable change to the human ear. The human ear is not able to recognize a low tone

frequency signal in the presence of a higher frequency; this is called frequency masking. This discovered property is used in different ways to exploit audio files for embedding data inside it secretly.

Audio steganography uses the following techniques for hiding secret messages:

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

Audio steganography is also part of the more common term of digital watermarking (antipiracy techniques), which is widely used in counterpiracy systems. This technique enables us to know whether a specific audio/video is illegally recorded (copy version) and when this happened (see fig 1.6)

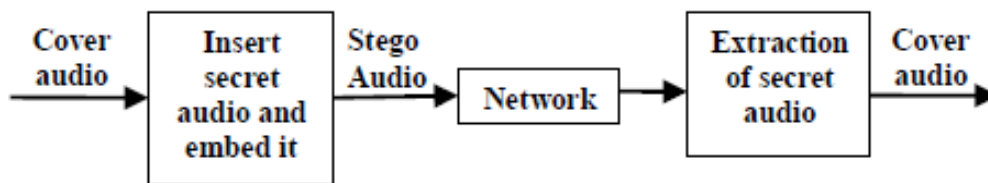


Figure 1.6. Example of Audio Steganography

Video uses a combination of both images and audio to deliver its contents. Hidden data is usually embedded inside video images. The continual stream of images and sound will make it very hard for humans to know there is hidden data inside the video file (look to the example fig 1.7).

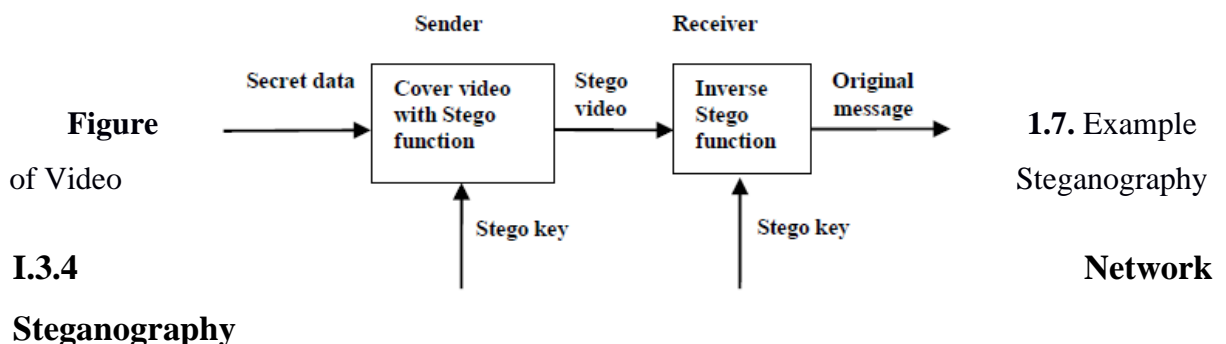


Figure 1.3.4
Example of Video Steganography

1.7. Example Steganography

Network

Network steganography works by exploiting different networking protocol features to hide its secret message. We can also consider concealing data messages inside images, then sending them across the Internet as a kind of networking stego. In this thesis, however, we will only refer to the methods where we can exploit hidden areas inside networking protocol channels as networking steganography.

There are basically two ways in which we can hide our secret messages using network steganography:

- Exploiting some networking protocols in unused header space to conceal data.
- Masking secret messages as ordinary network traffic [5].

I.3.5 Techniques of Steganography

the fig 1.8 present the different techniques of steganography

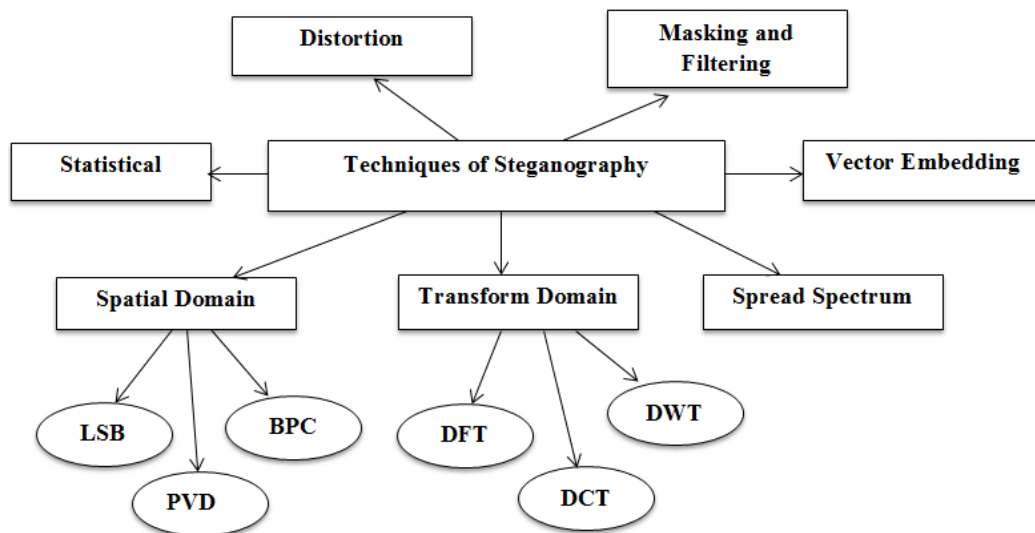


Figure 1.8. Techniques of Steganography

I.3.5.1 Spatial Domain Methods:

Spatial domain Steganography technique refers to methods in which data hiding is performed directly on the pixel value of cover image in such a way that the effect of message is not visible on the cover image. The spatial domain methods are classified as following:

I.3.5.1.A LSB: LSB is one the technique of spatial domain methods. LSB is the simple but susceptible to lossy compression and image manipulations. Some bits are change directly in

the image pixel values in hiding the data. Changes in the value of the LSB are imperceptible for human eyes. Ex (fig 1.9)

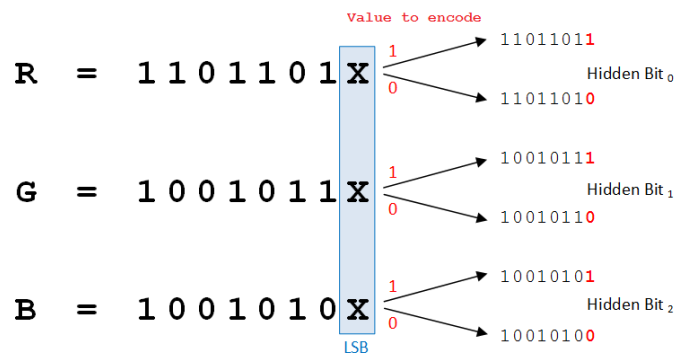


Figure 1.9. Example of LSB Conversion

In the spatial domain LSB technique there is less chance for degradation of the original image, more information can be stored in an image and covert communication of sensitive data. fig 1.10 show an example of LSB conversion.

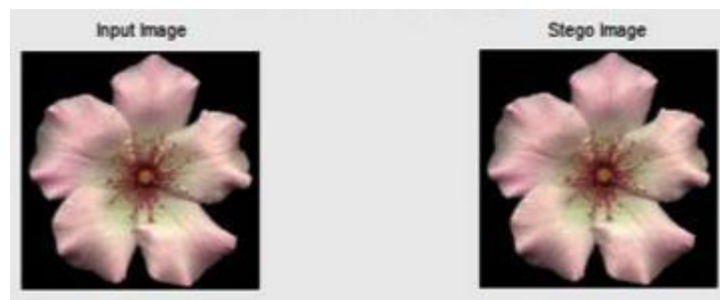


Figure 1.10. LSB Conversion

I.3.5.1.B Pixel Value Differencing: To embedding the data in PVD the two consecutive pixels are selected. Whether the pixels are determined from smooth area or an edge area. Payload is determined by calculating the difference between two regular pixels.

I.3.5.1.C BPC: The Binary Pattern complexity approach is used to measure the noise factor in the image complexity. The noisy portion is replaced by binary Pattern and it is mapped from the secret data. The image will remain same when the reverse noise factor will be determined.

I.3.5.2 Transform Domain Steganography:

It is a more complex way to hide the information in an image. The different algorithms and transformations are used to hide information in the images. In the frequency domain, the process of embedding data of a signal is much stronger than embedding principles that operate in the time domain. The transform domain techniques over the spatial domain techniques is to hide the information in the images that are less exposed to compression, image processing and cropping. Some transform domain techniques are not depending on the image format and they run the lossless and lossy format conversions. Transform domain techniques are classified into various categories such as Discrete Fourier transformation (DFT), discrete cosine transformation (DCT), Discrete Wavelet transformation (DWT).

1.3.5.2.A The Discrete Fourier Transform (DFT):

Discrete Fourier transform is the transform that are purely discrete: discrete-time signals are converted into discrete number of frequencies. DFT converts a finite list of equally spaced samples of a function into the list of coefficients of a finite combination of complex sinusoids ordered by their frequencies. It can be said to convert the sampled function from its original domain often time or position along a line to the frequency domain. The Discrete Time Fourier transforms uses the discrete time but it converts into the continuous frequency. The algorithm for computing the DFT is very fast on modern computers. This algorithm is known as Fast Fourier Transform i.e. FFT and it produces the same result as of the DFT by using the Inverse Discrete Fourier Transform.

1.3.5.2.B The Discrete Cosine Transform (DCT):

This method is similar to the Discrete Fourier Transform. DCT transform the signal or image from spatial domain to the frequency domain. The mathematical transforms convert the pixels in such a way as to give the effect of “spreading” the location of the pixel values over part of the image. The DCT is used in steganography as the Image is broken into 8×8 pixel blocks and transforms these pixel blocks into 64 DCT. (see fig 1.11).

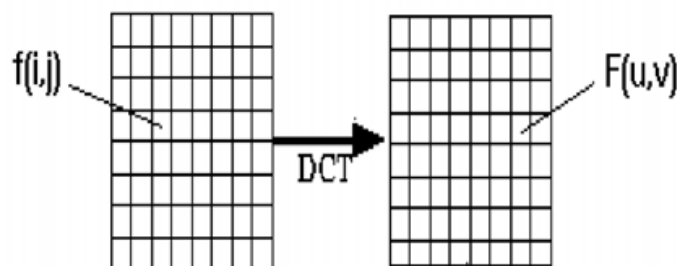


Figure 1.11. Process of DCT

Working from left to right, up to down, the DCT is applied to each block. Through quantization table each block is compressed to scale the DCT coefficients and message is embedded in DCT coefficients. The array of compressed blocks that constitute the image is stored in drastically reduced the amount of space. When desired, image is reconstructed through decompression, a process that uses the Inverse discrete cosine transform i.e. IDCT.

I.3.5.2.C Discrete Wavelet Transform (DWT):

It is used to transform the image from a spatial domain to the frequency domain. In the process of steganography DWT identifies the high frequency and low frequency information of each pixel of the image. It is mathematical tool for decomposing an image hierarchically. It is mainly used for processing of non-stationary signals. The wavelet transform is based on small waves, Known as wavelets, of different frequency and limited duration. It provides both frequency and spatial description of the image. Wavelets are created by translations and dilations of a fixed function are known as mother wavelet. DWT performs in one dimension and in the two-dimensional plane. The DWT is the accurate model than the DFT or the DCT and it is multi resolution description of the image. The current image compression standard JPEG 2000 is based on the wavelet transforms.

I.3.5.3 Vector Embedding:

A vector embedding method that uses robust algorithm with codec standard (MPEG-1 and MPEG -2). This method embeds audio information to pixels of frames in host video. It is based on the H.264/AVC Video coding standard. The algorithm designed a motion vector component feature to control embedding, and also to be the secret carrier. The information embedded will not significantly affect the video sequence's visual invisibility and statistical invisibility. The algorithm has a large embedding capacity with high carrier utilization, and can be implementing fast and effectively.

I.3.5.4 Spread spectrum:

The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it becomes difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover

the data. Thus, it is difficult to remove the data completely without entirely destroying the cover. It is a very robust approach used in military communication.

I.3.5.5 Statistical Technique:

In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.

I.3.5.6 Distortion Techniques:

The distortion method is used to store the secret data by distorting the signal. An encoder applies a sequence of modifications to the cover image and the decoder phase decodes the encrypted data to the original data with the secret data by using some secret key.

I.3.5.7 Masking and Filtering:

This approach is used to hide the data by marking an image. This approach is valuable where watermarks become a portion of the image. The data will be embedded where the more significant part of the image rather than hiding it into the noisy portion. The watermarking techniques are more integrated into the image and it can be applied without the fear of destruction of the image. This technique is used in 24 bit and grey scale images [5].

I.4 Cryptography

Human being from ages had two inherent needs: (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. The word ‘cryptography’ was coined by combining two Greek words, ‘Krypto’ meaning hidden and ‘graphene’ meaning writing.

I.4.1 What is cryptography?

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While

cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis. [7].

The fig 1.12 show the stages of operation of encryption and decryption

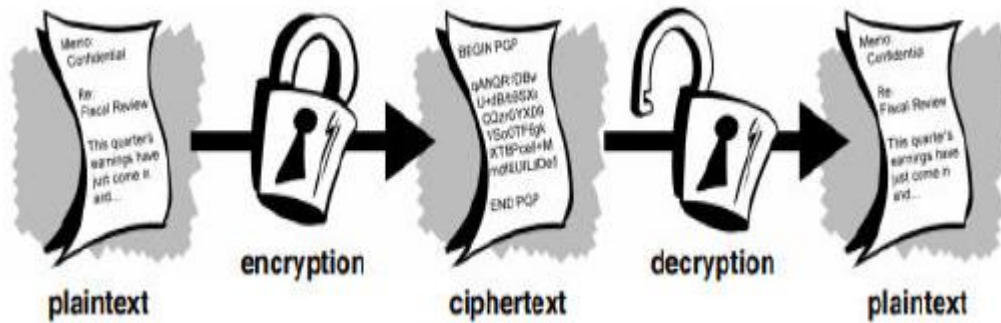


Figure 1.12 encryption and decryption

I.4.2 History of Cryptography

The art of cryptography is considered to be born along with the art of writing. As civilizations evolved, human beings got organized in tribes, groups, and kingdoms. This led to the emergence of ideas such as power, battles, supremacy, and politics. These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well. The roots of cryptography are found in Roman and Egyptian civilizations.

I.4.2.1 Hieroglyph – The Oldest Cryptographic Technique

The first known evidence of cryptography can be traced to the use of 'hieroglyph'. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph. This code was the secret known only to the scribes who used to transmit messages on behalf of the kings. One such hieroglyph is shown below. (fig 1.13 example of hieroglyph writing).



Figure 1.13 hieroglyph writing

Later, the scholars moved on to using simple mono-alphabetic substitution ciphers during 500 to 600 BC. This involved replacing alphabets of message with other alphabets with some secret rule. This rule became a key to retrieve the message back from the garbled message.

The earlier Roman method of cryptography, popularly known as the Caesar Shift Cipher, relies on shifting the letters of a message by an agreed number (three was a common choice), the recipient of this message would then shift the letters back by the same number and obtain the original message [8].

The fig 1.14 show an example of encryption by shifting 2 letters.

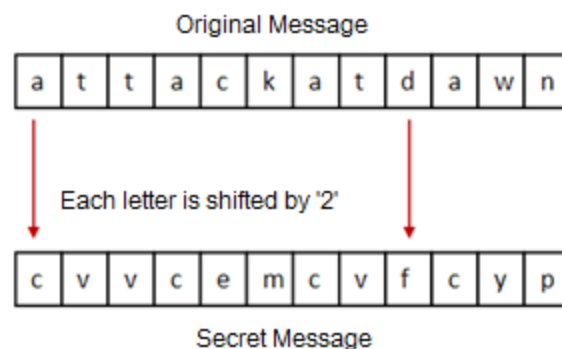


Figure 1.14 example of encryption

I.4.3 Techniques used in cryptography

We can classify the cryptography in 2 methods: classical and modern.

I.4.3.1 Classical cryptography

We use three method for encrypt information: Substitution, Transposition and Codes.

I.4.3.1.A Substitution ciphers

- **mono-alphabetic cipher:** One of the earliest encryption methods is shift cipher. A cipher is a step method or algorithm, that converts plaintext to ciphertext (encryption) or ciphertext to plaintext (decryption). Caesar's shift cipher is known as mono-alphabetic substitution shift cipher as shown in the figure [1.15].

Mono-Alphabetic Substitution Cipher

Caesar's Cipher

- Plaintext:

MESSAGE FROM MARY STUART KILL THE QUEEN

- Substitution table: Caesar's Cipher

– Given: "key = 3": construct the substitution table by shifting the alphabet three characters to the left:



- Ciphertext:

PHVVDJH IURP PDUB VWXDUW NLOO WKH TXHHQ

Figure 1.15 Mono-Alphabetic Substitution Cipher.

Mono-alphabetic means One cipher alphabet.

- **Poly Alphabetic Cipher:** In mono-alphabetic, for a given key the plain alphabet is fixed throughout the encryption or decryption process means if „A“ is substituted by „D“, So All the Occurrence of A's in plain alphabet is substituted by D but In Poly-alphabetic, substituted alphabet in plaintext may be different in different places during encryption or decryption process. There are Two Examples of Poly-Alphabetic Cipher Playfair and Vignere Cipher
- **Playfair Cipher:** In this type of Ploy-Alphabetic, pairs of Alphabet are encrypted as an alternatively a single alphabet is encrypted in Mono-alphabetic substitution cipher. In Playfair, initially, A key table is created where it has 5*5 grid alphabet is put in a sequential

manner. Also, at the starting, a key alphabet is kept for encrypted plaintext instead of this all alphabet is put in sequentially. But there are 25 alphabets (instead of 26) kept in grid So, usually, J is omitted in that table. If the plaintext contains J, then it is replaced by I. fig 1.16 is The Example to explain Playfair Cipher,

H	A	C	K	E
R	B	D	F	G
I	L	M	N	O
P	Q	S	T	U
V	W	X	Y	Z

Figure 1.16 Playfair Cipher

Suppose The key which sender can be used is „HACKER“ instead of this all alphabet is put in a sequential manner as it explained in above.

- **Vignere Cipher:** In this Type of Poly-alphabetic, Caesar shift is modified of their shifting in Vignere Cipher. Also, Key makes the important task for encrypted plaintext in all Cryptography So, Obviously Here is too it applied. As we know the Plaintext can be written in Lowercase and the Ciphertext can be written in Uppercase So, as it, we can create 27×27 grid alphabet where rows of Lowercase alphabet and columns of the Uppercase Alphabet. Each subsequent row represents a cipher alphabet. For each alphabet, the first character is shifted one position farther than the previous one. In some table, the letter replaced by numbers corresponds letter's position in the standard alphabet [5]. For Example- 'A' is replaced with "1", 'C' is replaced with "3", etc.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figure 1.17 Vignere Cipher

As this above Vignere table (fig 1.17) shows different rows, columns and shifting process also.

I.4.3.1.B Transposition Cipher

It is another type of technique for encryption is Transposition where rearrangement or reordering of Plaintext message can happen to obtain more difficult to break and provide better security as an above form. It has mainly Two Important Types of Transposition Cipher are:

- Simple Columnar Transposition
- Rail Fence Transposition

- Simple Columnar Transposition

In this Type of Transposition have some format of written where Plaintext are written Horizontally and Ciphertext are read Vertically as we mention below in fig 1.18:

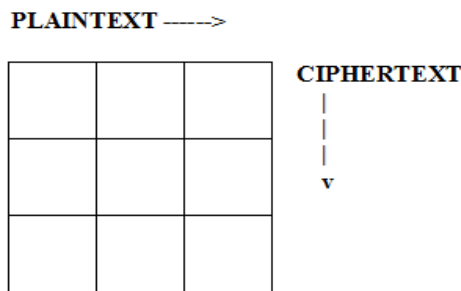


Figure 1.18 sample columnar transposition**- Rail Fence Transposition**

In this type of Transposition, The Plaintext is written with every other letter on a second line. To create the Ciphertext, the letter on the first line is written first and then the letters on the second.

I.4.3.1.C Codebooks

This is a special method of encryption where it gives more security of message transmission and also gives more difficulty to break the code by Cryptanalyst.

Here, it uses the “Code” replaces a word or phrase with a character, which includes some special symbols used in encrypting. These codes are used by Contemporary Cryptography.

Using Code, it was a good way to obfuscate meaning if the message is small and the Codebooks were safe. However, using Codebook to allow safe communication of long or Complex messages between multiple locations was difficult [9].

I.4.3.2 Modern Cryptography

the modern cryptography divides in two: Secret-Key (Private) and Asymmetric Key (Public) Cryptography.

I.4.3.2.1 Secret-Key (Private) Cryptography

Secret-key cryptography, also known as symmetric-key cryptography, employs identical private keys for users, while they also hold unique public keys. “Symmetric key” refers to the identical private keys shared by users. Users employ public keys for the encryption of data, while the private keys serve a necessary purpose in the decryption of data. People wishing to engage in a secure exchange of information will swap public keys and use some method to ensure the existence of identical private keys. In theory, private keys would be brought into the transaction through either the duplication of an existing key or the creation of two identical keys. In modern practice, users utilize key generators to create both keys, but the private keys must still be distributed in a confidential mode.

I.4.3.2.2 Asymmetric Key (Public) Cryptography

Asymmetric key cryptography is also known as the public key cryptography. There are two types of key first one is public key which is used for encryption and second is private key which is used for decryption. Only a particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication (see fig 1.19). The major drawbacks of asymmetric ciphers are their speed and security strength; they are much slower than the symmetric algorithms and more vulnerable to intruder attacks but they make key exchange easier. Asymmetric popular ciphers RSA (Rivest, Shamir, Adleman), Elliptic curve, Diffiehellman key exchange algorithm, Digital signature. Advantages of asymmetric key algorithm are it solves the problem of distributing the key for encryption. Everyone publishes their public keys and private keys are kept secret. Public key encryption allows the use of digital signatures which enables the recipient of a message verify that the message is truly from a particular sender. The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature [7].

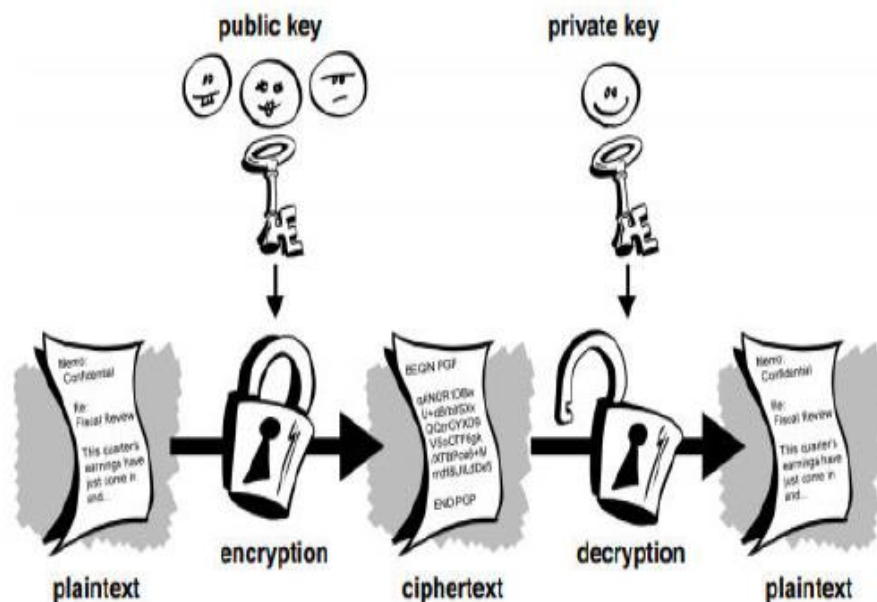


Figure.1.19. Type of keys in encryption and decryption

The fig 1.20 show the classification of the cryptography methods.

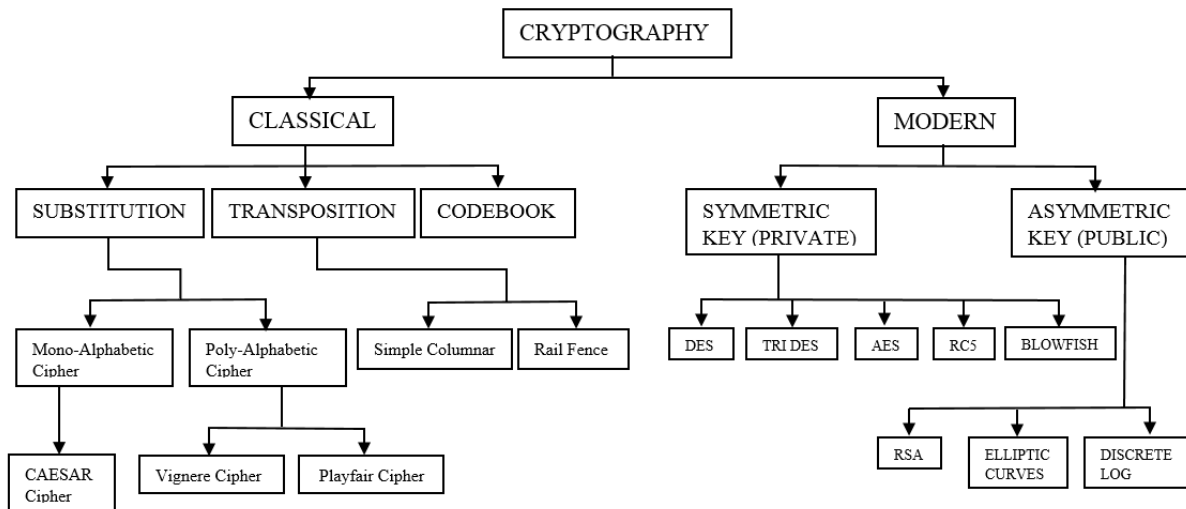


Figure 1.20 Classification of cryptography methods

I.5 Comparatives study between Steganography and Cryptography

They do not share the same goal, although embedding a hidden watermark inside a digital file is considered a type of steganography, but the ultimate goal is to track copyright infringements and prove the ownership of the file in case of a dispute, and steganography's goal is to hide data secretly. Steganography tries to hide as much data as possible while watermarking tends to hide a small amount of data inside the overt file [2].

Both steganography and cryptography share the goal in providing secret communications, but they differ in the methods used to achieve this goal. Some researchers argue that steganography is a form of cryptography because it is used to cover communications.

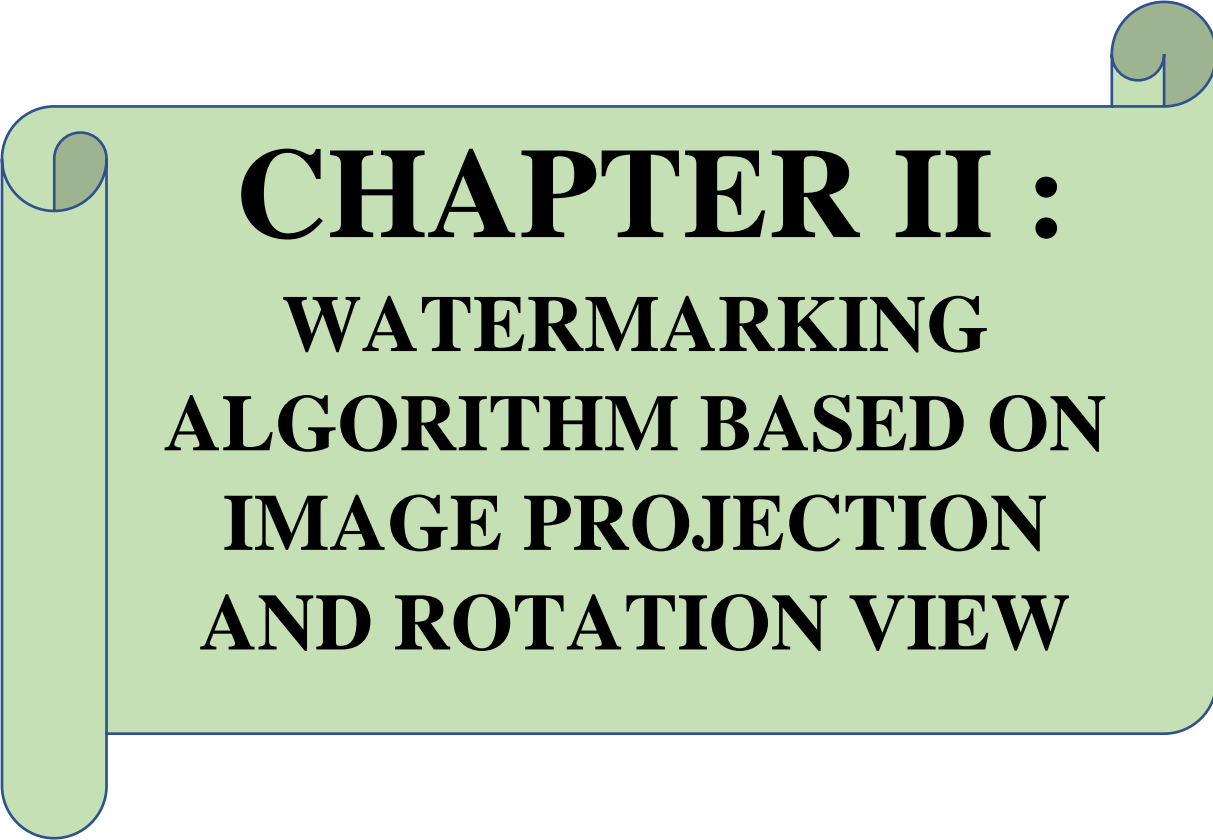
Cryptography offers more secure services but it also comes with some problems. However, this does not form conclusive proof that Steganography cannot be used instead of Cryptography. Thus, combination of cryptography and Steganography is used so all security purpose are solved [6]. We look in the table 1.1 below a comparison between them.

<i>Criteria/ Method</i>	<i>Steganography</i>	<i>Cryptography</i>
<i>Carrier</i>	Any digital media	Usually text
<i>Secret data</i>	payload	Plain text
<i>Key</i>	Optional	Necessary
<i>Input file</i>	At least two	one
<i>Output file</i>	Stego file	Cipher text
<i>Objective</i>	Secret communication	Data protection
<i>Services</i>	Confidentiality Authentication	Confidentiality Data Integrity Authentication Non-repudiation
<i>Techniques</i>	LSB Spatial Domain Jsteg	Transposition, Substitution, RSA
<i>Naked eye identification</i>	No, as message is Hide within other carrier (cover image)	Yes, as message is convert in Other way, which sough something is hidden
<i>Type of Attack</i>	steganalysis	cryptanalysis
<i>Fails</i>	when it is detected	de-ciphered

Table 1.1: Comparison of Steganography & Cryptography

I.6 Conclusion:

Along with the high-speed development of computer technology and network technology, various kinds of attacks faced by digital images also show the trend of diversification, which poses a serious challenge to the security of digital images. Therefore, the development and improvement of hiding data techniques for image content authentication are still a focus and hot spot in this area. In this chapter first introduces the basics principles of steganography and cryptography technologies and their characteristics that it needs to meet.



CHAPTER II :
WATERMARKING
ALGORITHM BASED ON
IMAGE PROJECTION
AND ROTATION VIEW

II.1 Introduction

Steganography is a method based on substitution of pixels in order to conceal them, and several works have suggested algorithms to ensure a certain strength and safety. In this context, we have suggested a new idea based on projection; the idea of this method is to consider the position where each pixel is projected on a new image. This position is defined by the intersection of the pixel's ray of light and the image to be considered depending on the virtual position of the observer.

II.2 Watermarking

Watermarking is not a new phenomenon. For nearly a thousand years, watermarks on paper have been used to visibly indicate a particular publisher and to discourage counterfeiting in currency. A watermark is a design impressed on a piece of paper during production and used for copyright identification (as illustrated in Figure 1.1). The design may be a pattern, a logo, or some other image. In the modern era, as most data and information are stored and communicated in digital form, proving authenticity plays an increasingly important role. As a result, digital watermarking is a process whereby arbitrary information is encoded into an image in such a way as to be imperceptible to observers.

Digital watermarking has been proposed as a suitable tool for identifying the source, creator, owner, distributor, or authorized consumer of a document or an image. It can also be used to detect a document or an image that has been illegally distributed or modified. Another technology, encryption, is the process of obscuring information to make it unreadable to observers without specific keys or knowledge.

This technology is sometimes referred to as data scrambling. Watermarking, when complemented by encryption, can serve a vast number of purposes including copyright protection, broadcast monitoring, and data authentication. In the digital world, a watermark is a pattern of bits inserted into a digital medium that can identify the creator or authorized users. Digital watermarks unlike traditional printed, visible watermarks are designed to be invisible to viewers. The bits embedded into an image are scattered all around to avoid identification or modification. Therefore, a digital watermark must be robust enough to survive detection, compression, and other operations that might be applied to a document.



Figure 2.1 A paper watermark.

Figure 2.1 depicts a general digital watermarking system. A watermark message W is embedded into a media message, which is defined as the host image H . The resulting image is the watermarked image H^* . In the embedding process, a secret key K that is, a random number generator is sometimes involved to generate a more secure watermark. The watermarked image H^* is then transmitted along a communication channel. The watermark can later be detected or extracted by the recipient.

Imperceptibility, security, capacity, and robustness are among the many aspects of watermark design. The watermarked image must look indistinguishable from the original image; if a watermarking system distorts the host image to the point of being perceptible, it is of no use. An ideal watermarking system should embed a large amount of information perfectly securely, but with no visible degradation to the host image. The embedded watermark should be robust, with invariance to intentional (e.g., noise) or unintentional (e.g., image enhancement, cropping, resizing, or compression) attacks. Many researchers have focused on security and robustness, but rarely on watermarking capacity. The amount of data an algorithm can embed in an image has implications for how the watermark can be applied. Indeed, both security and robustness are important because the embedded watermark is expected to be imperceptible and unremovable. Nevertheless, if a large watermark can be embedded into a host image, the process could be useful for many other applications.

II.2.1 Brief History

The term watermarking is derived from the history of traditional papermaking. Wet fiber is pressed to expel the water, and the enhanced contrast between the watermarked and non-watermarked areas of the paper forms a particular pattern and becomes visible.

Watermarking originated in the paper industry in the late Middle Ages roughly, the thirteenth century. The earliest known usage appears to record the paper brand and the mill that produced it so that authenticity could be clearly recognized. Later, watermarking was used to certify the composition of paper. Nowadays, many countries watermark their paper, currencies, and postage stamps to make counterfeiting more difficult.

The digitization of our world has supplemented traditional watermarking with digital forms. While paper watermarks were originally used to differentiate between different manufacturers, today's digital watermarks have more widespread uses. Stemming from the legal need to protect the intellectual property of the creator from unauthorized usage, digital watermarking technology attempts to reinforce copyright by embedding a digital message that can identify the creator or the intended recipients. When encryption is broken, watermarking is essentially the technology to protect unencrypted multimedia content.

In 1989, Komatsu and Tominaga proposed digital watermarking to detect illegal copies. They encoded a secret label into a copy using slight modifications to redundant information. When the label matches that of the registered owner, the provider can ensure that the document holder is the same person. As a method, digital watermarking has a long history, but it was only after 1990 that it gained large international interest. Today, a great number of conferences and workshops on this topic are held, and there are a large number of scientific journals on watermarking in publication. This renewed scientific interest in digital watermarking has quickly grabbed the attention of industry. Its widely used applications include copyright protection, labeling, monitoring, tamper proofing, and conditional access.

Watermarking or information embedding is a particular embodiment of steganography. The term steganography is derived from the Greek words for “covered or hidden” and “writing.” It is intended to hide the information in a medium in such a manner that no one except the anticipated recipient knows the existence of the information. This is in contrast to cryptography, which focuses on making information unreadable to any unauthorized persons.

II.2.2 Differences between Watermarking and Steganography

Watermarking is closely related to steganography; however, there are some differences between the two. Watermarking mainly deals with image authentication, whereas steganography deals with hiding data. Embedded watermarking messages usually pertain to host image information such as copyright, so they are bound with the cover image. Watermarking is often used whenever the cover image is available to users who are aware of the existence of the hidden information and may intend to remove it. Hidden messages in steganography are usually not related to the host image. They are designed to make extremely important information imperceptible to any interceptors.

In watermarking, the embedded information is related to an attribute of the carrier and conveys additional information about or the properties of the carrier. The primary object of the communication channel is the carrier itself. In steganography, the embedded message usually has nothing to do with the carrier, which is simply used as a mechanism to pass the message. The object of the communication channel is the hidden message. As with the application of watermarking, a balance between image perceptual quality and robustness is maintained. Constraints in maintaining image quality tend to reduce the capacity of information embedded. As the application of steganography is different, dealing with covert message transfer, the embedded capacity is often viewed with as much importance as robustness and image quality [4].

II.2.3 Digital Image Watermarking Working

Every digital watermarking technique includes two algorithms: one as the embedding algorithm and other as the detecting algorithm. These two processes are same for all the type of watermarking techniques. Figure 2.2 shows the watermark embedding process in which the watermark is embedded in the cover image by using the embedding algorithm. And Figure 2.3 shows the watermark detection process in which the embedded watermark is recovered by using the detection algorithm. [10].

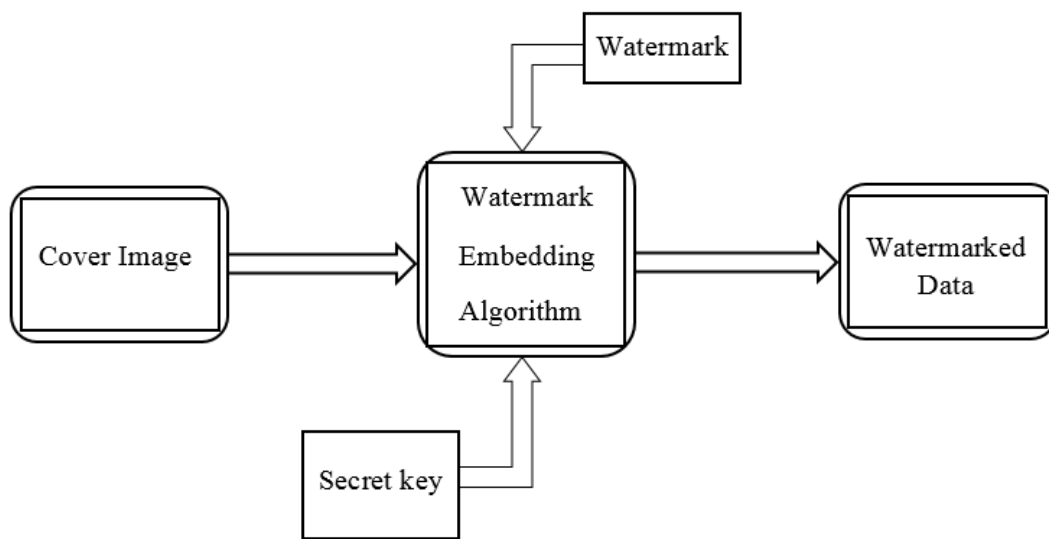


Figure 2.2. Watermark Embedding Process

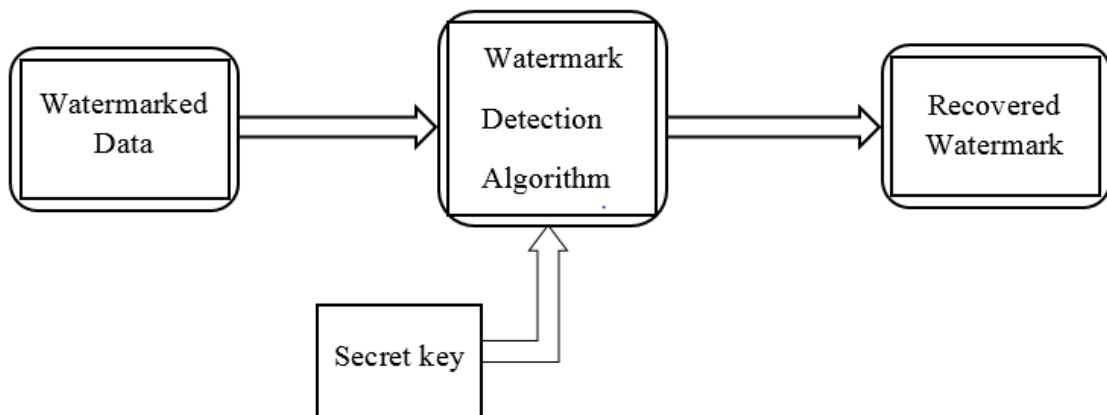


Figure 2.3. Watermark Detection Process

Digital Watermarking is a technique which is used in the digital signal processing of embedding hidden information into multimedia data. This information is not usually visible, only dedicated detector or extractor can see and extracts that information. Digital Image Watermarking use digital image for embedding the hidden information, after embedding the watermarked image is generated and the watermarked image is more robust against attacks. Figure 2.4 shows the stages of digital watermarking. Basically, working of digital image watermarking can be divided in three stages [10].

II.2.3.1. Embedding Stage

The embedding stage is the first stage in which the watermark is embedded in the original image by using the embedding algorithm and the secret key. Then the watermarked image is generated. So, the watermarked image is transmitted over the network.

II.2.3.2. Distortion/Attack Stage

In this stage, when the data is transmitted over the network. Either some noise is added with the watermarked image or some attacks are performed on the watermarked image. So, our watermarked data is either modified or destroyed.

II.2.3.3. Detection/Retrieval Stage

In the detection stage, the watermark is detected or extracted by the dedicated detector from the watermarked image by applying some detection algorithm and by using secret key. In addition to this, noise is also detected.

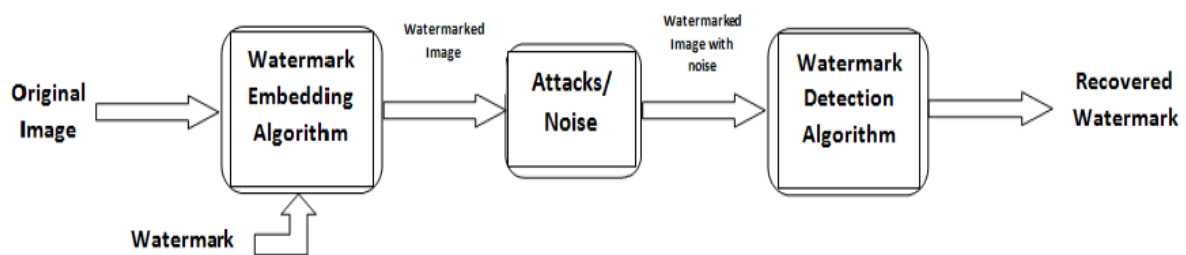


Figure 2.4. Stages in Digital Image Watermarking

II.2.4 Digital Watermarking Characteristics

Four main characteristics of digital watermarking are [11]:

II.2.4.A. Fidelity: The image quality should not get altered after it is watermarked; even watermarking should not make the distortions visible as it will reduce economic value of image.

II.2.4.B. Robustness: Watermarks are removed knowingly or unknowingly by image processing operations. It should be robust across several attacks.

II.2.4.C. Capacity: This characteristic defines amount of data that has to be embedded as a watermark for successfully detection during extraction.

II.2.4.D. Security: Watermark should be secret so that it cannot be identified by the unwanted users.

II.2.5 Applications of watermarking

The main applications of watermarking are [11]:

II.2.5.A. Copyright Protection: Watermarking protects redistribution of copyrighted material over the unreliable network.

II.2.5.B. Content Archiving: Watermarking inserts digital object descriptive or serial number for archiving video, audio or images. It is also used for classification and organization of digital contents.

II.2.5.C. Broadcast Monitoring: It is a cross-verification technique for verifying the data that was supposed to be broadcasted has been broadcasted or not.

II.2.5.D. Tamper Detection: With the help of watermarking, tampering with digital content is detected easily. For tampering detection fragile watermarks are added in the digital content and if added watermark is found to be degraded, indicate tampering with content.

II.2.5.E. Digital Fingerprinting: This technique detects the owner of the digital content on the basis of fingerprints that are unique.

II.2.5.F. Authentication and Integrity Verification: Watermarking also maintains authentication of data and verification of integrity through the use of fragile watermark.

II.2.6 Digital Watermarks Types

Watermarking techniques are classified into the following:

II.2.6.A. According to type of Document: On the basis of document that has to be watermarked, watermarking techniques are divided into the four types:

- Text Watermarking
- Image Watermarking
- Audio Watermarking
- Video Watermarking

II.2.6.B. According to human perception: In other way, digital watermarks techniques are divided as follows:

- **Visible watermark:** It is basically a secondary image that is imposed on original image for protection of that image. In this changes that are made to original image are visible. For example, Figure 2.5 (a) and (b) shows the original and visible watermarked image [11].
- **Invisible-Robust watermark:** In this type of watermarking technique the changes that are made to original image in the form of a watermark are unnoticeable and the changes made are easily recovered later with the help of suitable decoding algorithm.
- **Invisible-Fragile watermark:** Invisible fragile watermarks are added in digital content and if the added watermark is found to be degraded or altered, it indicates tampering with content or modification of image.



(a): original image

(b): Watermarked image

Figure 2.5. Digital Image Watermarking

II.2.7 Digital Image Watermarking Techniques

In the field of digital watermarking, digital image watermarking has attracted a lot of awareness in the research community for two reasons: one is its easy availability and the other is it convey enough redundant information that could be used to embed watermarks [10]. Digital watermarking contains various techniques for protecting the digital content. The entire digital image watermarking techniques always works in two domains either spatial domain or transform domain. The spatial domain techniques work directly on pixels. It embeds the watermark by modifying the pixels value. Most commonly used spatial domain techniques are LSB. Transform domain techniques embed the watermark by modifying the transform domain

coefficients. Most commonly used transform domain techniques are DCT, DWT and DFT. For achieving the robustness and imperceptibility, the transform domain techniques are more effective as compare to the spatial domain. We further elaborated these two domains and its techniques.

II.2.7.1 Spatial Domain Watermarking

The spatial domain represents the image in the form of pixels. The spatial domain watermarking embeds the watermark by modifying the intensity and the color value of some selected pixels [10]. The strength of the spatial domain watermarking is

- Simplicity.
- Very low computational complexity.
- Less time consuming.

The spatial domain watermarking is easier and its computing speed is high than transform domain but it is less robust against attacks. The spatial domain techniques can be easily applied to any image. The most important method of spatial domain is LSB.

Least Significant Bit (LSB):

The LSB is the simplest spatial domain watermarking technique to embed a watermark in the least significant bits of some randomly selected pixels of the cover image. Example of least significant bit watermarking [10]:

Image:	10010101	00111011	11001101	01010101....
Watermark:	1	0	1	0.....
Watermarked Image:	10010101	00111010	11001101	01010100.....

The steps used to embed the watermark in the original image by using the LSB [10]:

- 1) Convert RGB image to grey scale image.
- 2) Make double precision for image.
- 3) Shift most significant bits to low significant bits of watermark image.
- 4) Make least significant bits of host image zero.
- 5) Add shifted version (step 3) of watermarked image to modified (step 4) host image.

The main advantage of this method is that it is easily performed on images. And it provides high perceptual transparency. When we embed the watermark by using LSB the quality of the image will not degrade. The main drawback of LSB technique is its poor robustness to common signal processing operations because by using this technique watermark can easily be destroyed

by any signal processing attacks. It is not vulnerable to attacks and noise but it is very much imperceptible.

II.2.7.2 Frequency(transform) Domain Watermarking

The transform domain watermarking is achieving very much success as compared to the spatial domain watermarking. In the transform domain watermarking, the image is represented in the form of frequency. In the transform domain watermarking techniques, firstly the original image is converted by a predefined transformation. Then the watermark is embedded in the transform image or in the transformation coefficients. Finally, the inverse transform is performed to obtain the watermarked image [10]. Most commonly used transform domain methods are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT).

II.2.7.2.1 Discrete Cosine Transform: Discrete Cosine Transform (DCT) used for the signal processing. It transforms a signal from the spatial domain to the frequency domain. DCT is applied in many fields like data compression, pattern recognition and every field of image processing. DCT watermarking is more robust as compared to the spatial domain watermarking techniques. The main steps which used in DCT [10]:

- 1) Segment the image into non-overlapping blocks of 8x8.
- 2) Apply forward DCT to each of these blocks.
- 3) Apply some block selection criteria (e.g. HVS).
- 4) Apply coefficient selection criteria (e.g. highest).
- 5) Embedded watermark by modifying the selected Co-efficient.
- 6) Apply inverse DCT transform on each block.

In DCT, for embedding the watermark information, we divide the image into different frequency bands. In Figure 2.6 FL denotes the lowest frequency component of the block, while FH denotes the higher frequency component and FM denotes the middle frequency component which is chosen as the embedding region. The Discrete cosine transform achieves good robustness against various signal processing attacks because of the selection of perceptually significant frequency domain coefficients.

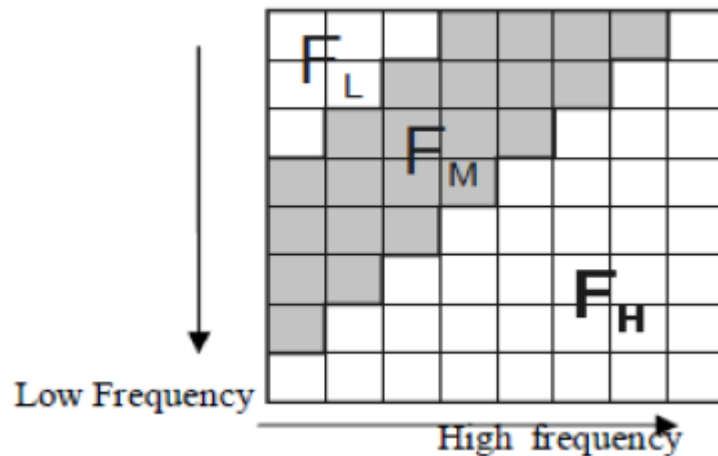


Figure 2.6. Discrete Cosine Transform Region

Merits of DCT:

- DCT is better than any of the spatial domain techniques because it is robust against various kinds of attacks like cropping, noising, filtering and sharpening.
- DCT is a real transform with better computational efficiency.
- The DCT gives a better performance in the bit rate reduction.
- DCT also implements fast algorithms.

II.2.7.2.2 Discrete Wavelet Transform: Discrete wavelet transform (DWT) of the image produces multi-resolution representation of an image. The multi-resolution representation provides a simple framework for interpreting the image information. The DWT analyzes the signal at multiple resolutions. DWT divides the image into high-frequency quadrants and low-frequency quadrants. The low-frequency quadrant is again split into two more parts of high and low frequencies, and this process is repeated until the signal has been entirely decomposed.

The single DWT transformed two-dimensional image into four parts: one part is the low frequency of the original image, the top right contains horizontal details of the image, the one bottom left contains vertical details of the original image, the bottom right contains high frequency of the original image. The low frequency coefficients are more robust to embed a watermark because they contain more information of the original image. The reconstruction of the

original image from the decomposed image is performed by IDWT (the fig 2.7 explain that) [10].

The digital wavelet transform is scalable in nature. DWT more frequently used in digital image watermarking because of its excellent spatial localization and multi resolution techniques. The excellent spatial localization property is very convenient to recognize the area in the cover image in which the watermark is embedded efficiently.

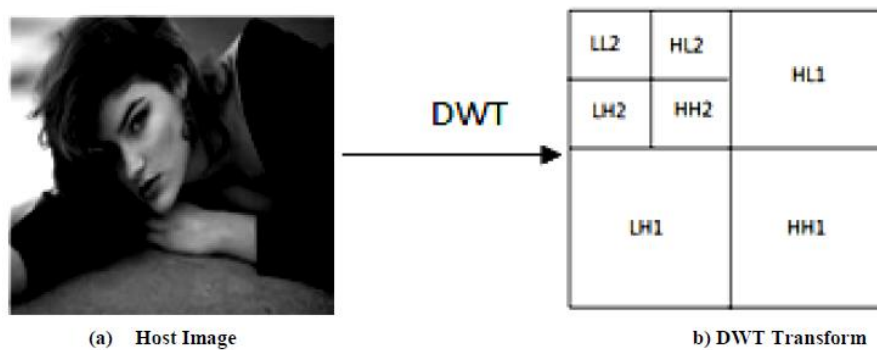


Figure 2.7. Two Level Decomposition

Merits of DWT over DCT:

- DWT gives better visual image quality as compared to the DCT.
- In DWT, dividing the input coding into non overlapping 2-D block is not necessary; its higher compression ratios avoid blocking artefacts.
- DWT allows better localization as compared to the DCT.
- The watermarking method is robust to wavelet transform based image compression as well as to other common image distortions like rescaling half toning, additive noise etc. This is also an advantage over DCT [10].
- The DWT understands the working of HVS more clearly than the DCT.
- DWT defines the multi resolution description of the image. So, the image can be shown in different levels of resolution and proceed from low resolution to high resolution.

Demerits of DWT over DCT:

The main disadvantage of DWT is that the DWT is more complex than the DCT. When DCT is used it takes 54 multiplications to compute for a block of 8x8, distinct wavelet calculation depends upon the length of the filter used, whom at least one multiplication per coefficient. The other drawback is that computation cost is higher and its computation time is longer.

II.2.7.2.3 Discrete Fourier Transform: Discrete Fourier Transform (DFT) offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. DFT decomposes an image in sine and cosine form. The DFT based watermark embedding techniques are divided in two types: one is the direct embedding and the other one is the template-based embedding.

According to the direct embedding technique the watermark is embedded by modifying DFT magnitude and phase coefficients. The template based embedding technique introduces the concept of templates. A template is structure which is embedded in the DFT domain to estimate the transformation factor. Once the image undergoes a transformation this template is searched to resynchronize the image, and then the detector is used to extract the embedded spread spectrum watermark [10].

Advantages of DFT over DWT and DCT:

The DFT is Rotation Scaling Translation (RST) invariant. So, DFT can be used to recover from geometric distortion, whereas the spatial domain, DCT and DWT are not RST invariant. Hence, it is difficult to overcome from geometric distortions [10].

Disadvantage of DFT over DWT and DCT:

The main disadvantage of the DFT is that the output of the DFT is always in complex value and it requires more frequency rate.

II.2.8 Comparison Between Spatial and Frequency Watermarking Domain

The table 2.I present the Comparison between Watermarking Domains [11]

Factors	Spatial Domain	Frequency Domain
Cost	Very low	Very high
Robustness	Fragile	Robust
Perceptually	Highly controllable	Low controllable
Complexity	Low	High
Time consumption	Less	More

Table 2.1: Comparison between Watermarking Domains

II.3 Projection

In our algorithm, we have suggested a new substitution idea of the image's pixels as to conceal it. It is based on projection of each pixel of the original image on another virtual image that appears as a rotated one. This rotation is explained by a virtual observer that is supposed to turn around the center of the original image. Therefore, the relation between these two pictures is ensured by the original image plan is perpendicular to the observer's direction. Since each pixel has a light beam, the intersection position of its direction with that of the virtual image is used as a projection position. However, this projection has a drawback so that some parts of the original image disappear while others are projected into the same positions. The reason is that positions of the projected pixels must be fully rounded.

II.3.1 Directs projection positions

The original image is viewed from a position in a perpendicular direction to its center, while its projection is viewed from a tilted position. First, the different observer's positions are

assumed to be located on the circle around the image. The ray of this circle defines the distance of the image's center. The reference position is then where the observer's direction is perpendicular to the original image's plan. Therefore, any other position is defined by its tilt angle compared to the reference position. (see fig 2.8).

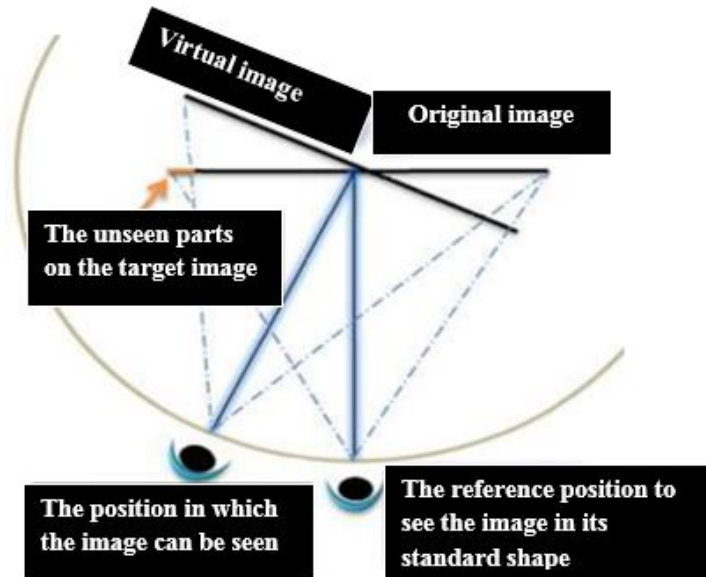


Figure 2.8: image projection system

The projection process is based on the intersection of the light beam direction to the observer of each pixel of the original and virtual image of which the plan is perpendicular toward the current direction of the observer. The intersection point is the position to use in order to paste the original pixel. Besides, it is obvious that the new position is slightly different from the original one. Therefore, and according to tilt, while all pixels are being projected, the image obtained is either expanded or condensed compared to the original.

Consider the pixel located at P_o from the center O of the image, and given the position reference V_o , when the observer moves around the center of the image along the circle having its radius equal to OV_o , the position that will take the P_o pixel in the target image becomes P_t . In other words, P_t is the position where the P_o pixel is supposed to be seen in the target image when tilting the observer's position. Therefore, the aim is to determine the Opt value.

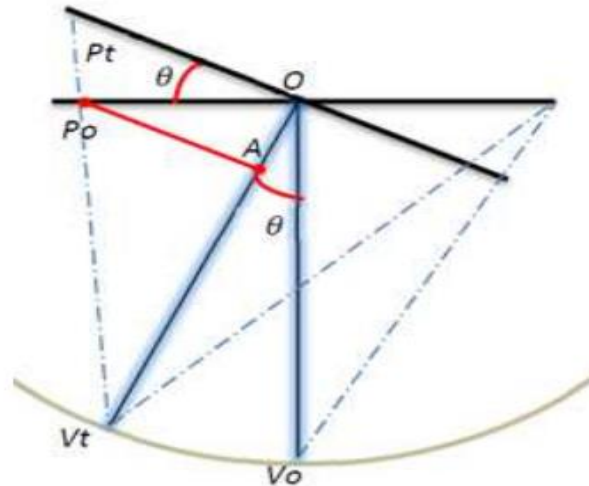


Figure 2.9: estimation of a pixel projection position

Be θ the angle between the directions of the reference position and the new position. This angle is the same between the original image plan and the titled one. Be A the perpendicular projection of P_o on the new direction $\overrightarrow{OV_t}$ such that ΔP_oAO is to a right triangle and $OP_oA = \theta$ is easy to see that $AP_o = OP_o \cdot \cos\theta$. If we take into account ΔOP_tV_t , using this expression and based on the truth of the following expression:

$$\frac{OP_t}{AP_o} = \frac{OV_t}{AV_t} \quad (1)$$

The OPT value can easily be calculated from the resulting expression:

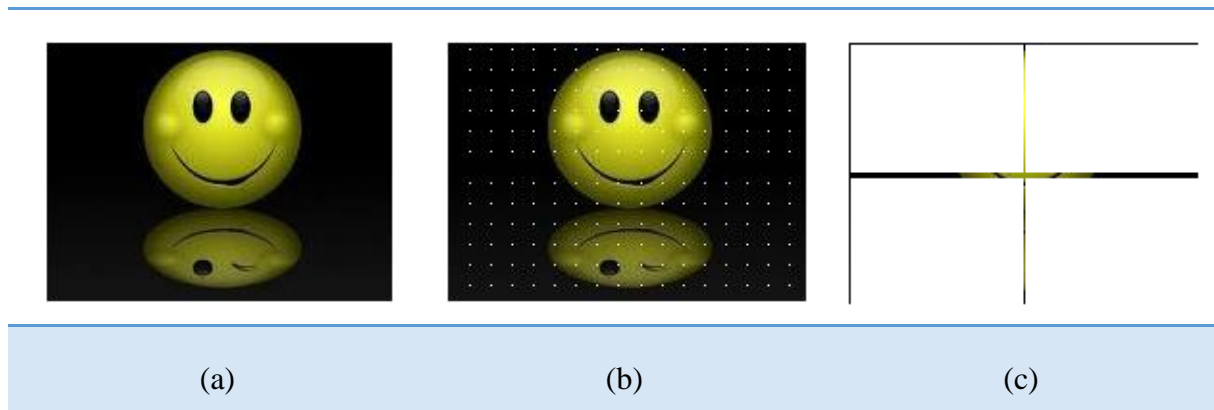
$$OPT = \frac{OV_t \cdot OP_o \cdot \cos\theta}{OV_t - OP_o \cdot \sin\theta} \quad (2)$$

Because: $AV_t = OV_t - OA$.

- According to figure 2.9, formula 2 is only true for a part which is half of the image located on the same -side of the position of the observer with compared to the original one. In fact, the other part of the image is projected onto the target image using different formulas.
- Since the expected results in the substitution algorithm depend neither on the complexity of the formulas, nor on their number, only formula 2 was used. Therefore, it is used simultaneously on two sides of the image. Moreover, the construction of the new virtual image does use the whole line or the whole column as a transformation unit, instead of using

each pixel. Therefore, the formula 2 is used to assess the new pixel position; it uses the whole line or the whole column of a color plan to copy it on this position.

- On the formula 2, the reconstruction of the virtual image needs two main parameters that are the distance $OV_o = OV_t$ from the observer, and the side it takes compared to reference position (angle θ).
- Moreover, the OV_t distance and the angle θ are both composed of two components representing the horizontal (OV_{tx} and θ_x) and vertical (OV_{ty} and θ_y) displacement, because the algorithm transforms the image in the horizontal and vertical directions. This means that the observer has moved from his original position in/or horizontal-vertical direction.
- This is an example of a projected image where pixels in white are the intersection of the positions of the horizontal and vertical vector.



Figures 2.10: (a) original image, (b) and (c) positions projected from (a).

- When making pixel positions, two problems arise. The first one is that of the pixels having their projection positions outside the limit of the virtual image. For instance, we notice in figure 2.10 on the image C that positions or holes are not in white. This means that they are not affected by the projection.
- The second issue is due to the fact that each estimated position of Opt is rounded to its nearest integer of its value, which enables to obtain several pixel lines or columns having the same projection position. This takes place in case where large angles are used that wave a whole part of the original image in a reduced part of the projected one. Therefore, for a given position, only one row point or column point is kept, while the others are ignored.

- The projection algorithm repeats the same operation on the two sides of the image, which means that the projection is applied on the other side as if the virtual observer has moved to the left side then to the right side.
- The idea of our algorithm does not require restoring the lost positions. Therefore, these two issues do not need to be corrected. Regardless, it is too easy to detect the difference in using small or big angles.

% Algorithm: Image Project

For each OPo position (column/line) of the original image

Estimate Opt;

If Opt is not off limits of the target image

If Opt is not used yet

Use the column / line Opt of the target image

Mark the use of OPT

End

II.3.2 The substitution:

this algorithm part includes two steps:

II.3.2.1 Hiding process

The colors of an image are a combination of three basic colors red, green, and blue which constitute the three planes of the image. Bits substitution is made in the least significant bit of the foreground. Once the plan has all its inputs used, we go to the 2nd plan, and then to the 3rd plan. Thereafter, we go to the 2nd least significant bit and so on until we conceal the whole image.

The basic idea is to make the intersection between the lines and the columns of the projected image, and to use the least significant bit and substitute it with a bit of the image to be concealed. Consequently, the substitution algorithm is:

% Algorithm: Image Hide

End = false

Tlin = PosProjV (image)

Tcol = PosProjH (image)

Lin = col = K = I = J = Bs = P = O

While non end do

Substitute the Bs bit rank of the pixel (Tlin (lin), Tcol (col)) of the plan P of the original image by the K bit rank of the pixel (i, j)

j=j+1;

if j = number of image columns to conceal

i := i+1;

if I = number of the image lines to conceal

end = true

end if

j := 0;

end if

if line+1 = size (Tlin) then

p++;

if P = 3 then

bs ++

if bs = 8 then

end = true;

end if

end if

if not

lin++

end if

if col+1 = size (Tcol) then

col = 0;

if not

col = col+1;

end if

end while

end

II.3.2.2 Extraction process

In order to extract a concealed image, the concept of projection has to be respected. During this step we project an original image. The steps to follow are the opposite of “Image Hide” Algorithm. We extract the bits of the least significant original image in order to combine them as bits of the image to be reconstituted. The algorithm is as it follows:

```
% Algorithm: “Image Extract”
End = false;
Tlin = PosProjV (image)
Nbr := 0;
Pix (24);
Lin = col = K = I = J = Bs = P = 0;
While non end do
If Nbr < 24 do
Extract b the bit of bs rank from the pixel (Tlin (lin), Tcol (col)) from the scheme P of the
original image;
pix:= concat (pix,b) ; // insert the bit on its position on the pixel pix
nbr = nbr +1;
if then
Assign pix to pixel (i,j) of the image to be extracted
j = j +1;
if j = number of columns of the image to be extracted
if i = number of lines of the image to be extracted
end = true
end if
j := 0 ;
end if
end if
if lin+1 = size (Tlin) then
p++ ;
if P = 3 then
bs ++
if bs = 8 then
end = true ;
```

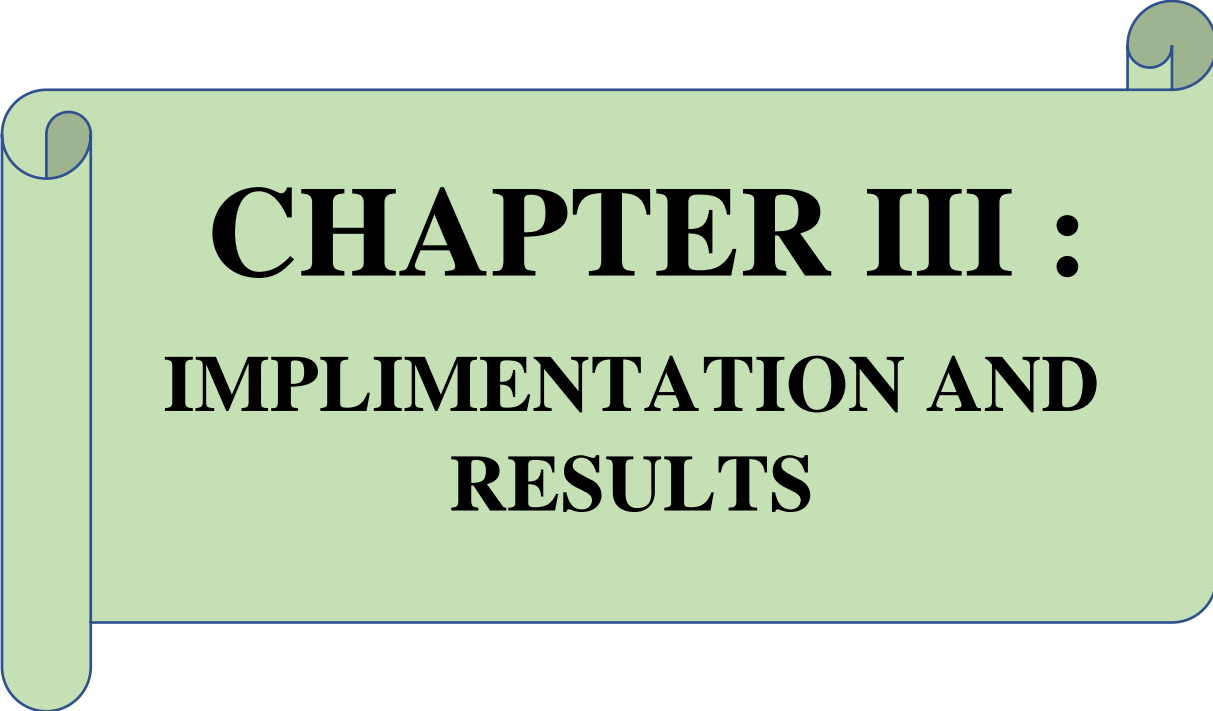


```
end if
end if
while
lin ++ :
end if
if col+1 = size (Tcol) then
col = 0 ;
while
col = col+1 ;
end if
end while
end
```

II.4 Conclusion:

In this chapter we have presented watermarking overview and also briefly discussed various watermarking techniques. Apart from this a brief and comparative analysis of watermarking techniques is presented with their advantages and disadvantages.

The suggested method will be a good and acceptable steganography scheme. the hidden message resides in more robust areas, spread across the entire stego image, and provides better resistance against Steganalysis process than other techniques.



CHAPTER III :
IMPLIMENTATION AND
RESULTS

III.1 Introduction:

The statistical tests are intended to verify whether the properties of the inserted image have been modified. In general, the decision is made by comparing the quality standards of a particular image to the standards. A watermark algorithm is said to be effective if the resulting metric measures are equal to the criteria. In this chapter, we examined the results obtained in our work and compare them with methods LSB based on many statistical measures. In addition, objective cognitive quality measures are used as an alternative method of determining the differences that result from a picture watermark.

III.2 Materials Used in Development:

The application is developed on a PC with the characteristics next:

- Operating System: Windows7 64-bit.
- Ram: 8 GB.
- Processor: Intel® Core™ i3-3rd Gen

The chosen programming language is very efficient to develop the application. This is the C++.

III.3 Image Quality Metrics

Statistical tests aim at investigating whether the characteristics of an input image have been modified or not. Generally, a decision is taken by comparing the quality metrics of a given image with norms (Avcibas et al., 2003). A watermarking algorithm is said to be efficient if the yielded metric measures are equal to the norms (Cox et al., 2008). In this work, we investigated the quality performance of the proposed watermarking method using numerous statistical metrics. Additionally, perceptual objective quality measures are exploited as an alternative approach to quantify the dissimilarities caused by image watermarking (Lin et al., 2011). The investigated metrics are as follow:

III.3.1 Mean square error (MSE)

MSE stands for the mean squared difference between the original image and the projected image. It is calculated by formula 3. a_{ij} is the value of the pixel at the coordinates (i, j) in the original image. b_{ij} is the pixel's value at the same coordinates in the corresponding generated image [12].

$$MSE = \left(\frac{1}{M \times N} \right) \sum_{i=1}^M \sum_{j=1}^N (a_{ij} - b_{ij})^2 \quad (3)$$

III.3.2 Peak Signal to Noise Ratio (PSNR)

PSNR, given by Eq. 4, is a classical quality index defined as the ratio between the maximum possible pixel value (e.g., equals to 255 in case of RGB color images) and the mean square error [13]. It is given by:

$$PSNR = \frac{10 \log_{10} 255^2}{MSE} \quad (4)$$

PSNR of RGB color images can be calculated by evaluating then summing up MSEs of all channels.

That's to say, the peak value $\frac{255^2}{MSE}$ is replaced with $\frac{255^2 \times 3}{\sum_{i \in \{R,G,B\}} MSE_i}$. PSNR is more consistent with the presence of error compared to the SNR.

III.3.3 Average Difference (AD)

AD is the difference average between the original and the cover image. [12] AD is given by the Eq. 5:

$$AD = \frac{\sum_{i=1}^M \sum_{j=1}^N (a_{ij} - b_{ij})}{MN} \quad (5)$$

III.3.4 Maximum Difference (MD)

MD, given by Eq. 6, is the maximum difference among pixels of the original image and their corresponding ones in the cover image. [12]:

$$MD = MAX |a_{ij} - b_{ij}| \quad (6)$$

III.3.5 Peak Mean Square Error (PMSE)

It stands for the mean square error (MSE) based on the square of the maximum value among original image pixels. [12]:

$$PMSE = \frac{1}{MN} \times \frac{\sum_{i=1}^M \sum_{j=1}^N (a_{ij} - b_{ij})^2}{[MAX(a_{ij})]^2} \quad (7)$$

III.3.6 Normalized Cross-Correlation (NCC)

$$NCC = \frac{\sum_{i=1}^M \sum_{j=1}^N (a_{ij} \times b_{ij})}{\sum_{i=1}^M \sum_{j=1}^N (a_{ij}^2)} \quad (8)$$

III.3.7 Structural Content (SC)

$$SC = \frac{\sum_{i=1}^M \sum_{j=1}^N (a_{ij}^2)}{\sum_{i=1}^M \sum_{j=1}^N (b_{ij}^2)} \quad (9)$$

III.3.8 Laplacian Mean Square Error (LMSE)

$$LMSE = \frac{\sum_{i=1}^M \sum_{j=1}^N (o(a_{ij}) - o(b_{ij}))}{\sum_{i=1}^M \sum_{j=1}^N (o(a_{ij}))^2} \quad (10)$$

where $O(a_{ij}) = a_{i+1j} + a_{i-1j} + a_{ij+1} + a_{ij-1} - 4a_{ij}$

III.3.9 Normalized Absolute Error (NAE)

$$NAE = \frac{\sum_{i=1}^M \sum_{j=1}^N |a_{ij} - b_{ij}|}{\sum_{i=1}^M \sum_{j=1}^N |a_{ij}|} \quad (11)$$

III.3.10 Robustness Test (BER)

Robustness test aims at examining the capability of a system to resist signal modifications in real-life applications. It is measured by using Eq. 12.

$$BER = \frac{Ext_{bit}}{T_{bit}} \quad (12)$$

where, Ext_{bit} is the number of successfully extracted watermark bits, and T_{bit} is the total number of original watermark bits.

III.4 Direct Image Projection Analysis:

1 - The relationship between the size of the image and the corresponding max size of the watermark. The distance and angle have respectively been set to 2.0 and 30° for both vertical and horizontal projection.

Fig 3.1 and Fig 3.2 show the difference between a small and big watermark from the cover image.

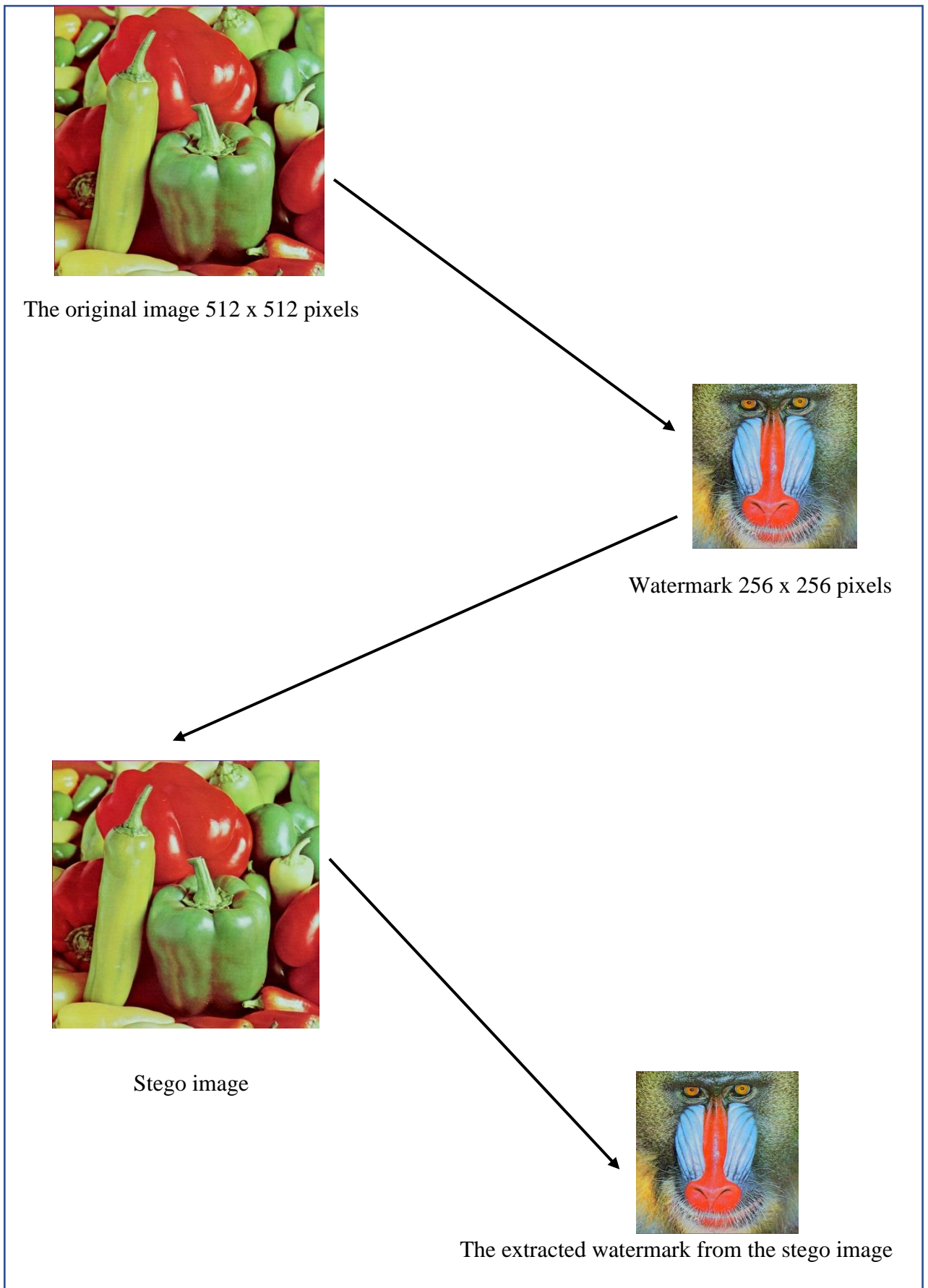


Figure 3.1 Hiding A small watermark in the Cover Image using the Projection method

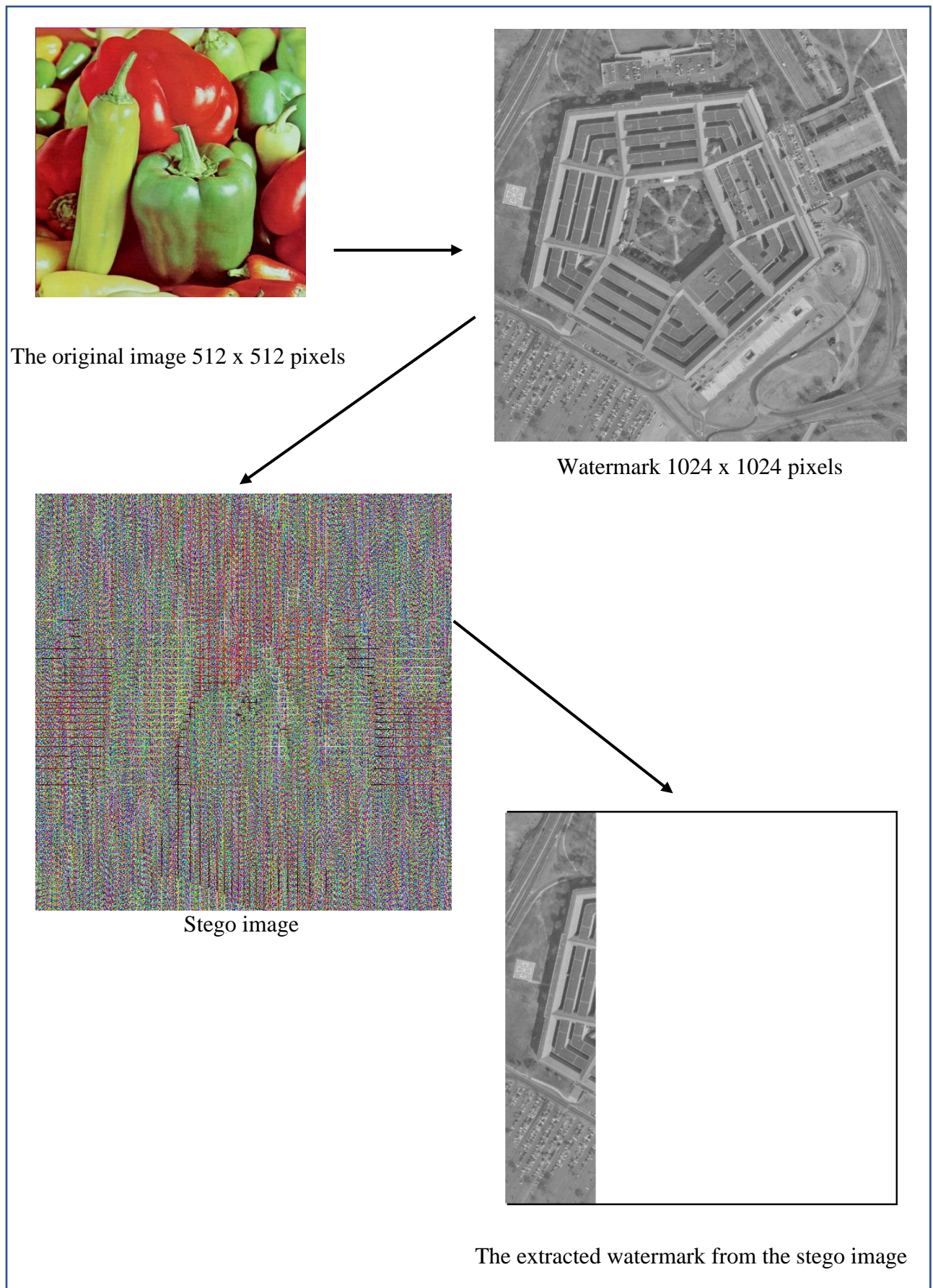


Figure 3.2 Hiding A big watermark in the Cover Image using the Projection method

watermark size	64x64	128x128	256x256	512x512	1024x1024
BER %	100	100	100	92.71	23.17

Table 3.1: The Relationship Between the Size of the Image and the Corresponding Max Size of the Watermark.

From Table 3.1, it appears that

- As long as the watermark size is smaller than the original image size, the BER percentage will reach 100%. (the hidden watermark is extracted completely).
- when the watermark size borders or exceeds the size of the original image, the BER percentage decreases. (the hidden watermark is partially refundable).
- the size of the watermark must be smaller than the size of the original picture.

2 - Some outcomes yielded by our proposed technique in different scenarios where the images from up to down are the original image, the watermark, the generated cover image and the extracted watermark (see fig 3.3). (a) 66x66 pixels watermark and 225x225 pixels image (b) 200x200 pixels watermark and 225x225 pixels image (c) 220x220 pixels watermark and 225x225 pixels image.

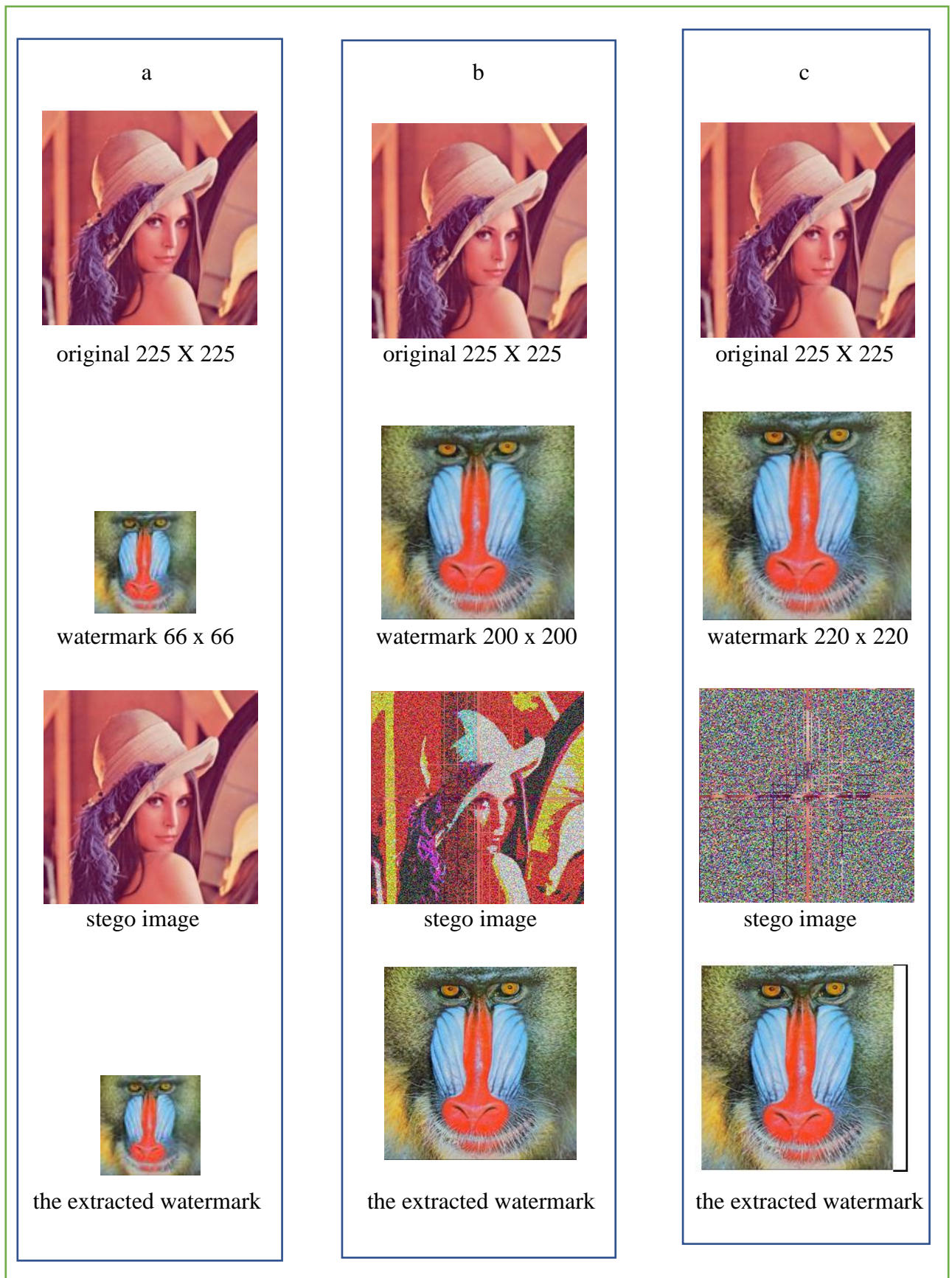


Figure 3.3 Some outcomes yielded by our proposed technique in different scenarios

➤ Results:

Figure (a) shows that when the watermark is smaller in size than the original image, there is no change in the stego image. The cover before and after the hiding is the same.

Figure (b) shows that when the watermark is almost the same size with the original image, there is a noticed change in the Stego image. The cover before and after the hiding is not similar.

Figure (c) shows that when the watermark and original images have the same dimensions, the Stego image is totally damaged. The cover before and after hiding is deformed, incomplete and not identical to the original.

3. The effect of the rotation angle on the hiding available proportion. The image size and distance are 250x250 and 1.5 respectively in all cases. (Watermark size is 66 x 66)

Angle (rad)	0	0.26	0.52	0.78	1.04	1.30	1.57
Available proportion %	0	89.11	87.6	79.56	50.12	15.68	0.001

Table 3.2: The effect of the rotation angle on the hiding.

➤ From Table 3.2, we note that as the rotation angle increases, the available hiding ratio decreases in image size.

➤ There is an inverse relationship between angle and percentage of disappearance, the larger the rotation angle, the less pixels used in the masking process.

4. The effect of the distance on the hiding available proportion. The image size and angle are 250x250 and 0.5 respectively in all cases. (Watermark size is 66 x 66)

Distance	0.4	0.8	1.2	1.6	2.0	2.4	2.8
Available proportion %	45.15	69.88	82.44	89.11	92.92	92.92	91.39

Table 3.3: The effect of the distance on the hiding.

➤ Note from the table3.3 that the greater the distance (a specific distance), the greater the hiding percentage available in the image size, meaning that there is a direct relationship between the distance and the percentage of disappearance. (but the distance shouldn't exceed certain value).

5. Quality metrics results yielded by the proposed method compared to the conventional LSB substitution. (The original image size is 512 x 512)

Method	Secret message (Kbytes)	MSE	PSNR	AD	MD	PMSE	BER	NCC	SC	LMSE	NAE
Proposed	8	0,04142	61,95870	0,00110	1	7,37E-07	100	1	0,99999	-8,47E-08	0
	16	0,08122	59,03397	-0,00282	1	1,45E-06	100	1	0,99998	-1,16E-07	0
	32	0,16495	55,95738	-0,00515	1	2,94E-06	100	1	0,99996	-6,24E-07	0
	64	0,33087	52,93419	-0,01885	1	5,89E-06	100	1	0,99982	-1,70E-06	2,98E-05
	128	1,25611	47,14051	-0,04906	3	2,24E-05	100	1	0,99963	-2,75E-06	1,75E-03
	256	9,03777	38,57019	-0,22374	7	1,61E-04	100	1	0,99802	-9,27E-06	9,33E-03

Conventional LSB	8	0,1108	57,9861	-0,016	1	1,72E-06	100		0,5999	6,70E-07	0
	16	0,2099	55,3564	-0,0307	1	3,25E-06	100		0,5873	6,40E-07	0
	32	0,7912	50,33585	-0,0828	2	0,00001	100		0,4722	5,90E-07	0,0009
	64	6,9511	42,68024	-0,3065	8	0,0001	100		0,1873	5,80E-07	0,0053
	128	8,6301	42,0279	-0,3434	8	0,0001	100		0,0981	5,30E-07	0,0099
	256	69,6951	27,71169	-3,6689	67	0,0082	100		0,0012	5,20E-07	0,0616

Table3.4: Quality Metrics Results.

- We notice from the table 3.4 that the quality measures differ between conventional LSB method and the projection method.
- Results obtained when using a method Projection shows the best quality compared to the LSB method.
- We notice from the table in the two methods that the value of MSE is decreasing, the value of PSNR increases, and AD gives negative values, MD is variable, PMSE is variable, BER is constant at 100, NCC is constant at 1, SC approaches 1, LMSE is variable, and NAE approaches zero.

All these results indicate that our method is more accurate than the LSB method.

The following figures show the difference between the two methods

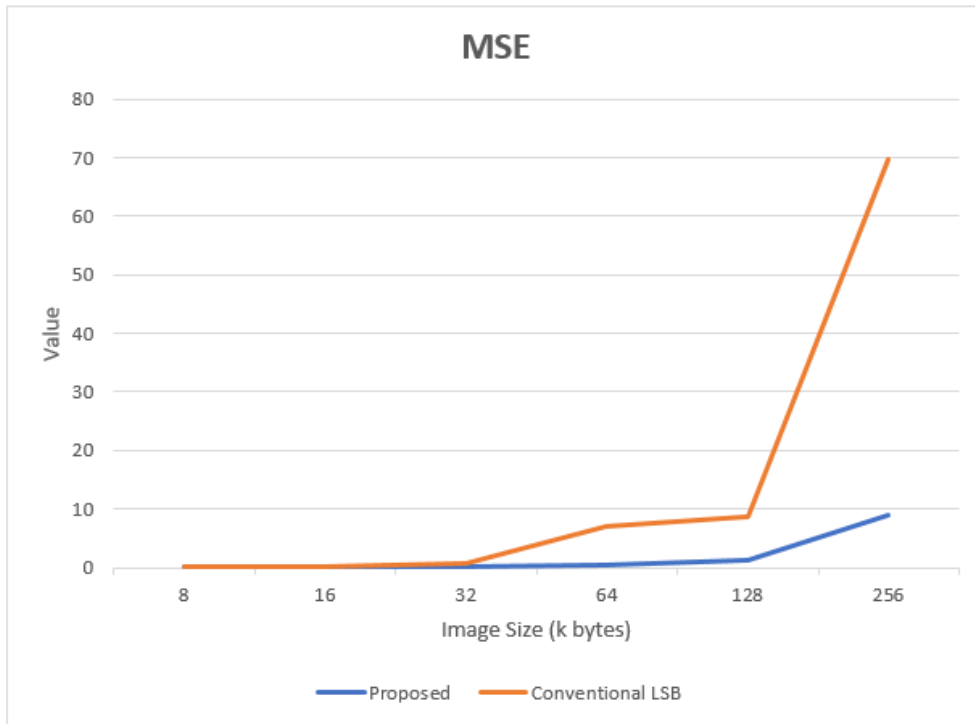


Figure 3.4. Comparison between the proposed and the LSB methods in MSE parameter

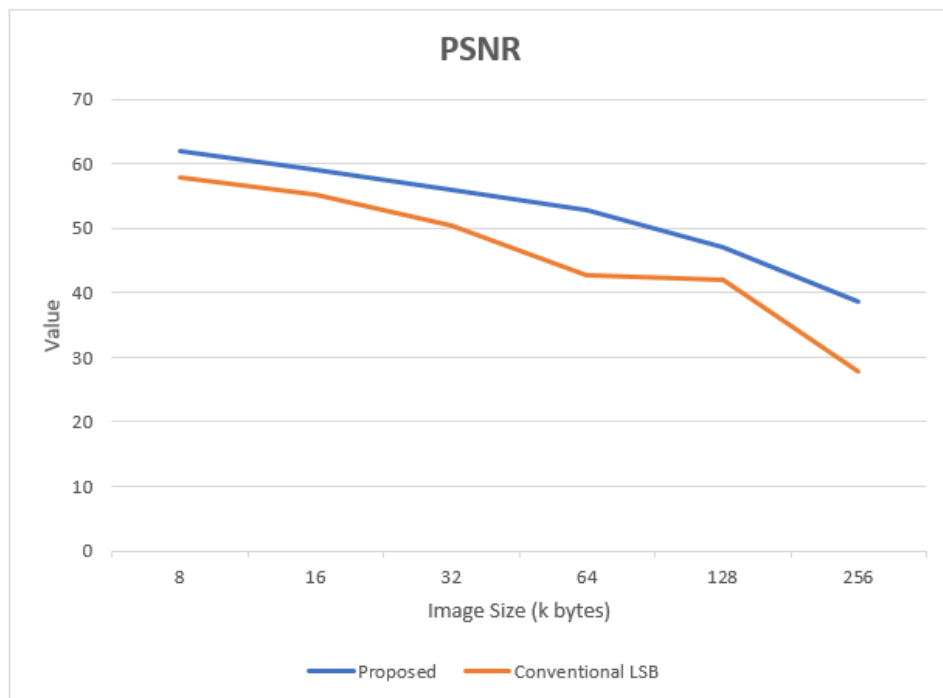


Figure 3.5. Comparison between the proposed and the LSB methods in PSNR parameter

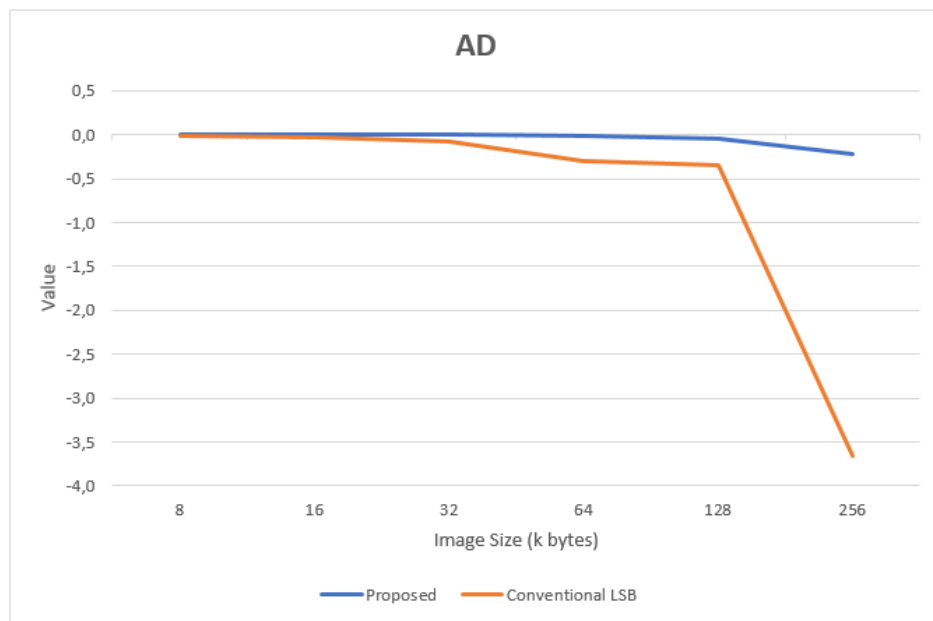


Figure 3.6. Comparison between the proposed and the LSB methods in AD parameter

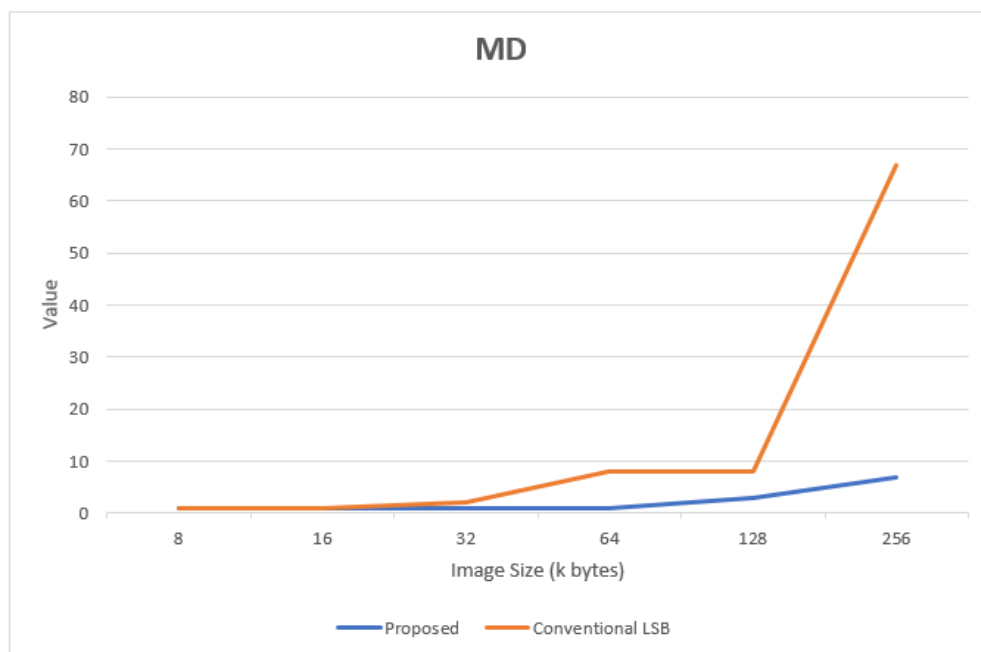


Figure 3.7. Comparison between the proposed and the LSB methods in MD parameter

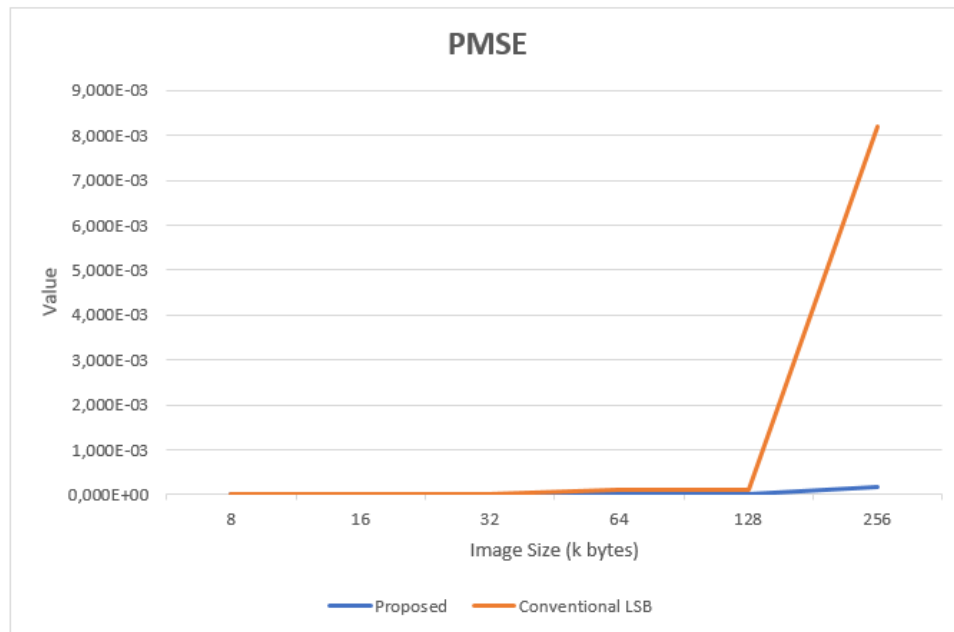


Figure 3.8. Comparison between the proposed and the LSB methods in PMSE parameter

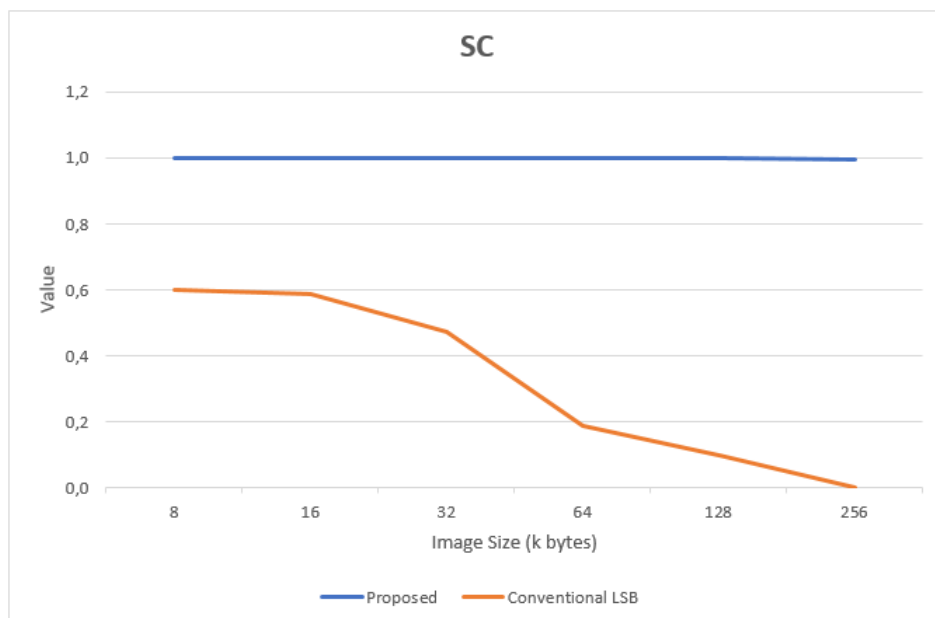


Figure 3.9. Comparison between the proposed and the LSB methods in SC parameter

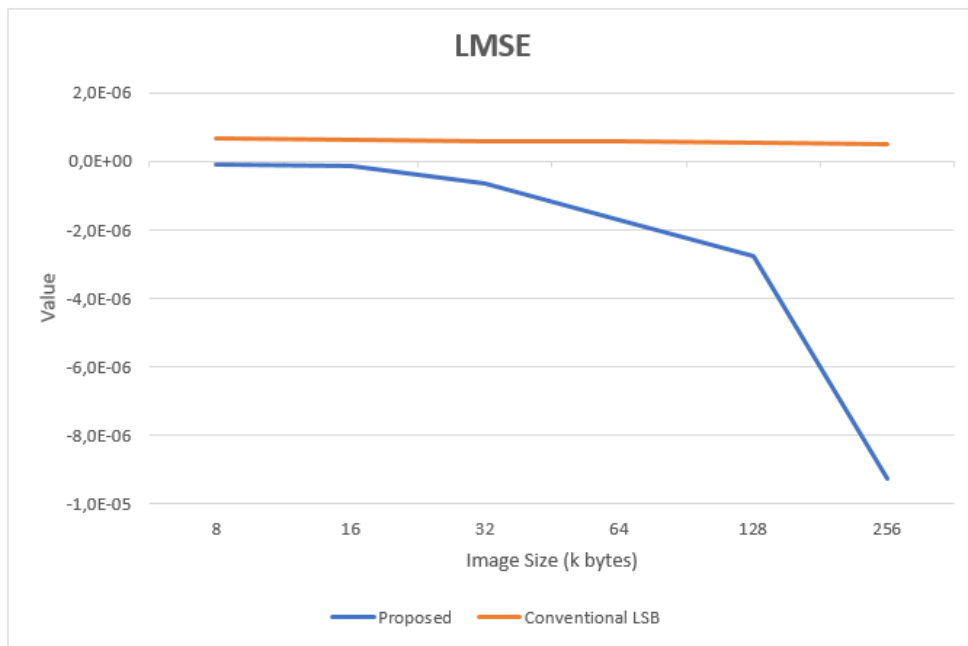


Figure 3.10. Comparison between the proposed and the LSB methods in LMSE parameter



Figure 3.11. Comparison between the proposed and the LSB methods in NAE parameter

III.5 Security Analysis

- The outcomes of attacking cover images generated by the proposed method

Steganalysis Method	Tool	Detection Outcome
Jsteg	StegDetect 0.4	Negative
Jphide	StegDetect 0.4	Negative
Outguess	StegDetect 0.4	Negative

Table3.5: The Outcomes of Attacking.

➤ From table 3.5 we deduce that the three methods (jsteg, jphide and outguess) can't detect the confidential information in the stego image so our method is very confident.

III.6 Integrity Analysis

In order to demonstrate the efficiency of our proposed stego method, it is necessary to prove not only its robustness and security but also its integrity. During transmission, hidden data can be lost due to image manipulation that is done by some steganalysis. The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload. If the hidden message was hard to be detected, image manipulation (such as; filter, image compression. etc) will be done.

In order to prove the integrity of our steganography method, we made some analysis under the same assumption of transmitted images over Gmail, WIFI (AD HOC) and external devices (USB)... etc. The results obtained in term of number of successfully extracted watermark bits and robustness test (eq.12) are illustrated in the following table.

Size of original image	Size of watermark	WIFI		Gmail		USB	
		BER	Ext-bit	BER	Ext-bit	BER	Ext-bit
225x225	66x66	100	4356	100	4356	100	4356
225x225	200x200	100	40000	100	40000	100	40000
225x225	220x220	100	48400	100	48400	100	48400

Table3.6 Results of transmission stego image through different methods

➤ From the following table, we can notice that when transmit the stego image through Wifi, Gmail and Usb device the BER remains 100 % after the extraction (the stego image keeps its watermark perfectly without wasting). In addition to that, the value of Ext-bit remains the same after the transmission and the extraction.

III.7 Conclusion:

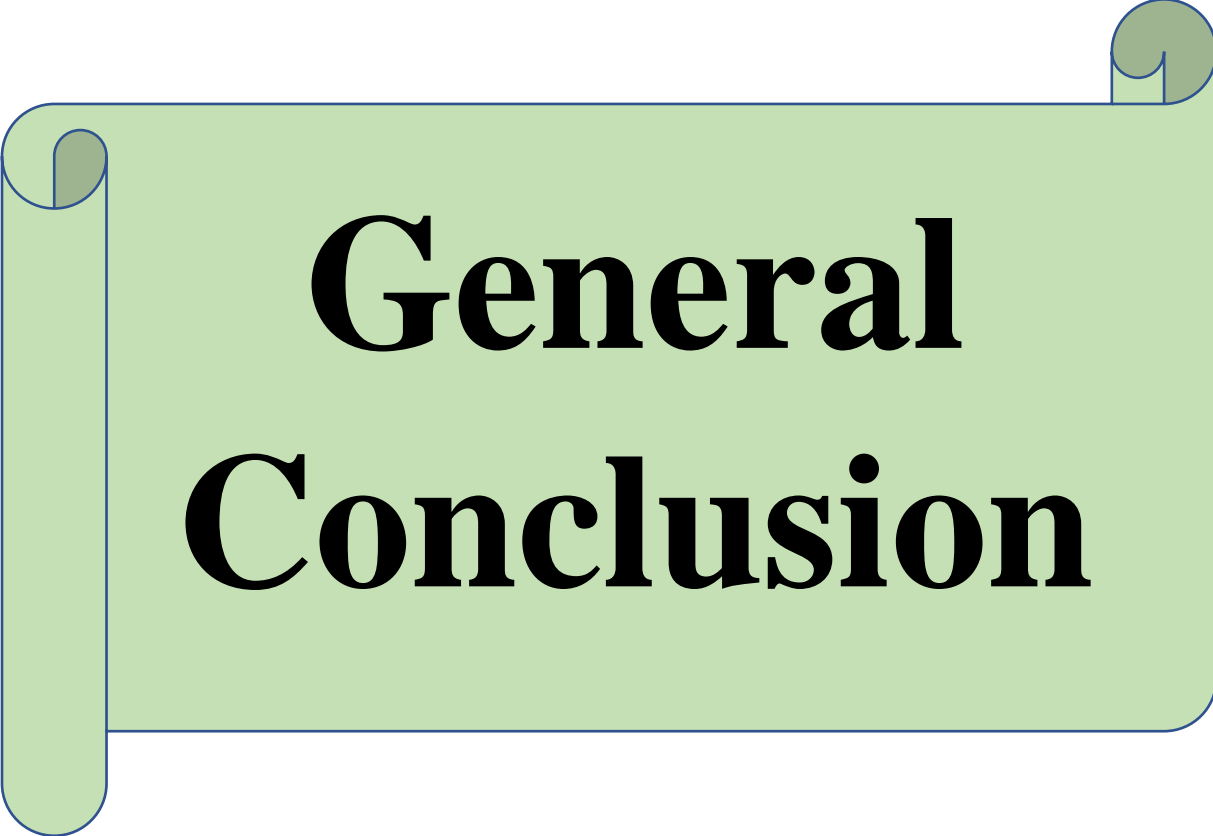
This chapter represented the following results:

- The size of the watermark mustn't exceed the size the covered picture.
- The distance plays an important role in saving the quality of watermark (the distance of projection).
- The value of the angle of rotation is also a major factor in the process.

After the comparison of results of our proposed method with the conventional LSB we found that our way is more effective specially through the outcomes of MSE and PSNR parameters.

Although we had exposed the stego image to many steganalysis method, the watermark couldn't be discovered.

Our method proved its efficiency in saving the quality of the stego image during the transmission.



General Conclusion

GENERAL CONCLUSION

In this thesis, the various steganography techniques in both spatial and transform domains are mentioned. The different proposed technique is based on factors like the increase in the stego image quality, low MSE, Higher PSNR rates and embedding capacity to provide the Robust Image and to avoid various attacks and High secure image analysis method are illustrated.

After having studied a fairly diverse panel of watermarking techniques, we ended up with implemented substitution of projection.

We can consider this technique as an addition to the field of the steganography and watermarking.



Bibliography

Bibliography

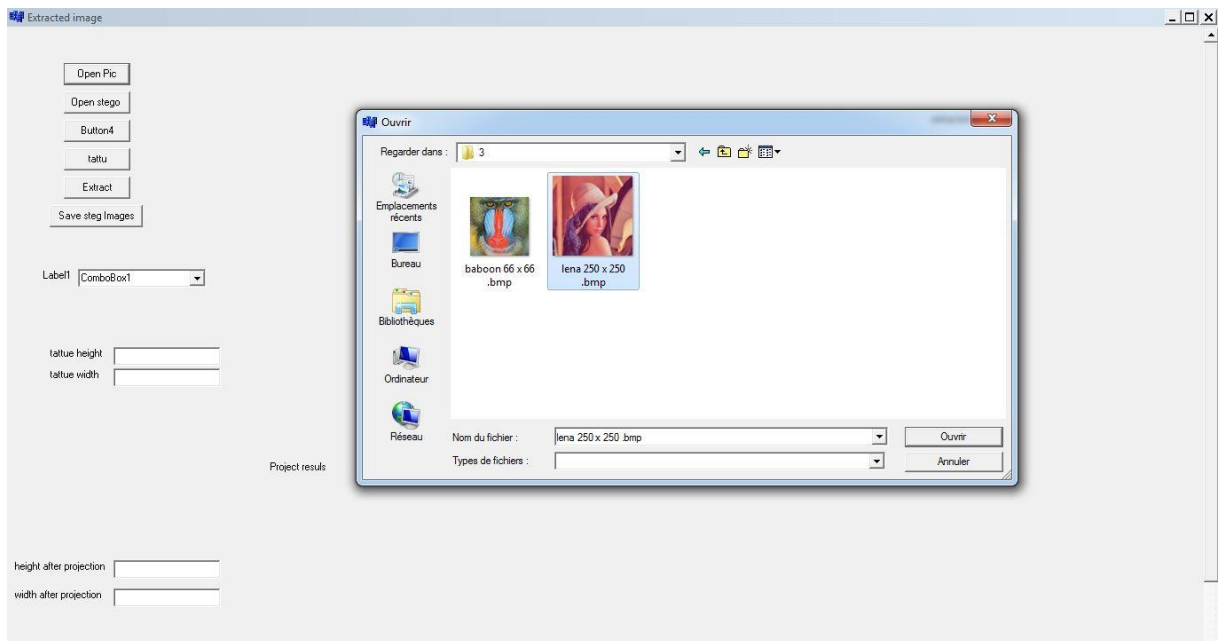
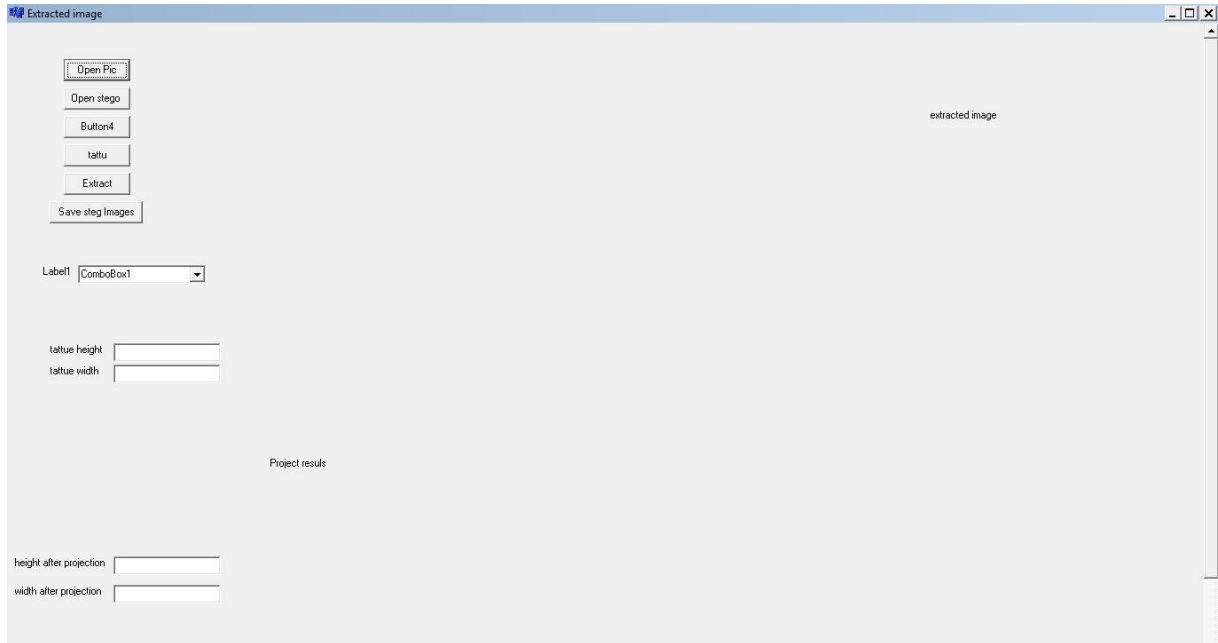
- [1] **Husrev T. Sencar, Mahalingam Ramkumar and Ali N. Akansu.** Data Hiding Fundamentals and Applications: Content Security in Digital Media. Elsevier Academic Press: Newark, New Jersey, 2004.
- [2] **Nihad Ahmad Hassan, Rami Hijazi and Helvi Salminen.** Data Hiding Techniques in Windows OS: A Practical Approach to Investigation and Defense. Elsevier Inc: United States, 2017.
- [3] **Jessica Fridrich.** Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 2010.
- [4] **Frank Y. Shih.** Digital Watermarking and Steganography: Fundamentals and Techniques (Second Edition). Taylor & Francis Group, LLC: N Y, 2017.
- [5] **Harpreet Kaur and Jyoti Rani.** A Survey on different techniques of steganography. ICAET, 2016.
- [6] **Pranali R. Ekatpure and Rutuja N Benkar.** A Comparative Study of Steganography & Cryptography. IGSR: Volume 4 Issue 7, July 2015.
- [7] **M. Abinaya.** Analysis of Cryptography and its Types. ISSN 2321 3361 © 2019 IJESC.
- [8] Cryptography: just for beginners. © Copyright 2015 by Tutorials Point (I) Pvt. Ltd.
- [9] **Ravi Kumar Choubey, Ahtisham Hashmi.** Cryptographic Techniques in Information Security, 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN: 2456-3307.
- [10] **Preeti Parashar and Rajeev Kumar Singh.** A Survey: Digital Image Watermarking Techniques. International Journal of Signal Processing, Image Processing and Pattern Recognition. MITS, Gwalior, India. Vol. 7, No. 6 (2014).
- [11] **Ritu Rawat, Nikita Kaushik & Soumya Tiwari.** Digital Watermarking Techniques. Graphic Era University, Dehradun, India. Vol. 5, Issue 4, April 2016.
- [12] **Ahmet M. Paul E. Fisher S.** Image Quality Measures and Their Performance IEEE. Trans. On.Commu., Dec.1995, 43, (12), pp. 2959-2965.
- [13] **Soliman M.M Hassanien A.E. Onsi, H.M.** An adaptive watermarking approach based on weighted quantum particle swarm optimization, Neural Comput. Appl. 2015, (27), pp. 469–481.

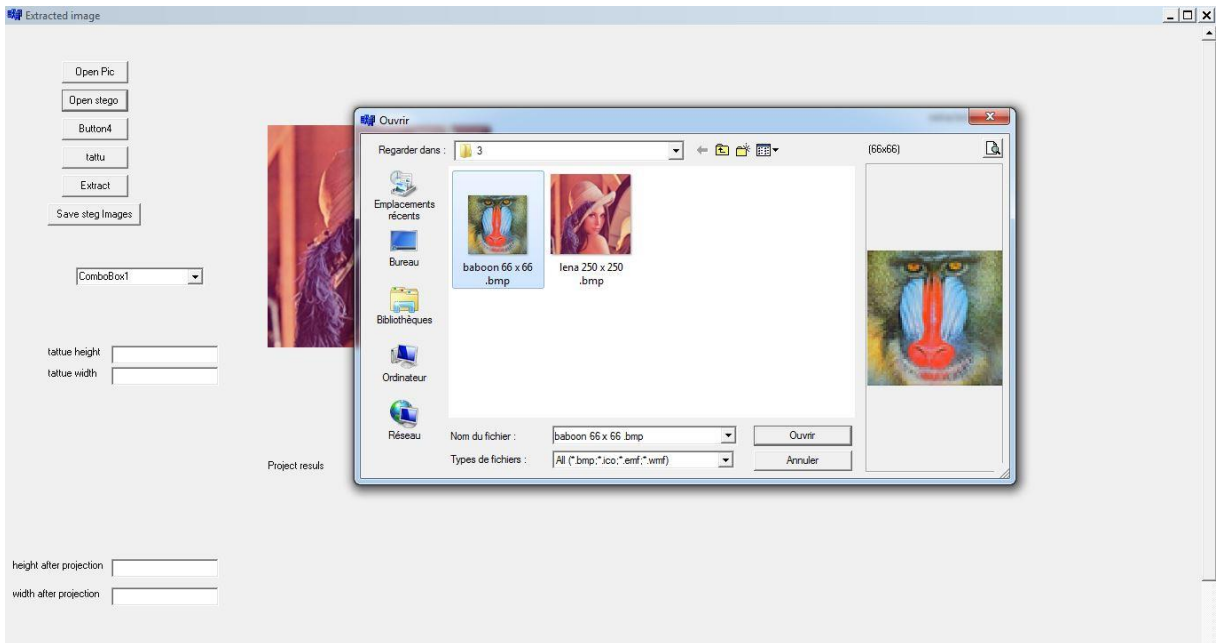
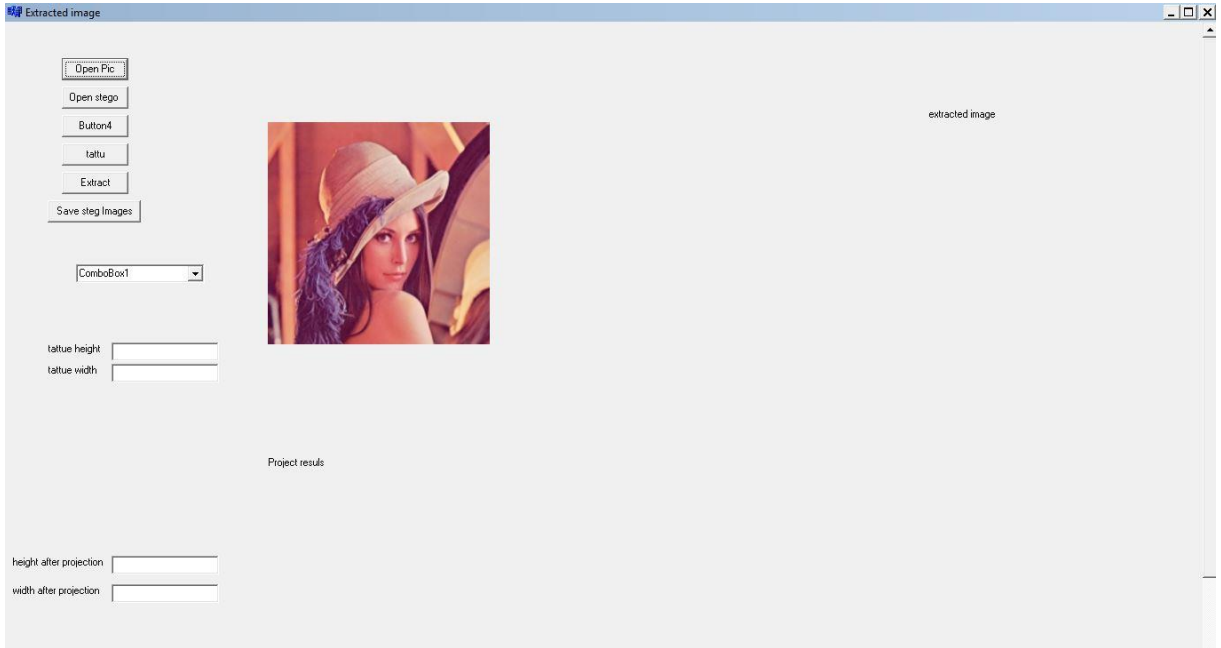


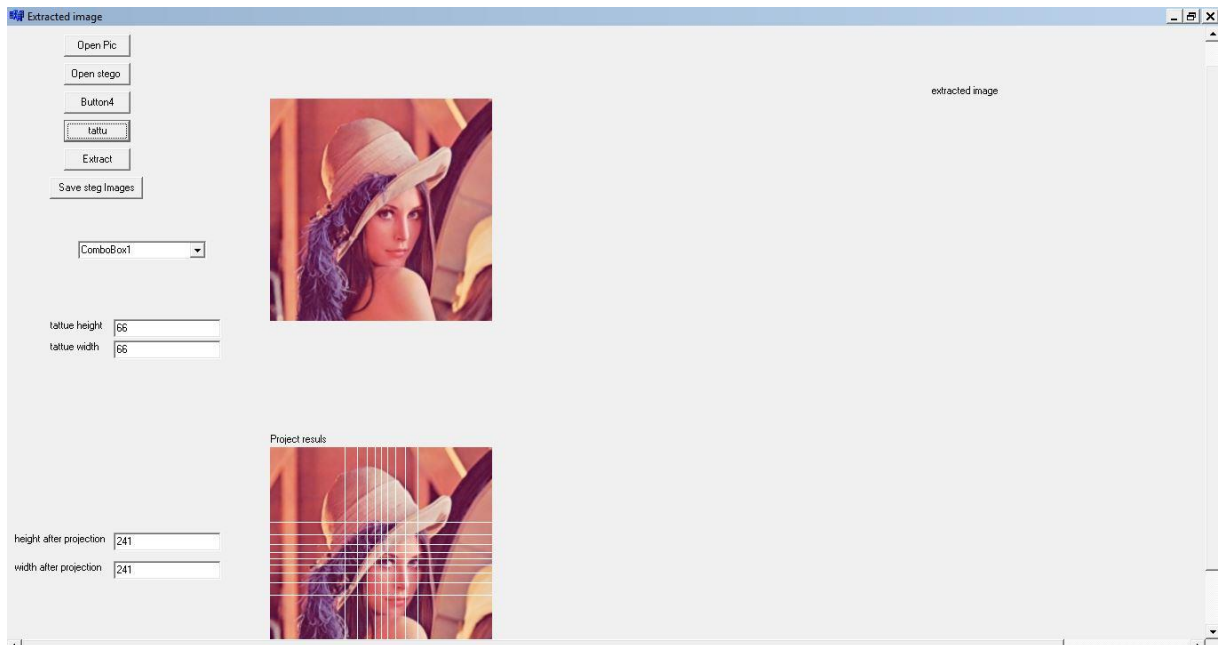
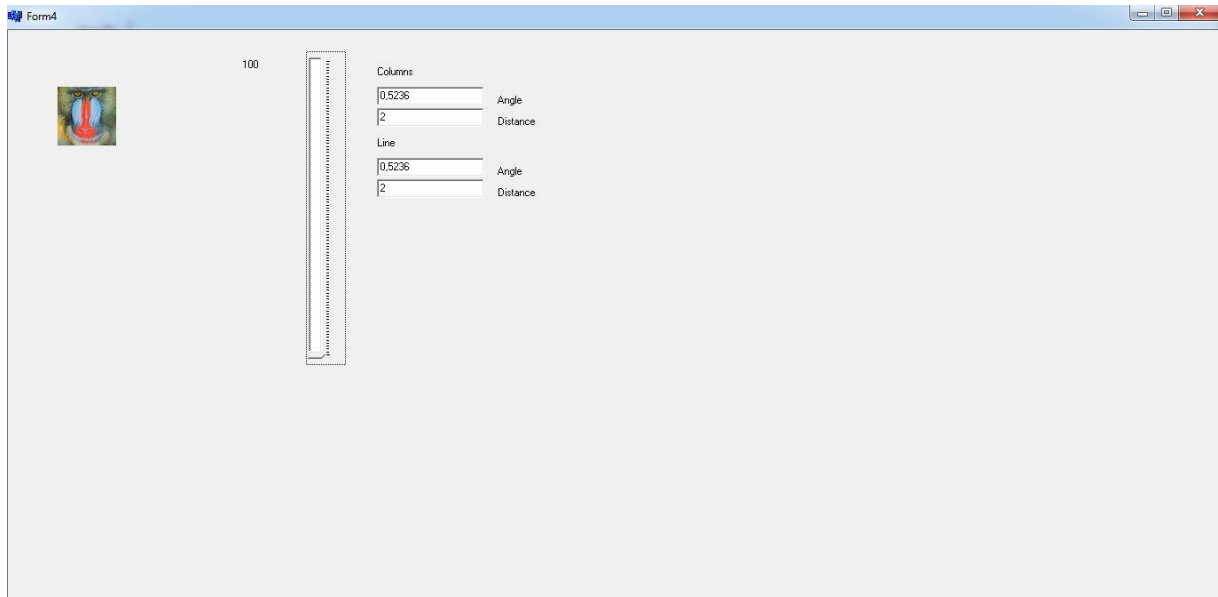
Annex

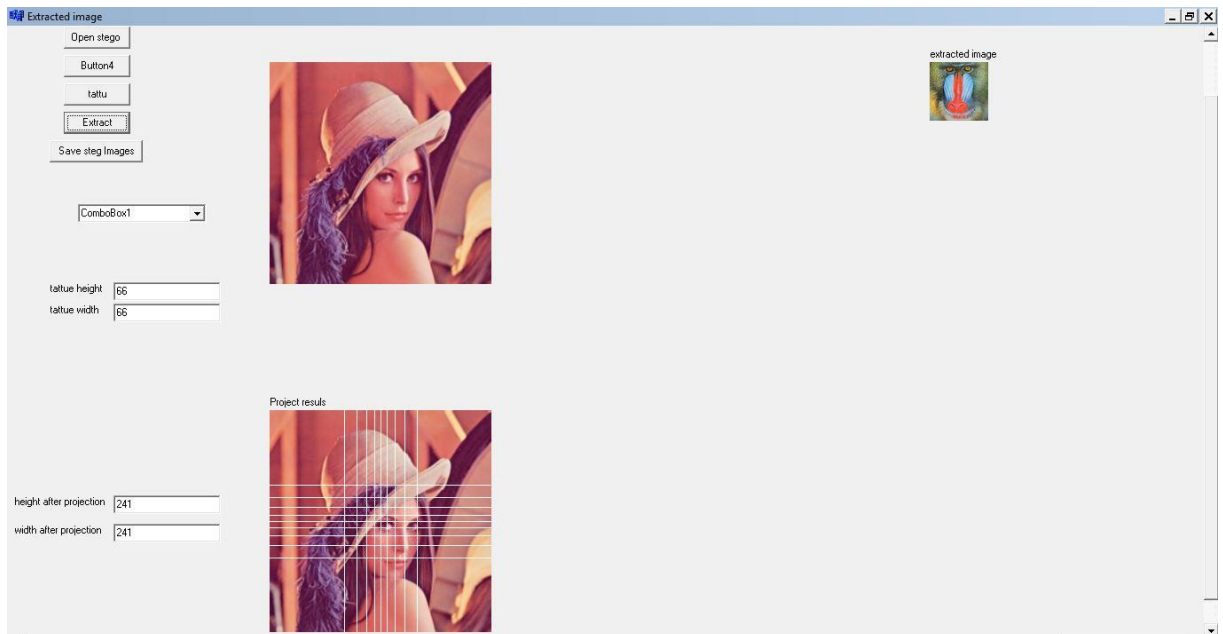
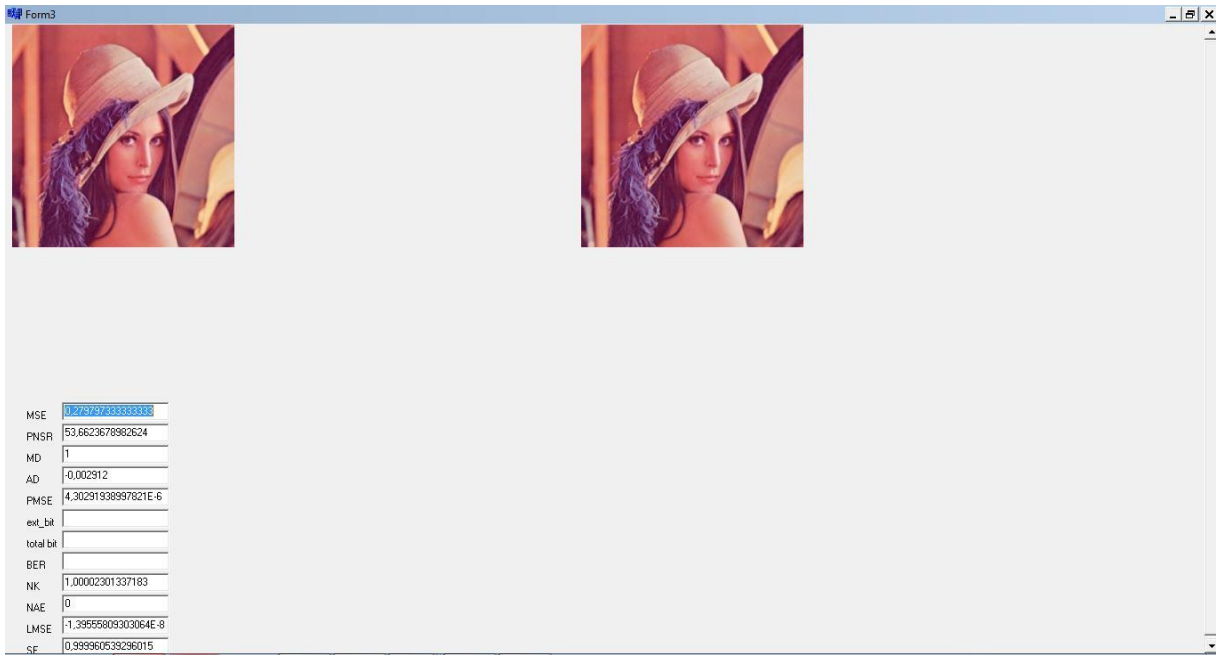
Annex

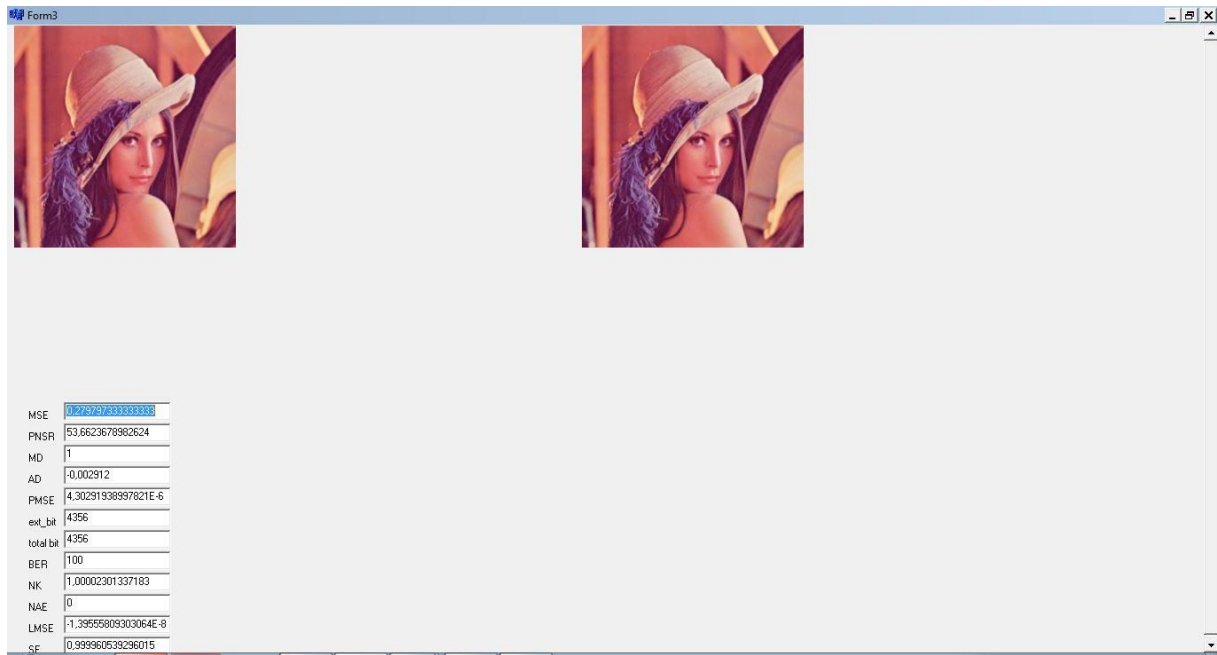
These are some pictures related to the used program











```

C++ Builder 6 - Project1
File Edit Search View Project Run Component Tools Window Help |<None>
Standard | Additional | Win32 | System | Internet | Dialogs | Win 3.1 | Samples | ActiveX |
Unit1.cpp
Unit1.cpp
//-----
#include <vol.h>
#pragma hdrstop

#include "Unit1.h"
#include "Unit2.h"
#include "Unit3.h"
#include "Unit4.h"
#include "Unit5.h"
#include "Math.h"
//-----
#pragma package (smart_init)

#pragma resource "*.dfm"
TForm1 *Form1;
char *Bit,*Bit9;
char Bits[24];

Double theta,OVo,OPt,OPo,length; int pos, nbout ,nbrep ;
bool end_hiding;

div_t rem , opt1 , opt2;
double collin;
int i, taille;
int *lin3;
int count;
int *lin2;
int *lin4, *lin8,*lin9;

```