CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

Visually Meaningful Image Encryption

by

Sultan Mehmood

A thesis submitted in partial fulfillment for the degree of Master of Philosophy

in the

Faculty of Computing

Department of Mathematics

2020

Dedicated to my beloved parents

CERTIFICATE OF APPROVAL

Visually Meaningful Image Encryption

by

Sultan Mehmood

(MMT163016)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Nasir Siddique	UET, Texla
(b)	Internal Examiner	Dr. Qamar Mehmood	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Supervisor Name
Dr. Rashid Ali
November, 2020

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
November, 2020

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
November, 2020

Author's Declaration

I, **Sultan Mehmood** hereby state that my M Phil thesis titled "**Visualy Meaningful Image Encryption**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my M Phil Degree.

(Sultan Mehmood)

Registration No: MMT163016

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**Visually Meaningful Image Encryption**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of M Phil Degree, the University reserves the right to withdraw/revoke my M Phil degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Sultan Mehmood)
Registration No: MMT163016

Acknowledgements

All praise to Almighty Allah, the most Benevolent and Merciful, the Creator of Universe and man, who gave me the vision and courage to accomplish this work successfully. A research project at any level is very difficult to be accomplished alone. The contributions of many people have made it possible for me to complete this work. I would like to extend my appreciation especially to the following.

First and foremost I extend my sincerest gratitude to my thesis supervisor Dr.Rashid Ali who has supported me throughout my thesis work in every possible way. He presented the things in simplest way. His efforts and encouragement is really appreciable. He gave me self-belief, and confidence and provided me his support and guidance all way along. Under the supervision of him I never felt anything difficult in my thesis. Dr.Rashid Ali provided me the friendly and comfortable environment to work in, without his guidance and support I would never be able to put this topic together.

The research oriented environment provided to students by Mian Amer Mehmood, Chancellor at CUST, Prof. Dr. Muhammad Mansoor Ahmed, Vice Chancellor at CUST and Dr.Muhammad Sagheer, Head of Department of Mathematics made the research work easier and more pleasant.

My friends, class mates and fellow research workers Tahir Bhai, Suleman Liaquat, Mujtaba Azim, Sohail Abid and Syed Burhan also helped me a lot and guided me whenever I needed it. Last but not least, I would like to pay high regards to my parents and all family members for their sincere encouragement and inspiration throughout my research work and lifting me uphill this phase of life.

(Sultan Mehmood)

Registration No: MMT163016

Abstract

Image encryption is a technique to convert an image into some coded form image so that it is not understood for an unauthorized person. Traditional image encryption schemes convert images into a texture or noise like shapes. But, noise or texture like images can be easily differentiated from normal images because of their appearance. So, to tackle this issue a scheme named as "Image encryption: Generating visually meaningful encrypted images" was proposed which generates meaningful encrypted images. By meaningful image, we mean that it looks like normal image but actually it hides the encrypted image into it and that is how we obtain some meaningful of the encrpyted image. The scheme has two phases; phase 1 converts the image into some texture or noise like shape and phase 2 then uses a reference image along with the pre-encrypted image to further hide it in the reference image. A reference image i a normal image, which must be double in size as compared to the original image. This provides an additional security to the pre-encrypted image and makes its appearance more protected. In this thesis, a complete review of the scheme has been presented and discussed along with its security analysis.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advance Encryption Standard
CWT	continuous Wavelet Transform
DES	Data Encryption Standard
DWTCT	Discrete Wavelet Transform based content transform
DWT	Discrete Wavelet Transform
GIF	Greatest Integer Function
IE	Image Encryption
LIF	least Integer Function
MPWLCM	Improved Piecewise Linear Chaotic Map
NEI	New Image Encryption
NIES	New Image Encryption Scheme
PWLCM	Piecewise Linear Chaotic Map
RC4	Rivest cipher 4
RSA	Rivest Shamir and Adelman
SPN	Substitution Permutation Network
VMEI	Visually Meaningful Image Encryption

Chapter 1

Introduction

It has always been a top priority of human being to secure the sensitive information. From the ancient Egypt till now, people have always tried to find the ways, from to protect the sensitive data. There are evidences which show that the ancient Egypt used secret symbols to keep their communication secure. There are ancient civilization which were very advanced, they used different techniques to keep their secret information protected. The use of pictorial like symbols in the encrypted data was very famous in the past, to deceive unauthorized reader.

In the current advanced era of advanced technologies. People communicate, share important and highly confidential information with each other over public network. Since the leakage of information can lead to a great disaster so there is a need of some modern methods that protect the data over Internet from going into the wrong hands. Cryptography is the platform that provides the methods capable to maintain the security of any data. It is the first branch of cryptology and highly effective in terms of security perspectives. The second branch works to break such a system that guarantees the security. The methods for securing data in cryptography usually contain an algorithm and a key (on which the security of the whole system depends). In order to communicate in a secure fashion, an encryption algorithm first transforms the original data into some coded version of it, so that it is not understandable to a person who is not intended to receive it; which is done using a secret key. Once the information is encrypted, it is all set to send over a public network. On the other end, receiver also performs some task to make the information readable. He decrypts using decryption algorithm and the decryption key. So, the algorithm must be well-known to everyone but the key must be kept hidden throughout in the exchange of the information.

The simplest and most famous example of such technique is “Caesar Cipher” [1]. It works on the basis of substitution where each alphabet is substituted with some other alphabet, basically each letter is shifted to a fixed number of places in the alphabets. There are other algorithms that have been used extensively like Hill cipher [2], DES [3], AES [4] etc. These algorithms work on the basis of different mathematical techniques like modulo arithmetics. Cryptosystem is further categorized as symmetric key and asymmetric key cryptography [5]. If in a security protocol, only one key is used by the sender and the receiver, then the cryptosystem is named as symmetric key crytosystem. whereas, if there are two keys involved in the system, one for encrypting the text and the other for decrypting it, then the system is called asymmetric key cryptosystem [5].

Since the invention of cryptographic techniques made the communication secure but the security of the cryptosystem is completely dependent on the key used in the encryption and decryption processes, so, it is necessary to keep it away from the reach of the hackers/attackers. The role of the second branch of cryptology then played its part by trying to know the secret communication without having the key. This branch is called cryptanalysis and the person who does so is recognized as cryptanalyst. There are different kinds of attacks that have been witnessed, we will talk about them in Chapter 2 of this thesis.

People also intend to secure images that require confidentiality. In our thesis, we will focus on image encryption schemes and how are they made more efficient and secure. Image encryption is a method that guarantees the security of the images by converting them into some meaningless pictures so that they are kept safe from unauthorized people. The procedure of encrypting images is slightly different as compared to the tradition message encryption schemes. First, the corresponding pixel values of the image are obtained and then several operations are performed on them and hence the required results are obtained. Once the image is encrypted in the conventional image encryption schemes, it takes a shape of noise-texture like image [6] which does not reveal any information of the original image. The two main roles, that take part for ensuring image encryption, are confusion and diffusion which are made possible using substitution and permutation tools. The idea of bringing confusion and diffusion [7] in image encryption schemes is to alter the image into noise or texture like form. Algorithms like Advanced Encryption Standards (AES) [4], elliptic curve elgamal, choatic systems [8] etc are used to make sure that confusion and diffusion [7] elements in the image. These two main elements of encrypting and decrypting an image are discussed in Chapter 2.

AES is a technique for altering the message into unintelligible format. It is also used to encrypt the images. The four main stages of AES are substitution bytes, shift rows, mix columns and add round key. Substitution of bytes is done by using a s-box [9] which is the only nonlinear function in AES. It provides confusion in the image. The operations such as shift rows and mix columns create diffusion in the image. The number of rounds that these steps are repeated depends on the key size used in the algorithm. There are 10, 12 and 14 rounds corresponding to the key sizes of 128, 192 and 256 bits, respectively. After the image is finally passed through these rounds, a texture or noise like image is obtained and finally considered as the image is in its encrypted version.

Chaos theory [10] is also implemented in image encryption algorithms because it is based on the functions which behave completely random. They provide confusion and a complete disorder in the pixel values of the original image and hence the encrypted image is hard to recognize. In 2012, Bao et. al. [11] proposed an image encryption scheme based on chaotic system using the substitution-permutation. There are other chaotic based image encryption algorithms such as [12], [13].

1.1 Contribution

In the scheme proposed by Bao and Zhou [14]. They found out that the noise or texture like encrypted images catch the attention of the attackers. Since, by appearance they are do not like normal images so it is obvious that they have been some encrypted form of plain images. In order to tackle with this issue they used a reference which looks like a normal image and hide the original plain image in the reference which become the encrypted form of the plain image and apparently looks like a normal image. In that way, they prevented the encrypted image to catch the attention of the attackers. In their scheme, the image is passed through two phases. In phase 1, original image is encrypted and converted in the form of noise or texture like by using any existing technique. In phase 2 DWTCT (Discrete wavelet transformation function) [15] is used with a reference image that hides the noise or texture like image in the reference image and hence makes it more secure as compared to existing techniques of image encryption Such technique are known as Visually meaningful image encryption schemes. The scheme is successfully implemented in the MATLAB as well to encrypt and decrypt the image. It gives a meaningful encrypted image. The algorithms for MATLAB are mentioned in the next chapters.

Thesis Layout

The 2^{nd} chapter of this thesis will cover the basics of cryptography along with the introduction with preliminaries of image encryption. Chapter 3 will be based on chaos theory along with piecewise linear chaotic map and how they are used in the cryptography to make more secure algorithm for image encryption. In the begning of Chapter 4, we will explain wavelet transform particularly discrete wavelet transform and will see how meaningful encrypted images are obtain using discrete wavelet transform. A complete review of scheme proposed by Bao and Zhou [14] is also mentioned in Chapter 4. The last chapter of this thesis will cover the security analysis of the scheme and conclusion.

Chapter 2

Preliminaries

In this chapter, we will discuss some basics points of cryptography along with its applications. Cryptographic attributes like confidentiality, integrity, authentication etc are discussed. The necessary ingredients that are helpful in the proposed scheme are also discussed.

2.1 Cryptography

Cryptography is the art of hiding the data in coded form. A sender uses the confidential information to convert in the coded form so that it can not be understood by any other person who is not allowed to get it. Cryptography is basically a system or a technique that is used to make the data secure until used in communication.

While studying the cryptography, we introduce commonly used named of two parties who share information with each other as Alice and Bob. We have some technical terms that are used in any cryptographic process by which Alice and Bob will communicate with each other. The original information that is sent by Alice to Bob that can be easily understood by anyone is called **Plaintext**. Plaintext cannot be sent in its original form rather it is changed into a form that cannot be understood and then this information will be sent to its intended receiver. This coded message which cannot be understood by an unauthorized person is called **Ciphertext**.

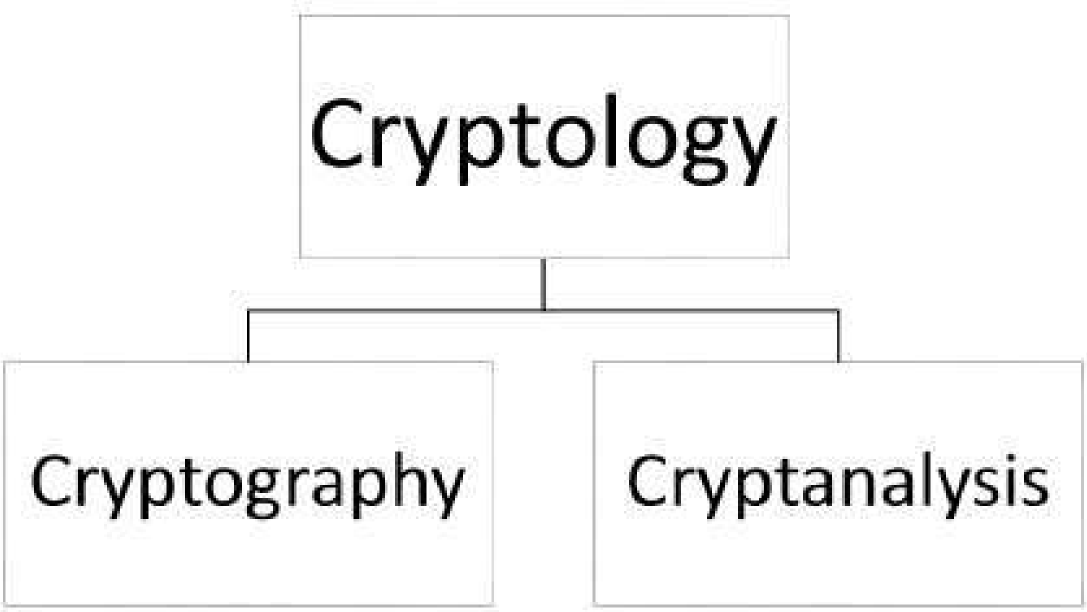


Figure 2.1: Branches of Cryptology

Ciphertext is also known as encoded information as it contains a form of the original plaintext that is meaningless for reading by a computer or a person without the proper key to decrypt it. **Decryption** is a process of turning coded message or ciphertext into readable plaintext. An algorithm that is used to alter the plaintext into ciphertext is known as **Encrption Algorithm**. A ciphertext cannot be understood to the receiver untill it is transformed back into the plaintext.

The algorithm that is used to get the plaintext from the ciphertext is called **Decryption Algorithm**. For conversion of plaintext to ciphertext and vice versa is done by the help of a very highly sensitive information, known as **Key**. This key must be kept secret during this process because the security of whole communication completely depends on it.
Here are some basic aspects of cryptographic [1] scheme that ensures the security of the system.

2.1.1 Confidentiality

In a simple manner, unapproved parties cannot approach the secret data. confidentiality refers to a situation where the data that has been sent by a sender can only be recognized by the actual receiver. Suppose, Alice wants to send some encrypted information to Bob. If another person, say, George obtains the encrypted information then he is unable to understand the information. This is called confidentiality that keeps the original information secret and secure.

2.1.2 Integrity

During transmission of information, integrity assures that the message was not altered or modified. It means that there is no change occurred in the original message during the storage or transmission to the designated receiver. For example, if Alice sends some encrypted information to Bob then integrity makes sure that the data is not altered or changed during sending or storing and it makes to Bob believe that the data is in its original form.

2.1.3 Authentication

A cryptographic scheme also contains authentication which means the sender's or recipient's identity can be verified. It makes sure that the data comes from a trusted source. It identifies the source of message and transmitter or receiver properly. In short, it ensures that the transmitter and accepter verify each other. Let us consider the situation where Alice and Bob follow a proper algorithm to communicate securely. They must be able to verify each other's identity with the help of cryptographic scheme in order to be avoid from being deceived. The authentication property helps participants to make sure that they are communicating with each other and not the attacker.

2.1.4 Non-Repudiation

In this cryptographic aspect, a sender cannot deny by sending the message at a later time. It means that if data is sent from Bob, then for Bob there is no more option to deny it at any stage later during communication. It will help both the sender and receiver to trust each other in any cryptographic protocol.

These properties help to provide secure and strong bond between sender and receiver. In cryptographic manners, it provides more reliability and authenticity that gives a better platform to fulfill the basic necessities of a secure communication.

There are two types of cryptographic methods. These methods are categorized by the use of keys in them.

1. Symmetric key
2. Asymmetric Key

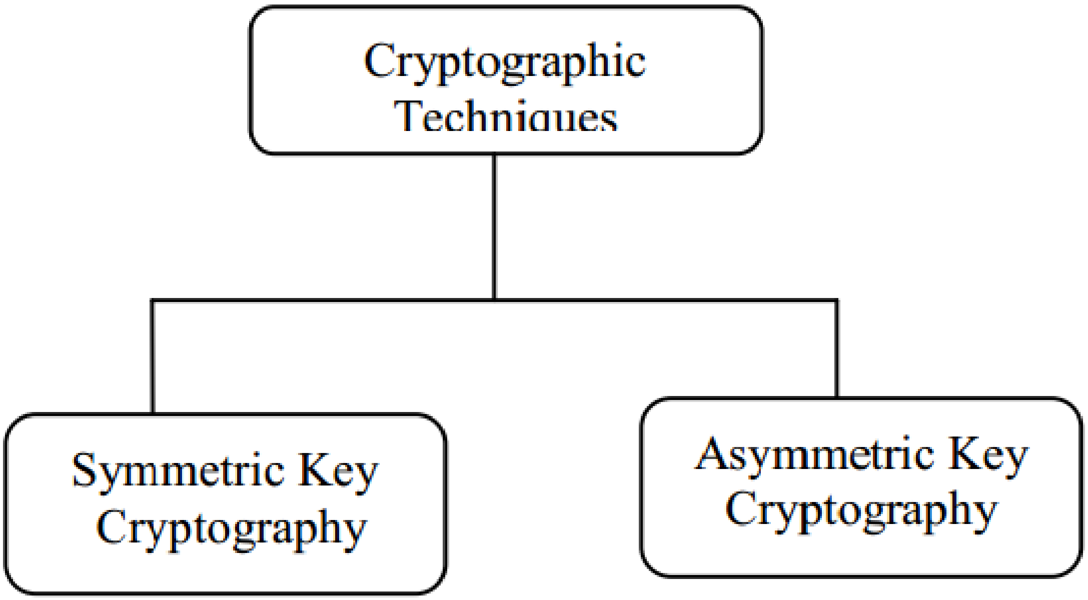


Figure 2.2: Cryptographic Protocols

2.1.5 Symmetric key Cryptography

Symmetric key Cryptography [2] is also famous as secret key cryptography. This is a form of encryption/decryption that involves single confidential key or its copy to cipher and decipher the data. It utilizes a confidential key that can either be a number, a word which is involved with a plaintext of message to convert the component in a ciphered message. In this type, two parties use a single key for the encryption and decryption. There may be the same key to obtain the decryption results for encrypted message. This was the only method which was used for secure communication until 1976.

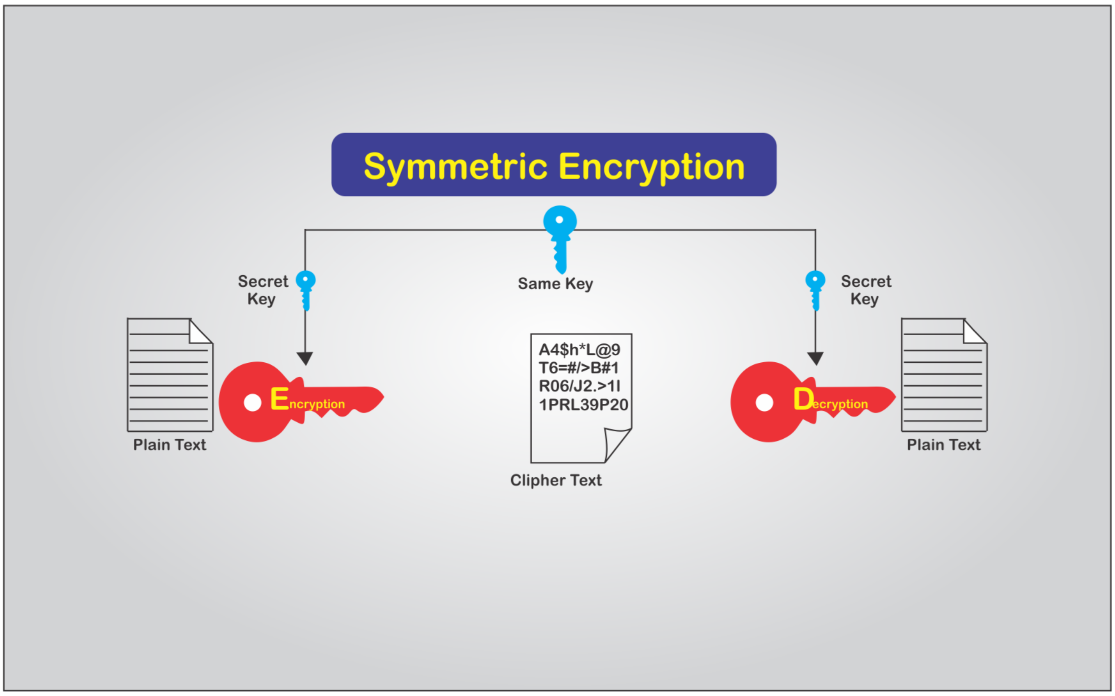


FIGURE 2.3: Symmetric Cryptography Diagram

Here, we will also look into the working of symmetric key cryptography. We consider two parties Alice and Bob for communication. Alice wants to communicate with Bob on an insecure channel, e.g, Internet. Alice uses a secret key which she must share with Bob along with the encryption algorithm. Now she sends the encrypted text to Bob on internet and also shares the key with Bob through a secure channel. When Bob receives the text as well as the key, he can easily decrypt the text with the help of decryption algorithm. It is necessary to have a confidential channel to send the key to the designated receiver. That is why a secure channel has to be used, else, the security cannot be achieved.

Two main problems with symmetric key cryptography are; key management as the same key is used by sender and receiver. The example of symmetric key based cryptographic schemes are AES [4], RC4 [16], DES [17], RC4 [16] and 3DES [3].

2.1.6 Asymmetric Key Cryptography

Considering the drawbacks of symmetric key cryptography, the other method with two different keys was proposed to improve security level and overcome the issues of sharing a key. Diffie and M.Hellman proposed the approach of using two different keys and named as public key and private key. A public key cryptography is also known as Asymmetric Key Cryptography [18] that adopts comparatively new procedure as to symmetric encryption.

In asymmetric encryption two keys are used; key 1 is for encryption and key 2 is for decryption. There is no need to use a secure channel for sending the key to the designated receiver. Encryption key is kept public but the decryption key must be kept confidential. It is essential to know that anybody with the confidential key can decrypt the text, that is why two related keys are used for boosting the security. Public key is made freely known so that anyone who intends to send a text, can send it. But, the decryption key is kept confidential, only the owner knows the key and hence able to gain the original message.

Asymmetric key has a far better approach in ensuring the security of information transmitted during communication. The security of public key is not necessary that is why it is publicly accessible and can be passed over the internet. Anybody can use public key for transferring text to someone but to decrypt the text only private key can be used that is only known to the owner of it. In this way, public key cryptography addresses the issues of secret key cryptography.

The use of secure channel to share the decryption key was no more needed and that improved the security. The authorized person of the private key can now make sure that they have full authority to decipher the text. Some examples of Asymmetric key cryptography include ElGamal [19], RSA [20] etc.

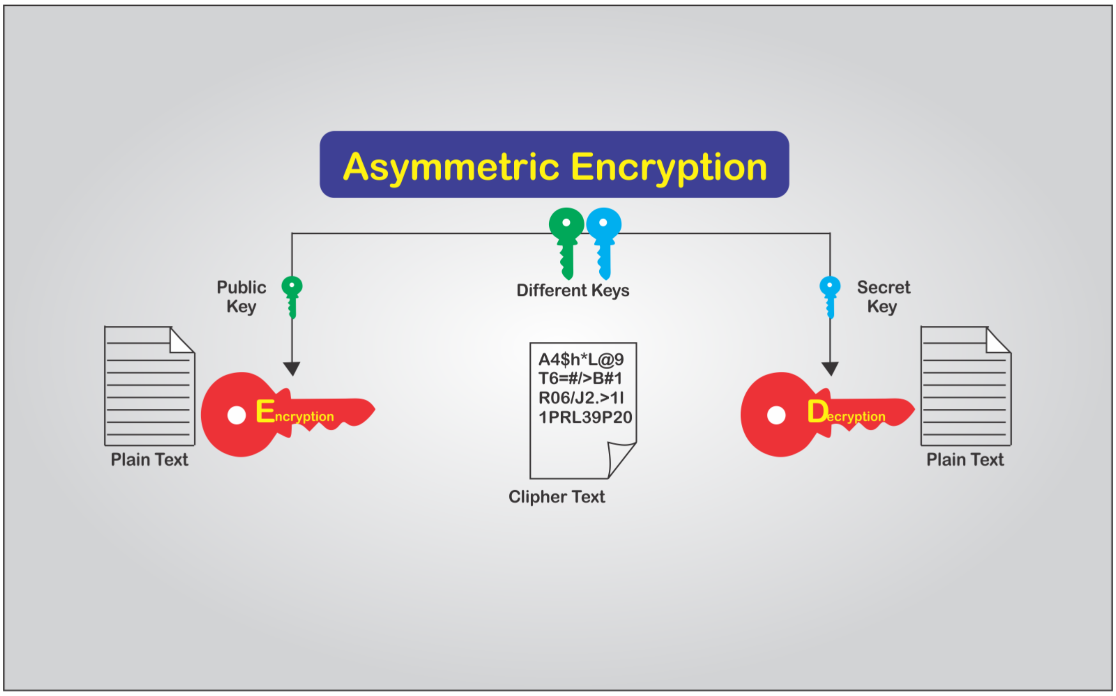


FIGURE 2.4: Asymmetric Key Cryptography Diagram

2.2 Cryptanalysis

Cryptanalysis [2] is the method used for analyzing the security of encrypted data, without knowing the confidential information that is needed to do so. Basically, it is a method of obtaining the plaintext from ciphertext without have the knowledge of key. The analyzed information is used to study the secret points of the system. Cryptanalyst is someone who tries to perform this task. Cryptanalyst attempts to decrypt ciphertext with the help of algorithm, without knowing the plaintext sources and encryption keys. It can also be said that a cryptanalyst works to improve the existing techniques by finding out the loopholes in a security protocol. This can be done by finding the key and improve the methods if it is weak in terms of the following four properties that are confidentiality, integrity, authentication and non-repudiation. If a system lacks any one of the four properties than the security of the communication is not be strong and the ciphertext can be decrypted easily.

Here, are some attacks that have been faced and discussed in the literature.

Ciphertext Only Attack

A kind of attack in which attacker uses known ciphertexts collection and tries to attack for the original text or the key. The main thing in regarding this attack is that the cryptanlyst does not know any thing about the original message so he uses ciphertext or an algorithm to get the plaintext. He can also use frequency of the letters to recover the plaintext.

Known Plaintext Attacks

In this kind of attack, a cryptanalyst knows the ciphertext with the corresponding known partial plaintext. Using this known information, he tries to make an effective algorithm to decrypt any ciphertext as well as the key of its corresponding plaintext.

Chosen Plaintext Attacks

In Chosen plaintext attack refers that the cryptanalyst uses ciphertext that matches arbitrarily with the selected plaintext the same algorithm. By using a proper algorithm, he can get the ciphertext for arbitrarily chosen plaintext. He tries to recover the key by using these plaintexts and ciphertexts.

Chosen Ciphertext Attacks

This is similar to chosen pliantext attacks. In this attack, the attacker uses ciphertext to gather information. He gets the plaintext of selected ciphertext and then he tries to figure out the secret key from these results and also tries to get the corresponding key.

Brute Force Attacks

In this kind of attack, the attacker does not know any information about the plaintext from ciphertext. He tries every possible guess to get the key from ciphertext. This attack can be made difficult, with bigger key space.

Man in Middle Attacks

It occurs when attackers find ways to communicate with the sender and receiver by interfering into the communication channel. This kind of attack is possible if the attacker chooses two fake secret keys and shares them with the sender and receiver. Both the original parties believe that they are communicating with each other but in actual all the confidential information is being shared with the attcker. Now, as the attacker delivered the keys of his own choice so it is not a big deal for him to decrypt the ciphertext as he knowns the private key. When he gets the reply in encrypted form from the first party, he can easily decrypt the message since the key is known to him. Then he decrypts the received message again using the second key and sends this message to the second party. Once he obtains a ciphertext from the second party he can again decrypt it using the key that he has. This is how the attacker plays a game and successfully manipulate the security protocols and at the end the attacker get control over the communication between two parties.

For further details in various cryptographic attacks, see [2].

2.3 Mathematical Background

Now, we discuss some basic concepts that are useful for understanding the mathematical operations used for the encryption and decryption purposes in a cryptographic technique.

Floor Function :

Floor function is also known as Greatest Integer Function (GIF) because it returns greatest integer which is less than or equal to the original number. In detail we can say that floor function rounds down the number to its closest integer. It is given as $f(u) = \lfloor u \rfloor$.

For any number $u \in \mathbb{R}$, the greatest integer less than u and the floor of u is symbolized by $\lfloor u \rfloor$.

i.e.$\forall\ u \in \mathbb{R}, n \in \mathbb{Z}$

$\lfloor u \rfloor = n \Leftrightarrow n \leq u < n + 1$

The graph of the floor function f shown in Figure 2.5

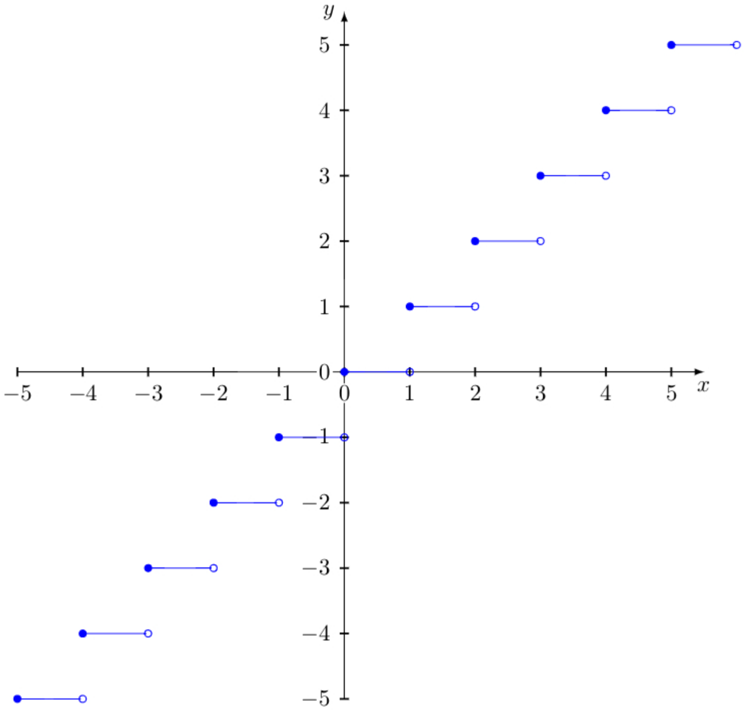


FIGURE 2.5: Floor Function

Ceiling Function:

Similarly we define the ceiling function as the Least Integer Function (LIF) which gives the least integer. This function is denoted by $\lceil x \rceil$

Ceiling function depends on the following rules :

1. If $v \in \mathbb{Z}$ is an integer then $\lceil v \rceil = v$
2. If $v \notin \mathbb{Z}$ is not an integer then ceiling(v) evaluates to least integer that is greater than v.

Mathematical representation of least integer function is $\lceil x \rceil$

let $v \in \mathbb{R}$ is the least integer greater than v

i.e.$\forall\ v \in \mathbb{R}, n \in \mathbb{Z}$,

$\lceil v \rceil = n \Leftrightarrow n - 1 \leq v < n$ Also,

$$f(v) = j \quad \text{if} \quad n - 1 \leq v < n, \quad j \in \mathbb{Z}$$

as the reduce of $f(v)$ is an $int(j)$.

The graph of the ceiling function is shown in figure 2.6

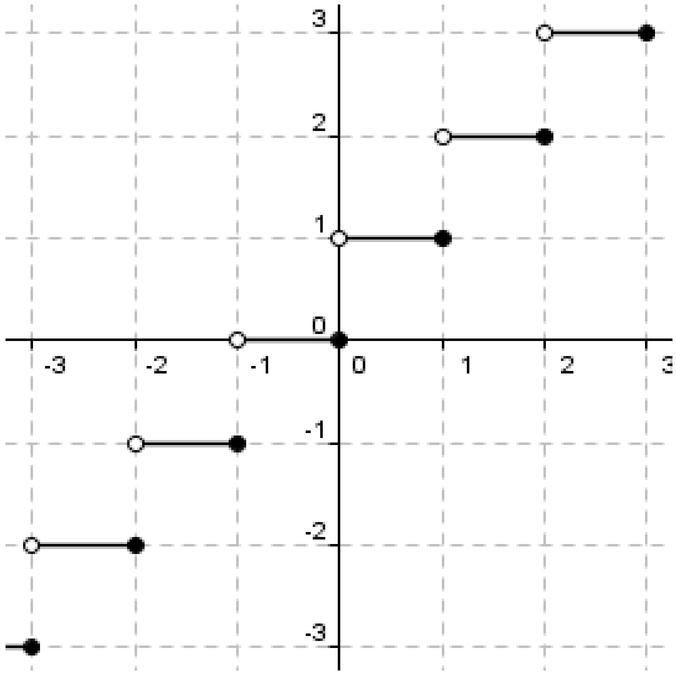


FIGURE 2.6: Ceiling Function

2.4 Confusion and Diffusion

In cryptography, confusion is defined as intense vagueness of ciphertext in a system. In other words, this technique makes sure the complexity and doubtfulness about plaintext. It gives no hint about plaintext. The relationship between association of ciphertext and value of encryption key is made as complex as possible. It basically each engages each bit of ciphertext with several parts of the key.

This property of confusion makes it hard for the attackers to guess the key from the ciphertext because with a change in a single bit of the key can affect the whole ciphertext. The confusion can be maintained by using complex algorithm that depends on key and plaintext. An original image with its pixel values arranged in rows and columns as shown in Table 2.1.

114	223	122	034	01	31	43	023
176	155	234	21	03	222	32	177
188	183	247	27	199	202	167	12
124	69	171	187	235	251	218	139
56	72	219	238	118	217	172	177
234	253	189	72	217	237	241	219
218	237	252	178	198	27	018	091
122	134	156	178	198	217	189	127

Table 2.1: Pixels Values of Original Image

The process of confusion used in Figure 2.2 can be understood in the following fashion:

1. Convert 2-D image of $M \times N$ in 1-D image by arranging N rows and M columns in a row with values $X = \{x_0, x_1, ..., x_{MN-1}\}$

2. Generate a random sequence $R = \{r_0, r_1, ..., r_{MN-1}\}$ using the following chaotic map:
$$x_{n+1} = \frac{x_n - \lfloor \frac{x_n}{q} \rfloor \times q}{q}$$
where q is the control parameter which is $0 < x \leq 0.5$. $\lfloor x \rfloor$ represent the maximal integer equal or less than x.

3. The generated random sequence is then sorted in an ascending order and named as $S = \{s_0, s_1, ..., s_{MN-1}\}$.

4. Now make a relationship between R and S by comparing the place of each value of S in R and write its place value in $T = \{t_0, t_1, ..., t_{MN-1}\}$.

5. Now, arrange X by following the place value in T and the modified version of X is named as Y.

6. Arrange Y in 2-D to obtain the permuted image.

155	171	34	122	134	178	217	176
217	69	251	237	234	177	218	241
252	237	217	127	219	56	198	253
222	32	235	72	167	1	122	247
183	18	114	172	189	23	199	31
43	188	234	27	178	21	118	18
156	238	198	177	124	218	12	27
202	139	219	3	72	91	187	223

Table 2.2: Pixels Values of Permuted Image

Diffusion is a technique that obscures the quality structure of plaintext for the prevention of any attempt by the attacker to deduce ciphertext or deducing the plaintext from ciphertext. Statistically, It is made possible when a change in a single bit of plaintext shows almost a change in half of the bits of ciphertext. We can also say that the arrangement of characters in plaintext is changed. Basically the main task of diffusion is to make the statistical association between the plaintext and ciphertext as complex as possible. It is achieved by spreading out each single plaintext digit over many cipher text digits in such a way that each bit is changed with any character or symbol which affects the whole ciphertext. Now, the diffusion is created in the pixels values of permuted image in the following fashion:

1. Generate a random sequence, say Z.

2. convert each value of the sequence into integer between 0 to 255.

3. Now use each pixel of permuted image Y with Z as follows:

$$R = (Y + Z) \mod 256$$

4. R is the diffused image and the each pixel's value is shown in Table 2.3.

1	225	50	70	67	16	134	4
116	72	109	23	13	5	184	81
154	164	181	105	215	50	125	173
198	32	250	197	220	87	163	246
112	49	139	110	96	65	101	232
254	17	197	17	118	56	191	201
101	252	0	161	13	225	180	211
75	19	63	198	161	94	171	144

Table 2.3: Pixels Values of Diffuse Image

2.5 Terminologies Related to Image Encryption

These are some basic terminologies which are frequently used in image encryption schemes.

Digital Image :

Digital image is the visual representation of an object that is encoded digitally. It is the numeric representation of two dimensional image, usually referred as raster image or bit mapped image. In a digital image, pixel are arranged in the form of 2-dimensional grid from or in a rectangular pattern that produces marix of M columns and N rows.

Pixel :

A digital image is a combination of many small elements. Each small element is termed as a pixel. Collectively they form a complete image. Individual or scattered pixels look like dots.

Image Resolution :

The total number of pixels used in an image is known as **Image Resolution**. Pixels of an image are arranged by the width and the height of the image. Suppose an image with resolution $M \times N$ shows that it contains M columns and N rows. So, if we have the order $M \times N$ then this shows total numbers of pixels contained in an image. For example, If an image has the number of columns 2048 and number of rows 800, then the total number of pixels present in it are $1,638,400$. Thus, the resolution of that image is 1.6 megapixels. Now, as an other example let we have image containing the number of columns 2048 of rows 1080 rows, then it has $2,21,840$ total number of pixels. Hence the resolution of this image is 2.2 megapixels. We can compare both these images with the help of thier resolutions. The image having resolution 2.2 megapixels will be better in quality than the image having resolution 1.6 megapixel. Therefore the image resolution of larges shows better quality.

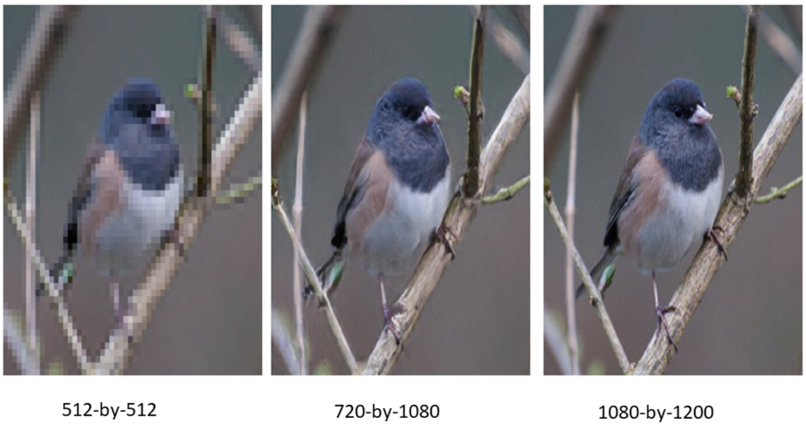


Figure 2.7: Image Resolution

In the example illustrated above as Figure 2.7, we can see three figures of resolution 512×512, 720×1080 and 1080×1080, it is clearly seen that 1080×1080

figure is visually better other figures.

Algorithm :

A step by step procedure or set of instructions given to the computer to solve a specific problem is called an algorithm.

2.6 Image Encryption and Decryption

The process of converting original image into coded image is known as image encryption. It makes image secure during its transmission over the public network. There is always a need to protect the information related to the secret image in order to maintain its security and no one other that the authentic receiver can identify them easily. An encrypted image is obtained by applying certain image encryption algorithm as shown in Figure 2.8.

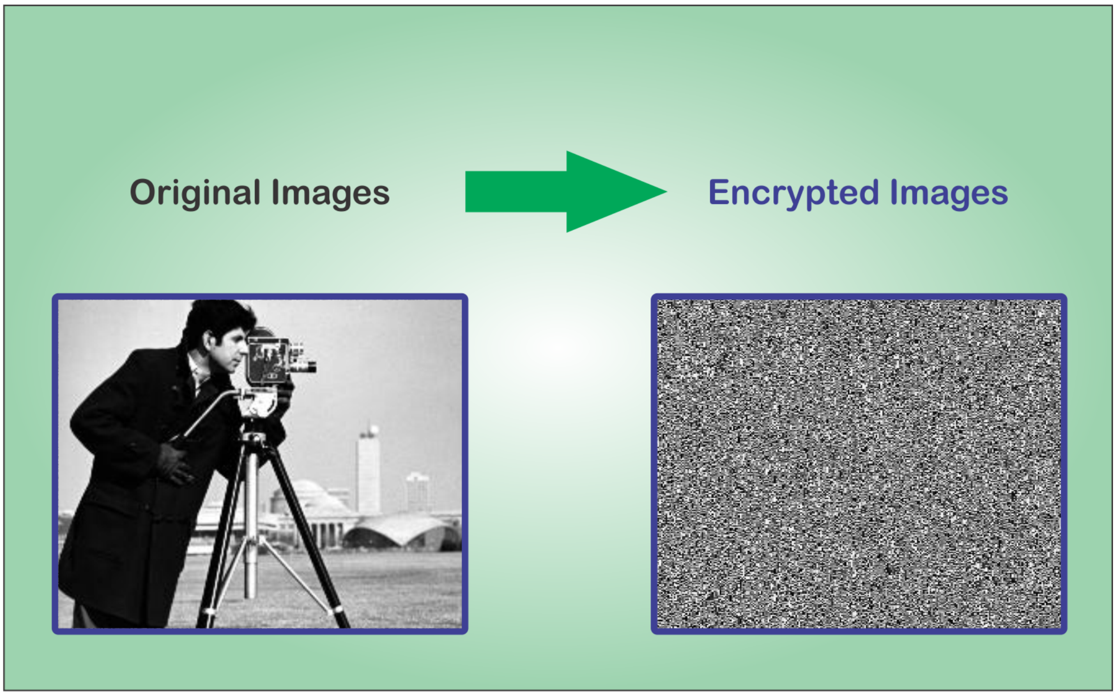


FIGURE 2.8: Image Encryption

Image encryption is basically method of converting an image into some other structures. While decryption recovers the original image only when the key is known. There are many encryption methods for encoding and decoding of the image. Chaos mapping [10] is considered the best technique to hold the multiple encryption strategies safely. There are many images that are highly confidential and their leakage can result a great loss. So, we want to secure them by altering in coded form so that their. The purpose of encryption is to only allow the authorized community to unveil the coded image.

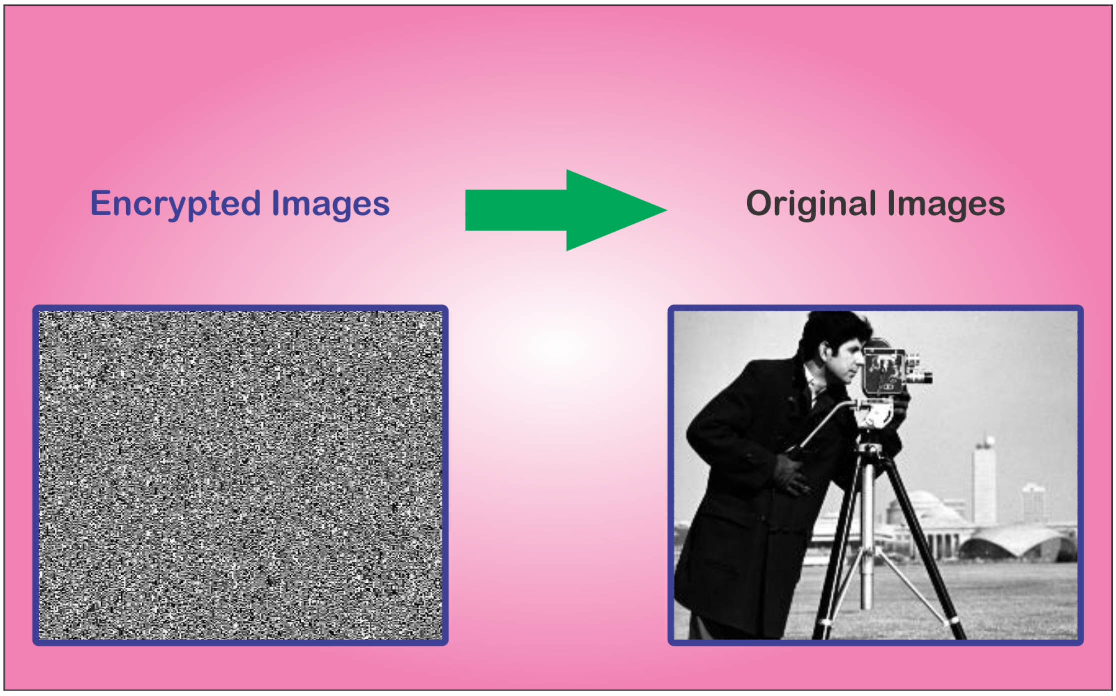


FIGURE 2.9: Image Decryption

The encrypted image is then forwarded to the authorized accepter. After that the decryption of that cipher image takes place. Decryption is the reversible procedure of encryption in which we convert encrypted image into its original form.

In this process, an authorized person can only get the original image by using the secret keys and decryption algorithm. Once the receiver gets the encrypted image, he decrypts the encrypted image to obtain the original image. Since, the key is only known to sender, so, the decryption can only be done by an authorized person who has the access of the secret key.

The receiver also applies the inverse procedure of diffusion and confusion and hence the image is decrypted. A decrypted image is obtained by applying certain image decryption algorithm as shown in Figure 2.10.

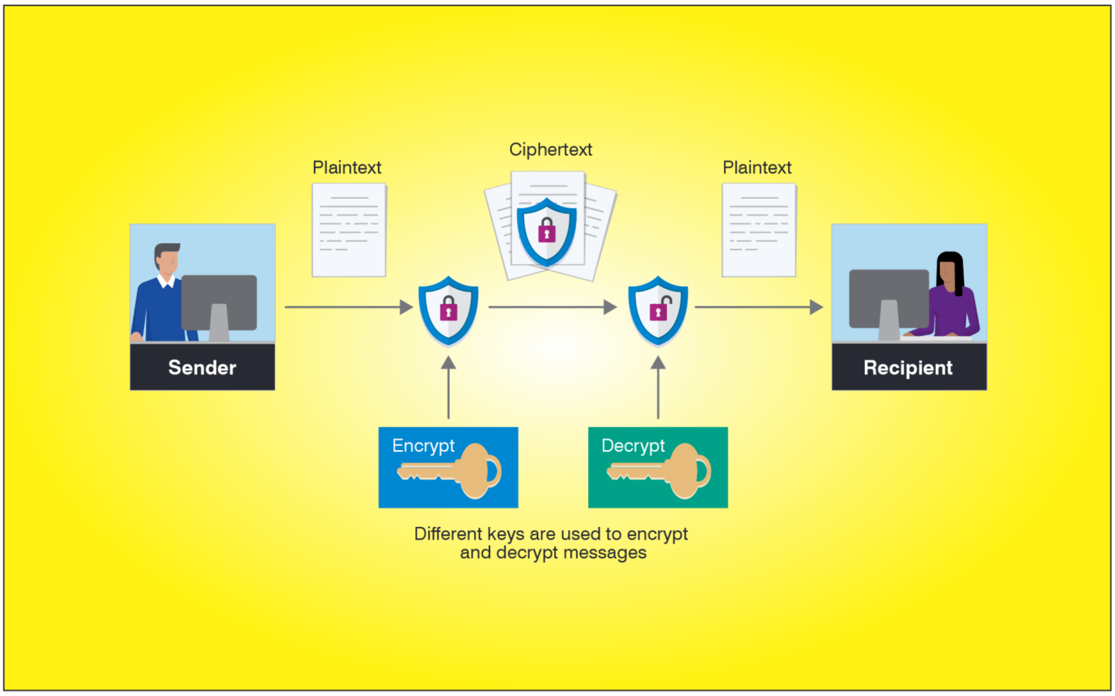


FIGURE 2.10: Image Encryption

Chapter 3

Image Encryption Based on Improved Piecewise Linear Chaotic Map

In this chapter, we will discuss some aspects of chaos theory, which is a building block of many secure image encryption schemes. In particular, we describe piecewise and improved piecewise linear chaotic map and their properties also a cryptographic schemes based on that improved piecewise linear chaotic map and its security. At the end of the chapter, a brief overview of meaningful image encryption is presented.

3.1 Chaos Theory

The word chaos refers to the science of surprises. By science of surprises, it means that the nonlinear and unpredictable behavior dynamic systems. The chaos theory prepares us to expect the unexpected. In the traditional science, the approach is used to deal with the predictable behaviors like gravity, electricity or chemical reaction. Whereas chaos theory gives an approach to deal with the unpredictable behavior such as turbulence weather, the stock market, our brain states etc.

Chaos theory often includes fractal mathematics. Fractal is a pattern which never ends and has a self-similar across different scales. The pattern exhibits complexity. Examples of fractal include trees, rivers, coastlines mountains, clouds, hurricanes etc. Many system around us are somehow a part of complex chaotic behavior. With the help of chaos theory we are be able to have a new insight, strength and ideas to understand the chaotic and fractal nature of our world. The example of balloon pilot best explains the whole scenario who reaches to his destination by keeping in mind the complex, chaotic change of atmosphere. Chaos theory provides us a platform to find a better approach towards things that have chaotic and fractal nature.

3.1.1 Butterfly Effect

The chaotic behavior can easily be understood by examine the phenomena of butter fly effect. The butterfly effect basically shows a great change that results due to a very small effect or change. So, a butterfly that flips wings in new Texas can be a reason for hurricanes in Brazil. So, a small change in the input can lead the major change in the output and that is what we learn from butterfly effect.
Chaos theory servers a great purpose in mathematics. Here, just to explain the concept in mathematics we will use linear equation to show the chaotic behavior. In order to give an example of chaos, let us give you an idea of approaching the sense of chaos in mathematical manner. Suppose we take an equation with some initial value and after some iterations it ends with a final number which is called the resulted value. By comparing the initial values and correspondence resulted values we will see if there is any chaos or not.

Example

Consider a linear equation.

$$u_{n+1} = u_n - 1 \qquad \text{with} \quad u_0 = 0.26734 \tag{3.1}$$

In the above equation, the variable involved is u. By performing iterations, we will obtain values for $u_1, u_2, u_3, ..., u_{10}$ as follows:

$$
\begin{aligned}
u_1 &= u_0 - 1 = 0.26734 - 1 = -0.73266\\
u_2 &= u_1 - 1 = -0.73266 - 1 = -1.73266\\
u_3 &= u_2 - 1 = -1.73266 - 1 = -2.73266\\
&.\\
&.\\
&.\\
u_{10} &= u_9 - 1 = -8.73266 - 1 = -9.73266
\end{aligned}
$$

Now, we check the behavior of it by considering $u_0 = 0.26733$.

$$
\begin{aligned}
u_1 &= u_0 - 1 = 0.26733 - 1 = -0.73267\\
u_2 &= u_1 - 1 = -0.73267 - 1 = -1.73267\\
u_3 &= u_2 - 1 = -1.73267 - 1 = -2.73267\\
&.\\
&.\\
&.\\
u_{10} &= u_9 - 1 = -8.73267 - 1 = -9.73267
\end{aligned}
$$

Observing the both resulted values, obtained from Eq (3.1), we conclude that after performing 10 iterations the both resulted values become same although the initial values supposed were different, so, it is a normal and predictable change in the final results and hence there is no chaos present in this example.

Now, we consider another equation and repeat the iterations with the same initial values.

$$u_{n+1} = 3u_n - 1 \tag{3.2}$$

Here are the results of a few iterations:

$$
\begin{aligned}
u_1 &= 3u_0 - 1 = 3(0.26734) - 1 = -0.19798\\
u_2 &= 3u_1 - 1 = 3(-0.19798) - 1 = -1.59394\\
u_3 &= 3u_2 - 1 = 3(-1.59394) - 1 = -5.78182\\
&.\\
&.\\
&.\\
u_{10} &= 3u_9 - 1 = 3(-4578.94678) - 1 = -13737.84034
\end{aligned}
$$

Now by performing the iterations for initial value $u_0 = 0.26733$

$$
\begin{aligned}
u_1 &= 3u_0 - 1 = 3(0.26733) - 1 = -0.19801\\
u_2 &= 3u_1 - 1 = 3(-0.19801) - 1 = -1.59403\\
u_3 &= 3u_2 - 1 = 3(-1.59403) - 1 = -5.78209\\
&.\\
&.\\
&.\\
u_{10} &= 3u_9 - 1 = 3(-4579.14361) - 1 = -13738.43083
\end{aligned}
$$

The resulting values for Eq. (3.2) show that the change in final results is 0.59049 although the change in the initial values was just 0.00001. This change in the final result is unexpected and it is unpredictable. Hence, there is a chaos present in this example.

3.1.2 Properties of Chaotic Systems

For many natural structures that cover a significant amount of technical and industrial areas, chaos has been witnessed. Such events indicate definite possessions which are difficult and unpredictable to mark. The mathematical theory of chaos has been discussed by many scholars due to its most important implication in various fields of science. These schemes adopt a definite range of enhancement procedures across a wide spectrum. The phenomena of chaos is typically found easily in almost all nonlinear deterministic systems. Apparently, chaos occurs when there exist is a continuous and disorganized progression in long-term mathematical benchmarks. There are certain set of properties which summarize the characteristics witnessed in chaotic systems. These met the mathematical concepts explaining chaos. The most suitable are [11]

Self-Similarity:

In an evolving system, in time or space, indicate the similar appearance at dissimilar scales of observation.

Aperiodicity:

The orbits system progresses system does not in an orbit replicate itself, or in other other words orbits are never periodic.

Long-term Prediction:

It is commonly difficult due to sensitivity to initial conditions, which can be recognized only to a limited amount of accuracy.

Sensitivity to Initial Conditions:

Slight variations in its early state can lead to completely dissimilar results.

3.2 Chaos and Cryptography

The phenomenon of chaos that exhibits pseudo-random behavior, is mostly seen in nonlinear definable structure and it is extremely sensitive to initial conditions of the system. System stability can be considered as an important parameter that can be observed by using Lyapunov exponent concept. An important feature of these systems is the comprehension of system output for an analyst who is aware of the initial conditions governing the characteristics. On the other hand, if the preliminary inputs to the system are uncertain, the system tends to be highly random. Unless the rightful owner of the data is aware of the pseudo-random behavior, this feature may be used to substitute and diffuse plaintext to achieve resistance and protection against unauthorized entities. Chaos based encryption schemes are capable of encrypting various types of data including text and other numerous formats that are used in communications systems.

3.2.1 Chaos Based Cryptosystems

It is impossible to escape from an unauthorized person who eaves drop in a communication network, like we use via satellite, mobile phone and internet. If we want to use any communication network and want to maintain the secrecy level then we have to apply some cryptographic technique. The security of contents like video and image has become increasing necessary in many applications such as used for the purpose of medical imaging, industrial imaging,video conferencing, military imaging systems, private multimedia messages.

Chaos theory, a field of mathematics, is developed in 1970 [21] has played a vital role to provide protection to confidential images and videos. Chaos theory is also playing its role in developing subjects like physics, economics, engineering and biology etc.

Chaotic system [8] is deterministic, non-linear system is highly sensitive to control parameters and initial conditions. It also has a pseudo-random behavior. in 1989 Mathews [22] presented a chaotic encryption algorithm. This can be used for the encryption of text based data. Fridrich introduced the important chaos based system [21] in his research. In his scheme, the confusion is gained by permuting all pixels as a whole using one of three types of $(2-D)$ chaotic maps, named as Standard map [23], Cat map [24] and baker map [25]. The diffusion system changes consecutive pixels values in such way that the change makes a collective effect to all the previous pixel values.

Mostly chaos-based encryption-decryption schemes depend on the substitution-permutation network (SPN) chaos theory due to its unpredictable behavior and cryptographic like properties is highly famous in the modern cryptographic research. Therefore nowadays many researches are using it for making secure cryptographic protocols. There are many chaos based cryptosystems like image secret sharing based on chaotic map [26], chaos based watermarking scheme [27]. The use of chaotic maps in these crpytographic algorithm enhanced their security level.

3.2.2 Confusion and Diffusion in Chaos

To make a better cryptographicly secure system it must gain confusion and diffusion effects as explained in Shannon papers [28]. The purpose of confusion property is to make the statistical relationship between the secret key and cipher-image complex. While the diffusion property makes the statistical relationship between cipher and plain image more complex. In other words, confusion principle states that there should not be any connection between the key and cipher. The diffusion principle states that change in any single bit of plain image effect many cipher bytes/bits. In most of the chaos based image cryptosystem confusion image can be accomplished using chaotic maps applying permutations and /or substitutions and the diffusion in the system can be accomplished sending single bit/byte effect to other bytes/bits.

3.2.3 Lyapunove Exponent

A Lyapunov exponent is the average divergence rate at very close points along the orbit as shown in the Figure 3.1 [29]. The Lyapunov exponent can therefore be used with chaotic action to measure the strength of the initial condition [30]. That means the Lyapunov exponent is used chaos to calculate the levels of separation of neighboring points along the real line. The Lyapunov exponent is used to for the better selection of the initial parameters of chaotic maps occurring in chaotic regions. For instance, f is a one-dimensional map and x_1, x_2 are two nearby points. Let $f'(x_1) = z$ with $z > 1$. the orbit x_2 will shift from orbit x_1 [29] almost at rate

z per iteration and this process goes on until x_2 orbit is moved at a significant distance from x_1 orbit. The Lyapunov exponent has three different dynamics cases as follows [29]:

1. When all exponents of Lyapunov are less than zero, then the orbit is directed to a fixed or stable point.
2. There is an ordinary attractor in case of Lyapunove exponent are zero. The ordinary attractor is simpler as comapred to a fixed point. This leads to a neutrally stable system in a steady state mode and the job of attractor is to keep constant separation.
3. If at least one exponent of Lyapunov is positive, the dynamic is chaotic, and vice versa

Lyapunov Number=

$$L(x_1) = \lim_{n\to\infty} (|f'(x_1)|...|f'(x_n)|)^{\frac{1}{n}} \tag{3.3}$$

where $(x_1, x_2, ..., x_n)$ is the orbit of the map f on the real line $\mathbb{R}$.
The existence of the limit in eq (3.3) of Lyapunov exponent further favors us to define the Lyapunov exponent in the following fashion:
Lyapunov exponent=

$$h(x_1) = \lim_{n\to\infty} (\frac{1}{n})[ln|f'(x_1)| + ... + ln|f'(x_n)|]$$

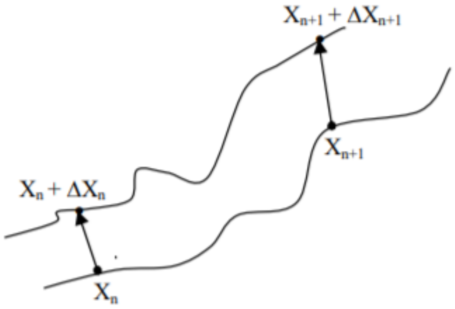


Figure 3.1: Principal of Lyapunov Exponent

3.2.4 Piecewise Linear Chaotic Map

It is a simple non-linear dynamical system with large positive exponent. Several properties of piecewise linear chaotic map(PWLCM) are discussed in [6]. PWLCM has properties like in variant distribution, auto-correlation function, ergodicity large positive exponent and mixing [31] properties that shows its highly dynamical behavior.

A sequence of real numbers between 0 and 1 called an orbit is generated by performing iterations of PWLCMs with initial value and control parameters. In order to get the chaotic behavior for large orbit, a large positive lyapunove exponent is used. correlation functions are used to test the correlation over time and space. The PWLCM is define as:

$$x_{n+1} = \begin{cases} \frac{x_n}{q} & \textbf{if} \quad 0 \leq x_n < q \\ \frac{(x_n - q)}{0.5 - q} & \textbf{if} \quad q \leq x_n < 0.5 \\ \frac{(1 - q - x_n)}{0.5 - q} & \textbf{if} \quad 0.5 < x_n < 1 - q \\ \frac{1 - x_n}{q} & \textbf{if} \quad 1 - q < x_n < 1 \end{cases}$$

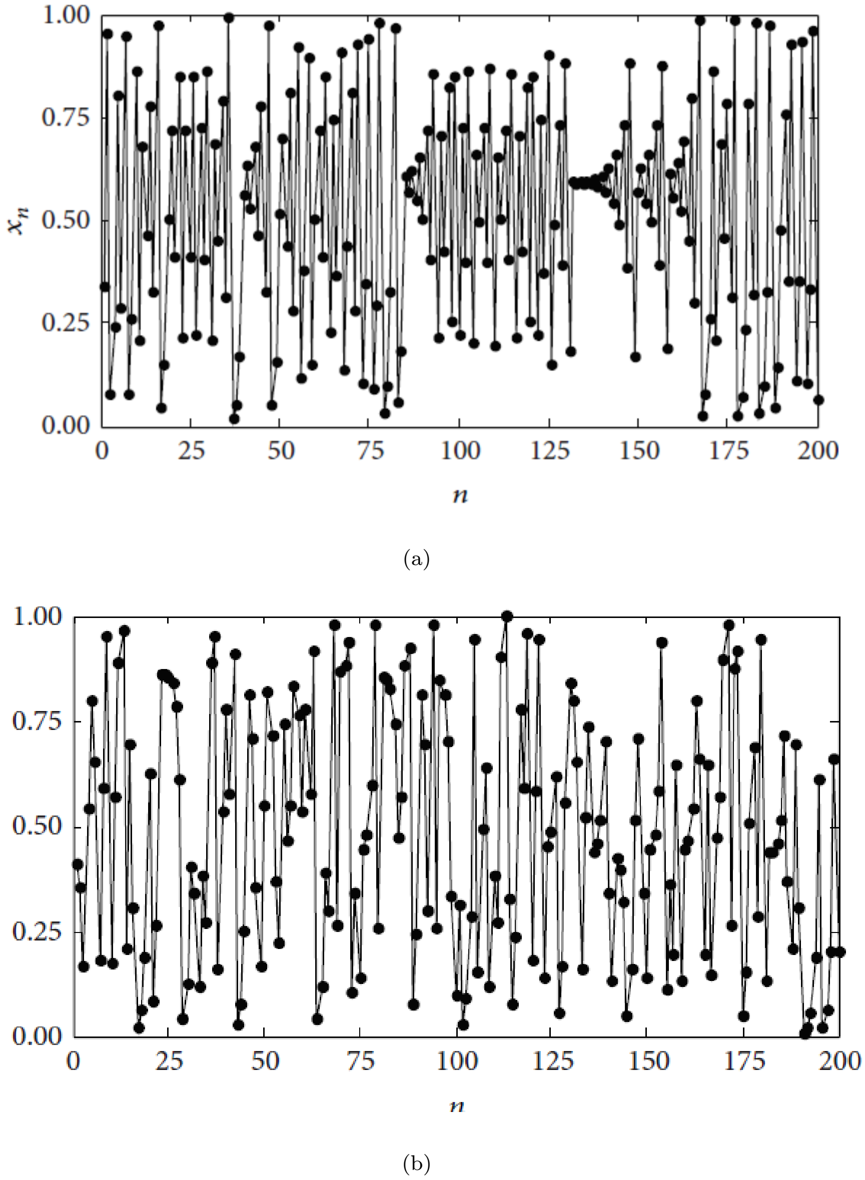
where the x_0 is the initial value, q is the control parameter which is $q \in (0, 0.5)$ and $x_n \in [0, 1)$.

3.2.5 Improved Piecewise Linear Chaotic Map

Using the idea of PWLCM, an improved piecewise linear chaotic map (MPWLCM) is proposed in [32]:

$$x_{n+1} = \frac{x_n - \lfloor \frac{x_n}{q} \rfloor \times q}{q} \tag{3.4}$$

q is used as control parameter and $q \in (0, 0.5)$. $\lfloor . \rfloor$ is a floor function that gives maximal integer equal or less than x. States of sequence for PWLCM and MPWLCM are shown in Figure (3.2) and Figure (3.2). Clearly, MPWLCM is better than PWLCM the randomness is concerned. Therefore, MPWLCM is a better option for use in cryptographic encryption scheme.



(a)

(b)

FIGURE 3.2: (a) PWLCMs (b) MPWLCMs

3.3 An Image Encrytpion Scheme Based on MPWLCM

In the scheme [32] proposed by Hu and Wang, a gray-scale image of size $L = M \times N$ is taken. After converting it in 1-D, first its pixel places will be changed and then pixel value are diffused. The working mechanism of proposed schemes [32] is as follow.

3.3.1 Generating Permutation

Given the initial condition x and control parameter q, we generate permutation sequence in order to change the pixel position of an image.

1. Convert 2-D image of $M \times N$ in 1-D image by arranging N rows and M columns in a row with values $X = \{x_0, x_1, ..., x_{MN-1}\}$
2. Generate a random sequence $R = \{r_0, r_1, ..., r_{MN-1}\}$ using the following chaotic map:
$$x_{n+1} = \frac{x_n - \lfloor \frac{x_n}{q} \rfloor \times q}{q}$$
where q is the control parameter which is $0 < q < 0.5$. $\lfloor x \rfloor$ represent the maximal integer equal or less than x.
3. The generated random sequence is then sorted in an ascending order as $S = \{s_0, s_1, ..., s_{MN-1}\}$.
4. Now we make a relationship between R and S by comparing the place of each value of S in R and write its place value in $T = \{t_0, t_1, ..., t_{MN-1}\}$.
5. Now, arrange X by following the place value in T and the modified version of X as Y.
6. Arrange Y in 2-D to obtain the permuted image.

3.3.2 Image Scrambling

In previous section, the place of pixels are changed and the obtained image is known as permuted image. Further in this section, the values of the pixels of permuted image will be changed. These are the steps that do so:

1. Generate diffusion sequence $K = k(1), k(2), ..., k(L)$ by using:
$$k(i) = \quad \text{mod}\ (\lfloor (x \times 10^2 - \lfloor x \times 10^2 \rfloor) \times 10^3 \rfloor, 256)$$

2. The permutation and diffusion will be repeated for R rounds. Ciphered images pixels are obtained through the following formulas:

$$c(j) = \mod(p(i) + c_1, 256) \oplus k(i) \quad \text{for} \quad r = 1$$

$$c(j) = \mod(c(i) + c_1, 256) \oplus k(i) \quad \text{for} \quad r > 1$$

   where,

   $p(i)$ is the ith pixel value of the plain image.

   $c(j)$ is the jth pixel value of current ciphered image.

   c_1 is the previously outputted ciphered pixel value, for $n = 1$ $c_1 = c_0$.
   $i, j = 1, 2, ..., L$.

After being done with both the procedures, the encrypted image looks texture-like image as shown in Figure 3.3.

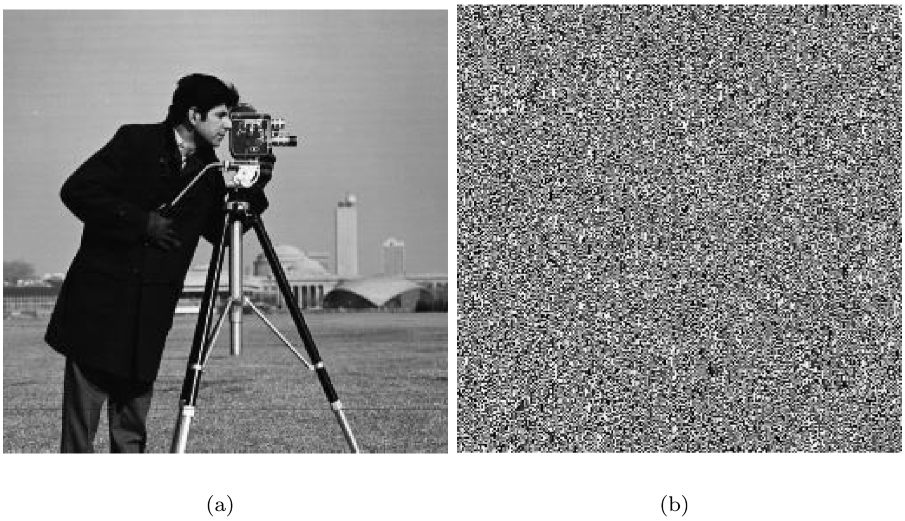

(a) (b)

FIGURE 3.3: (a) Original Image (b) Textur Like

3.4 Results and Discussion

A gray scale image of cameraman of size 256 × 256 is used as an example for the demonstrate of proposed encryption scheme with initial state $x_0 = 0.27$ and control parameter $q = 0.3$. Also, with $N_0 = 200$, $c_0 = 150$ and $R = 2$.

3.4.1 Key Space Analysis

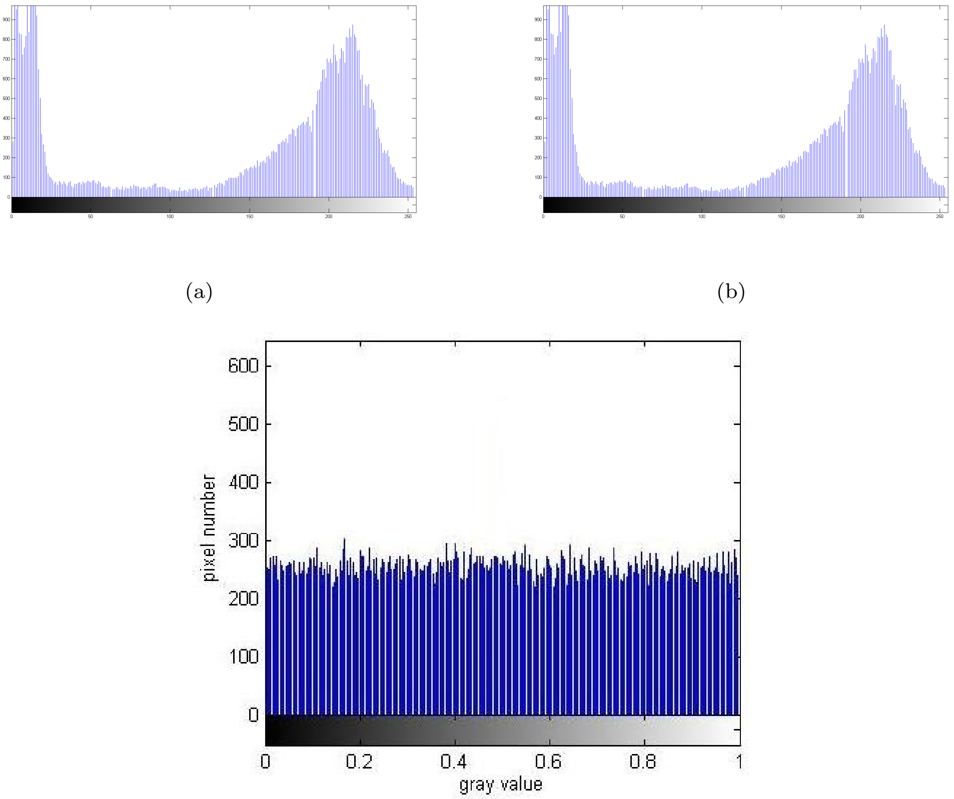
Key space size is the total possible keys that can be used during encryption. The hidden keys used in the proposed algorithm set $SK = (x_0, q, N, c_0)$. c_0 is a constant integer and $c_0 \in [1, 255]$ and N_0 is an integer. If the computational accuracy of x_0 and q is 10^{-16}, then $N_0 \in [1, 100]$. The key space is therefore greater than the $10^{16} \times 10^{16} \times 255 \times 1000$, which is much larger than 2^{124} as in [32]. Therefore the encryption algorithm has sufficient key space to resist all kinds of attacks by brute-force.

3.4.2 Statistical Analysis

For mathematical analysis, Shannon proposed two methods of diffusion and confusion. The confusion and diffusion properties of MPWLCM chaotic encryption method were demonstrated here.

3.4.2.1 Histograms of Encrypted Images

A gray scale image of size 256 × 256 chosen and than its histogram is measured. Figure (3.4) is shows one typical example (Cameraman). We can see from Figure (3.4) that the cipher image histogram is relatively uniform and completely different from that of the original image.



(a)

(b)

(c)

Figure 3.4: (a) Histogram of Plain Image (b) Histogram of Confused Image (c) Histogram of Cipher Image

3.4.2.2 Correlation Coefficients of Two Adjacent Pixels

Checking the similarity of two adjacent pixels in plain image and cipher image, all two-adjacent pairs of pixels (in vertical, horizontal and diagonal direction) of plain image and cipher image the correlation coefficients are calculated using the following formulae:

$$E(x) = \frac{1}{L} \times \sum_{i=1}^{L}(x_i) \tag{3.5}$$

$$D(x) = \frac{1}{L} \times \sum_{i=1}^{L}[x_i - E(x)]^2 \tag{3.6}$$

$$conv(x, y) = \frac{1}{L} \times \sum_{i=1}^{L}[x_i - E(x)][y_i - E(y)] \tag{3.7}$$

$$\gamma_{xy} = \frac{conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{3.8}$$

The gray scale values of two adjacent pixels are x and y, and their correlation coefficient is γ_{xy}. Table (3.1) displays the test results. This table also shows test result for a scheme [33] that is based on PWLCM. MPWLCM has superior performance as compared to [33], because it satisfies zero correlation that is required for strong security perspectives.

Correlation	**Horizontal**	**Vertical**	**Diagonal**
Cameraman	0.933475	0.959223	0.908663
Encrypted cameraman	-0.000090	-0.007362	-0.003039
Encrypted cameraman [33]	0.03217	0.027188	0.038391

Table 3.1: Correlation Coefficients

3.4.3 Information Entropy

The most important feature of the randomness is information entropy. Let s be the source of information, and the formula for calculating entropy of information is:

$$H(s) = -\sum_{i=0}^{2^n-1} P(s_i)\log_2[P(s_i)] \tag{3.9}$$

$P(s_i)$ is the probability of s_i and the total states of information are 2^n. The entropy for true random source emitting 2^n symbols is n. So, for a gray scala-image of size 256 with 2^8 possible values for pixels data, the ideal entropy must be equll to 8. The information entropy of cipher image is 7.9972 which is almost equal to the theoretical value 8.

3.5 Summary

A symmetric cryptographic method is proposed in [32] to encrypt gray scale image using the MPWLCM chaotic system. We can see that the proposed cryptosystem [32] is able to process any image. The security analysis and experimental results show that the proposed scheme has a great effectiveness. With large key space, it has the ability to tackle the brute-force attack. Statistical analysis shows the scheme can defend the image from statistical attack. The scheme is highly sensitive to plain image and key, so it has a strong ability to withstand differential attack. Since the scheme possesses high-level security [32] therefore it can be used in secure image communication. Once the cipher image is obtained, it can be covered by some visually meaningful image to change the appearance. That is before transmission of the cipher image a reference image is pasted in the encrypted image by using the method described in the next chapter.

Chapter 4

Generating Visually Meaningful Encrypted Images

In this chapter we have used DWT as discussed in [14]. The idea is to convert the encrypted images in some meaningful form that has an appearance similar to the normal image. the visual perception generated in this way, provide more protection. The DWT plays main role in generating visually meaning . therefore, we also are looking encrypted image into discrete wavelet transform function in this chapter and then its use for obtaining meaningful images.

4.1 Introduction

In the last 10 years it seen that many methods are used to store data, in the form of pictures, videos etc. These methods have made it possible for us to store bulge amount of data, and allow us to easily share it with others. Sometimes we have to share it with unknown people or untrusted party, then it becomes uncertain to belive that it is going in the right hands. For that we want to use a secure method. Image encryption is the method that enables us to share secret multimedia data easily and securely. There are different methods for image encryption that have been used since many years. Image encryption scheme usually changes places or

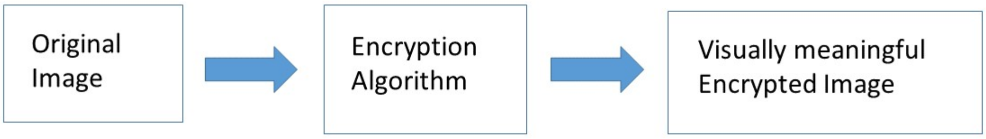
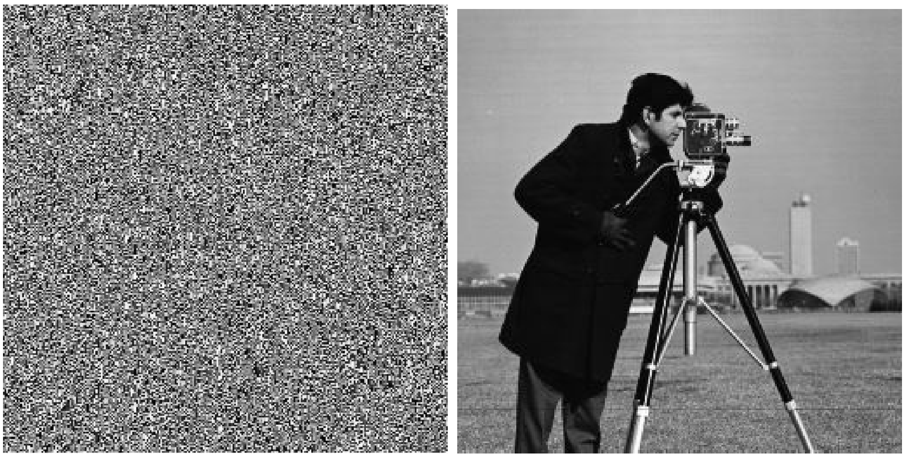


FIGURE 4.1: New Encryption Algorithm

values of pixels in the image as some of them are mentioned in [34, 35]. These techniques which are trying to ensure the security of the images are classified as frequency-domain and spatial domain image encryption techniques. In frequency domain, we transform the place of image's pixels using a transformation function such as [26, 36, 37]. On the other hand, in spatial domain, the values of pixel are modified using a substitution-permutation network like advanced encryption standard AES [38], gray code [39] and elliptic curve Elgamal [40]. Once the whole work is done, we get a ciphered image for the transmission over a public network.

4.2 Idea of Meaningful Image Encryption

The schemes that encrypt an image provide a great security during the transmission of the image. These schemes serve a great purpose for image data security. But, the image that is obtained by conventional image encryption schemes adopts a look that is different from normal images, usually it generates a texture or noise like shape [41]. Since, it is different from normal images so it gives a clear signal to attackers or cryptanalysis that it is an encrypted image. Now, due to its appearance, it still lacks the proper security. This issue was needed to address. L.Bao and Y.zho proposed a scheme named as visually meaningful image encryption scheme [14] that provides more security to the encrypted image by hiding it in a normal image. The idea of hiding the encrypted image in a normal image is obtained from the technologies like image hiding and reversible watermarking [42]. But the technology used in the proposed scheme is different because it only recovers the encrypted image while image hiding and watermarking recovers both images the cover image along with the image that is hidden. The other advantage that the proposed scheme has over watermarking is that it does not posses any restriction on final encrypted image to look similar to the reference image. A reference image is an image that is used to hide the encrypted image. So, the proposed scheme provides some extra protection to encrypted image and makes it appearance more secure.



(a) (b)

FIGURE 4.2: (a) Noise-like (b) Original Image

It is usually done by the use of wavelet transform. A wavelet transform particularly discrete wavelet transform is used to obtain meaningful encrypted images. The idea of wavelet transform is discussed in the next section.

4.3 Wavelet Transform

A mathematical transform is used to translate an image into different forms but usage of such transform depends upon their suitability for the subject it is to be used. Fourier transform is a well known and famous transform among others. Fourier transform helps us to change a signal into frequency-versus-amplitude from time-versus-amplitude. Generally, it can be said that Fourier transform represents the time-frequency of the signal. The term time-frequency representation of the signal suggests that two axis in the plain which are orthogonal to each other are used where one axis is for time and the other is for frequency. For a conventional Fourier transform it can be said that, it is a change in the representation of the signal corresponding to a rotation of the axis in the counter clockwise direction by an angle of $\frac{\pi}{2}$. The time axis can be inverted upon a signal's two successful rotations by $\frac{\pi}{2}$. Apart from these advantages, Fourier transform also lacks a few properties like for a specific time it fails to give any information for the the occurrence of frequency component and hence cannot be applicable for the the signals that are not stationary. Short-time Fourier transform then replace the Fourier transform which uses a moving window that moves over the whole real line. The Fourier transform is then applied to the signal that is in the window. Since short-time Fourier transform tackled the drawbacks of Fourier transform but still the problem appears when it fails to be applicable on real signals that have low frequencies of long duration and high frequencies of short duration. In order to overcome this issue, a transform that is effective at low frequencies and have high frequencies and low time resolution is used. Moreover, it should have high time resolution and low frequency at high frequencies. Wavelet transform has the capability to tackle with these type of situations and gives a better description of the image or signal. Wavelet is a mathematical function that is used in digital signal processing and image compression. The wavelet is a recent development of 1980s. It is capable of decomposing the signals into a set of functions over a spatial domain or modular spatial domain and then analyzing the function in both modular spatail domain and timing domain. This way it shows to have a better local capacity of time and frequency which lacks in Fourier transform. In signal processing, wavelet is used to make a signal strong and clean from noise. It recovers weak signals and in medical application, it proves its special feature in the processing of X-rays and magnetic- resonance images. Images are refined without blurring them. Wavelet compression of an image works by analyzing, reducing the size and converting the image into a set of mathematical function that can be decoded by the receiver. Wavelet compression has many types but most famous types avaiable in literature are:

1. Discrete Wavelet Transform (DWT)
2. Continuous Wavelet Transform (CWT)

The discretely sampled wavelet is known as DWT, whereas the wavelet that is continuously sampled is termed as CWT. In this work we will tend to focus on DWT only.

4.4 Discrete Wavelet Transform

DWT is a type of wavelet function that uses a wavelet function.

4.4.1 Two-Dimensional Wavelets

The two-dimensional wavelet transform is separable, which means we can apply a one-dimensional wavelet transform to an image. We apply one-dimensional DWT to all row and then one-dimensional DWT to all columns of the result. This is called the standard decomposition and it is illustrated in figure below.

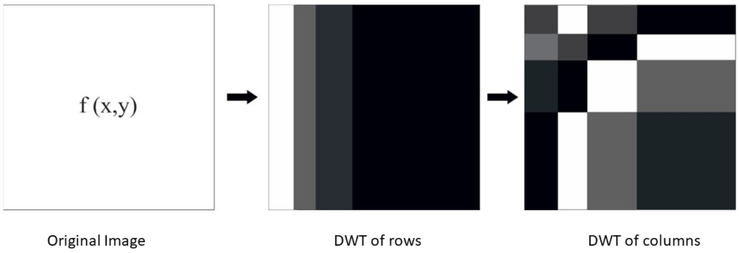


Figure 4.3: Two Dimensional DWT

Figure 4.3 the standard decomposition of the two-dimensional DWT. We can also apply a wavelet transform differently. Suppose we apply a wavelet transform to an image by rows, then by columns, but using our transform at one scale only. This technique will produce a result in four quarters: the top left will be a half-sized version of the image and the other quarters high-pass filtered images. These quarters will contain horizontal, vertical, and diagonal edges of the image. We then apply a one-scale DWT to the top-left quarter, creating smaller images, and so on. This is called the nonstandard decomposition, and is illustrated in the figure below.

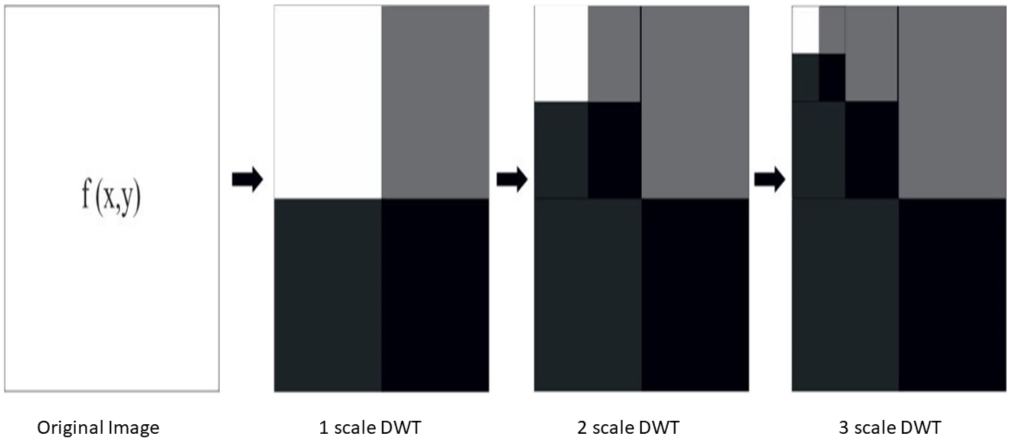


Figure 4.4: Two-Dimensional DWT

In the Figure 4.4 the nonstandard decomposition of the two-dimensional DWT. Steps for performing a one-scale wavelet transform are given below:

Step 1 : Convolve the image rows with the low-pass filter.

Step 2 : Convolve the columns of the result of Step 1 with the low-pass filter and resize it to half of its size by sub-sampling.

Step 3 : Convolve the result of step 1 with high-pass filter and again sub-sample to obtain an image of half the size.

Step 4 : Convolve the original image rows with the high-pass filter.

Step 5 : Convolve the columns of the step 4 with the low-pass filter and recycle this to the half of its size by sub-sampling.

Step 6 : Convolve the result of step 4 with the high-pass filter and again sub-sample to obtain an image of half the size.

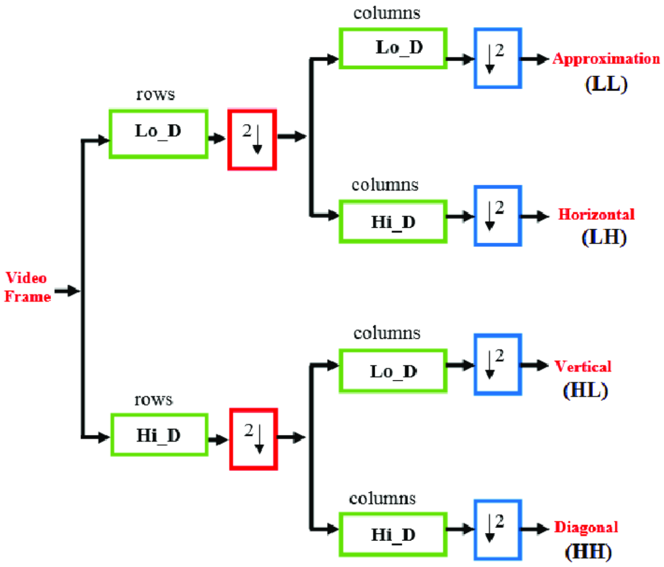


FIGURE 4.5: Two-Dimensional DWT

At the end of these steps there are four images and the size of each image is half of the original image.

1. The low-pass/low-pass image (LL), the result of step 2
2. The low-pass/high-pass image (LH), the result of step 3
3. The high-pass/low-pass image (HL), the result of step 5
4. The high-pass/high-pass image (HH), the result of step 6

These images can be placed into a single image grid as shown in the Figure (4.6) that is basically the one-scale wavelet transform in terms of filters.

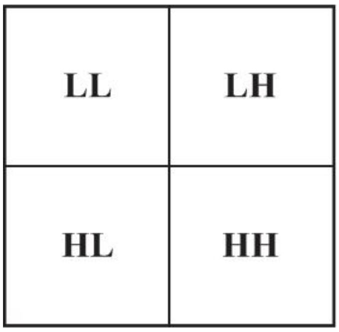


FIGURE 4.6: One Scale Wavelet

Figure (4.6) describes the basic DWT decomposition steps for an image in a block diagram form. The two-dimensional DWT leads to a decomposition of image into four components C_A, C_H, C_V and C_D, where C_A are approximation and C_H, C_V, C_D are details in three orientations (horizontal, vertical, and diagonal), these are same as LL, LH, HL, and HH. In these coefficients the watermark can be embedded.

In the paper [14], scheme proposed by L. Bao and Y. Zhou, converts the original image to visually meaningful encrypted image for its safekeeping. The image is emerged in an other image that looks like a normal image but here we hide the encrypted image in it. So that, an attacker cannot get any clue whether it is a normal or an encrypted image.

4.4.2 Visually Meaningful Image Encryption

Image encryption schemes exist that convert a plain image into like noise or texture. but these methods can be attacked because they are easily differentiable that is normal or Noise like cipher image. Therefore we use a method that convert a cipher image into normal image. Hence, it becomes difficult for attackers to differentiate secret image. In a consequence it is difficult to differentiate in between normal image and encrypted image and plain image. We overlay encryption algorithm on the normal image, so its security is enhanced. This process is different from others encryption algorithm.

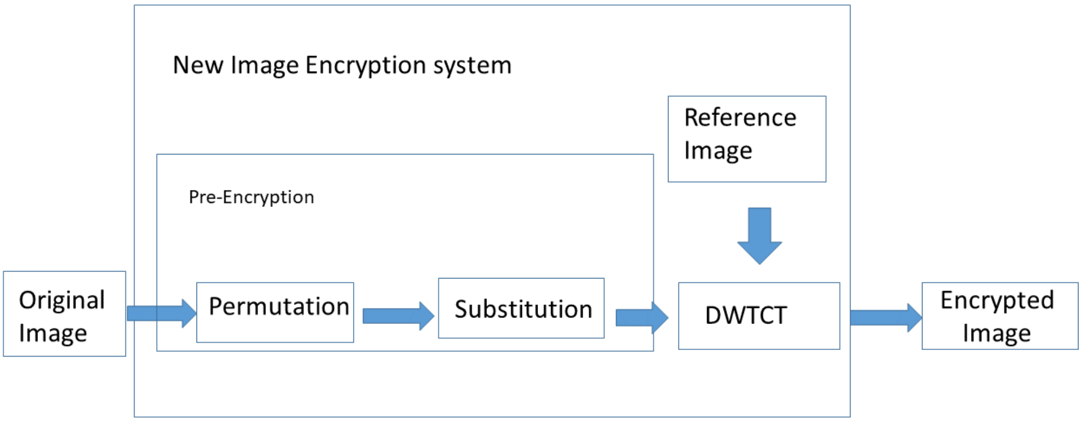


FIGURE 4.7: New Image Encryption system

4.4.3 Proposed System

In the proposed image encryption system, two images are taken, one is plain that is to be encrypted and the other is called reference image. With the help of reference image, we generate a visually meaningful encrypted image that completely resembles with the reference image but it is actually a result of visually meaningful encryption. This system consists of two parts. In the first part, the image is encrypted and gets a texture-like or noise-like structure by changing its pixels places or values. In the second phase, discrete wavelet transformation [43] is used for overlaying reference image. On the cipher image as a result a visually meaningful encrypted image is procured that exactly looks like reference image R.

The Pre-encryption is a procedure that helps us to change image's pixel and location using a transformation function that works on a substitution permutation network SPN. The pre-encrypted image P can be described as:

$$P = F(O, K_P)$$

Where O is normal image whose size is $M \times N$; F is a transformation function and K_p is the security key set. For pre-encrypted image already existed encryption algorithm overlaid. Pre-encrypted image takes a shape of noise or texture like image.
Discrete-wavelet-transform-based content transform (DWTCT) further converts the pre-encrypted image P into visually meaningful encrypted image VMEI which apparently looks exactly like reference image R. To accomplish this task, use the reference image R whose size is double than the normal image. It is also observed that different reference images produce different VMEIs. DWTCT is defined in the following way:

$$E = \mathbb{T}(P, R, K_t)$$

where

- P: Pre-encrypted image.
- R: Reference image.
- $\mathbb{T}$: Discrete wavelet transformation.
- K_t: Parameter of a wavelet filter.
- E: final encrypted iamge

As in the above the the size of the E and R have same.

DWTCT uses Calderbank's [15] proposed integer DWT in 1998 . DWT is invertible and change one integer to another integer. After the inverse DWT, the final encrypted image can be obtained, and hence vy applying decryption algorithm original image can be retrieved without any loss of data.

DWT convert image into four region therefore C_A, C_H, C_V and C_D describes the LL, HL, LH and HH of sub-band(L=Low-frequency, H=high-frequency), $\lfloor . \rfloor$ are the floor and modulo operator respectively.

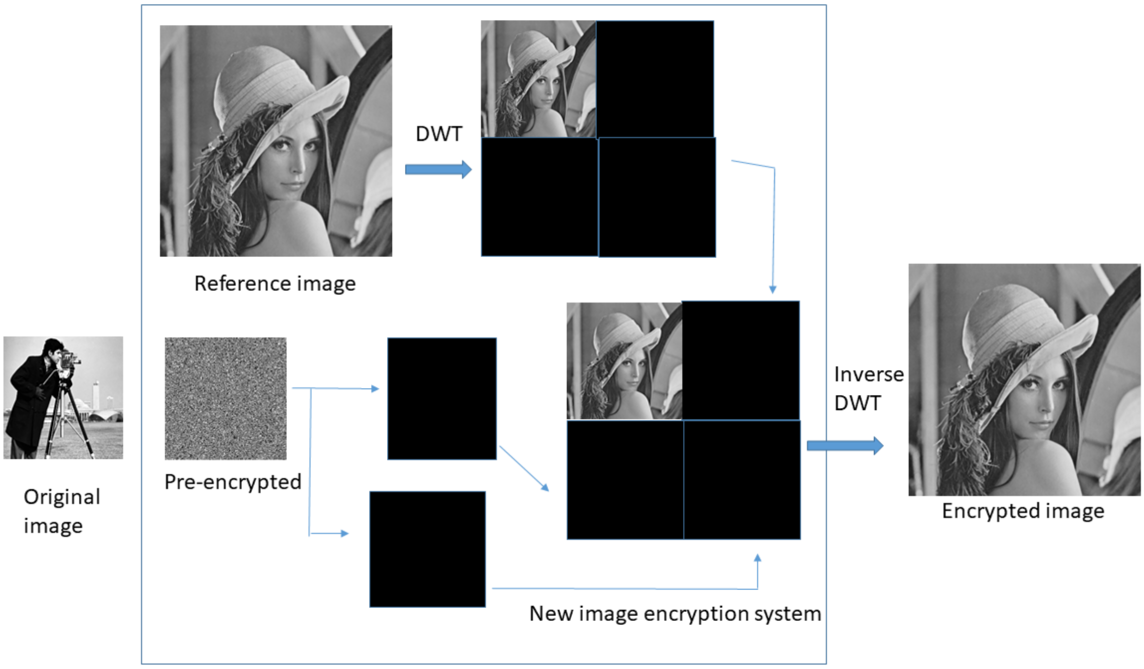


FIGURE 4.8: Encryption process

Algorithm:

Input: Plain Image P and reference image R.

Output: The final encrypted image E is obtained, and it is noted that size of the R and E are same.

1. load an image $P(m,n)$ withe the size of $M \times N$
2. Convert 2-D image of $M \times N$ in 1-D image by arranging N rows and M columns in a row with values $X = \{x_0, x_1, ..., x_{MN-1}\}$
3. Generate a random sequence $R = \{r_0, r_1, ..., r_{MN-1}\}$ using the following chaotic map:

$$x_{n+1} = \frac{x_n - \lfloor \frac{x_n}{q} \rfloor \times q}{q}$$

   where q is the control parameter which is $0 < q < 0.5$. $\lfloor x \rfloor$ represent the maximal integer or less than x.

4. The generated random sequence is then sorted in an ascending order and named as $S = \{s_0, s_1, ..., s_{MN-1}\}$.

5. Now make a relationship between R and S by comparing the place of each value of S in R and write its place value in $T = \{t_0, t_1, ..., t_{MN-1}\}$.

6. Now, arrange X by following the place value in T and the modified version of X as P'.

7. Arrange Y in 2-D to obtain the permuted image.

8. load an another image R which is reference image and the size of image is $2M \times 2N$.

9. Apply DWT defined by parameter K_t to the reference image R, obtain C_A, C_H, C_V and C_D.

10. **for** $m = 1$ to M **do**

11. **for** $n = 1$ to N **do**

12. $C_V(m,n) = \lfloor P'(m,n)/10 \rfloor$

13. $C_D(m,n) = P'(m,n) \mod 10$

14. Apply the inverse DWT to C_A, C_H, C_V and C_D sub-bands.

4.5 Decryption

In order to decrypt encrypted image E, the receiver needs to have a knowledge of pre-encryption together with the security key set K_p and also the parameter K_t of DWT. An authorized person can easily reconstruct the original image without knowing the reference image.

Decryption process firstly decompose the encrypted image into fours sub-bands using by the wavelet filter K_t of the DWT. The decryption process of the encrypted image describe below.

Algorithm

Input: Encrypted image E.

output: Plain image P.

1. Apply DWT on encrypted image E to obtain C'_A, C'_H, C'_V and C'_D sub-bands.
2. To obtain P'(pre-encrypted image) use C'_v and C'_D in the following equation:

$$P'(m,n) = 10C'_V(m,n) + C'_D(m,n)$$

   Here, C'_V and C'_D are the sub-bands equivalent to C_V and C_D. $P'(m,n)$ is the reconstructed pre-encrypted image.

3. Next, decrypt the pre-encrypted image P' using the decryption process of the scheme used in the pre-encryption stage.

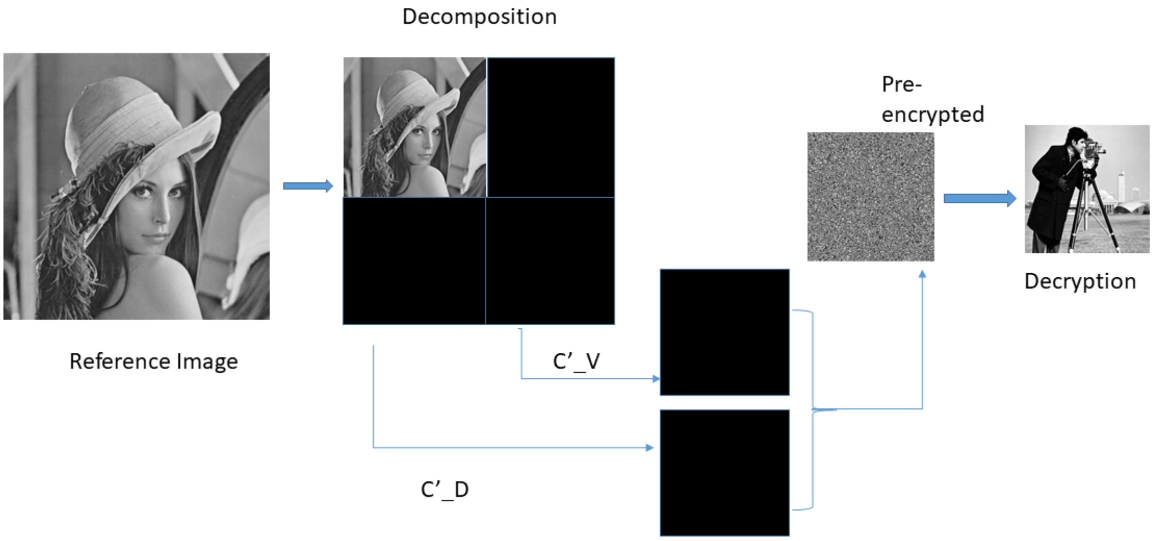


Figure 4.9: Decryption process

4.6 Discussion

The security of NIES is divided into two parts:

1. Image data security

2. Image appearance security

In image data security the pixel's places and values are changed using encryption algorithm. Hence we have a construction encrypted image that looks like noise or texture-like.

Image appearance security endorsed in such away that resulting image apparently looks like a plain image but acutely an encrypted image is hidden in it. It avoids from being attacked because an attacker cannot differentiate between a normal image and visually meaningful encrypted image. Therefore, VMIE is more reliable than other existing image encryption techniques.

NIES is inspired by the image hiding and other [44–46]. DWT is totally different from these existing schemes in the following aspects. The purpose of reversible watermarking and image hiding is to insert water marking or secret messages into a protected image with minimum distortion in the protected image [47–49]. In return, stego image (an image in which watermark or message is hidden) is truly similar to the cover image. It is difficult for unauthorized person to discover the existence of message by using various computer tools.

Whereas, DWTCT is also used for resolving the security lacks of noise-like encrypted image. It converts noise-like pre-encrypted image into visually meaningful encrypted image and provides additional security to pre-encrypted image. Furthermore reversible watermarking recreate both cover image and watermarks without any disturbance, while also pre-encrypted image is only recovered by DWTCT.

In NIES, we get visually meaningful encrypted image [26] that is not needed it to be similar to reference image. Therefore NIES shows naturalness of visual quality of final encrypted image, while reversible watermarking and image hiding raise high likeness between cover image and stego-image [50, 51]. This high naturalness quality makes sure that the resulting encrypted image can be considered as in ordinary image.

When it comes to the computational cost, DWTCT also has an upper hand compared to reversible water marking. The requirement of the DWTCT is time efficient and a has less computation cost for real time applications. In DWTCT, the size of real image is same as DWT sub-bands and reference image is 4 times larger than them. The size of the resulting visually meaningful encrypted image of suggested NIES has same as the reference image used. The size of original image is four time smaller than the resulting encrypted image of NIES. It is easy for a user to select a large size image as reference image. However, if the size of used reference image is large than it may result in high cost of storage and transmission.

Chapter 5

Security Analysis and Conclusion

This chapter summarizes the VMIE schemes presented in last chapter and highlights the important points that enhance the security the encrypted images. Also, the analysis of the VMIE is presented in which we will analysis the key space, key sensitivity, noise attack and data loss attack.

5.1 Security Analysis

The security of a cryptographic scheme based algorithm depends on the key designed and its role in encryption technique [1]. The proposed NIES has high key sensitivity and large key space.

5.1.1 Key Space Analysis

NIES's security key consists the pre-encryption algorithm [33] is security key set K_p, and DWTCT's K_t parameter. In the pre-encryption process an image encryption algorithm can be used to encrypt the image into pre-encrypted image. Since the integer DWT has at least 37 forms of existing wavelet filters, NIES has at least 37 times greater security key space than the pre-encryption algorithm. If we use Bao's algorithm [52] in the pre-encryption method, for example, K_p possible choices are 2^{240}. Therefore, NIES' key space is 37×2^{240}.

While the reference image is not required to reconstruct the original images in the decryption of images, it acts as visual protection measure for the original images. Different images of reference yield completely different visually meaningful encrypted images. Hence, NIES has a large security key space to withstand the brute force attacks.

5.1.2 Key Sensitivity Analysis

During the encryption process the high key sensitivity means that a small change in security key returns an unlike output in encryption and decryption. Here, the key sensitivity is executed by implementing a small replacement to the security key set (Key $= [K_p, K_t\ ]$) of NIES.

The simulation reults of visually meaningful image are depicted here in Figure 5.1. The pre-encryption phase uses Liao's algorithm [53] to encrypt the original image into encrypted form. Firstly we use $Key = [K_p, K_t]$ where

$$K_p = [605040302055865544852615981254537]$$

and $K_t = r9.7$ to encrypt the plain image and to get the resulting encrypted image. Another key set $Key_1 = [K_p, K_{t1}]$ without changing the K_p but $K_{t1} = sym8$ is then used to create visually meaningful image. As we observe from their histograms that here are two unlike encrypted images. This shows that the change of K_t will give two different encrypted images. Now, we use another $Key_2 = [K_{p1}, K_t]$ but same $K_t = r9.7$ but with different $K_{p1} = [605040302055865544852615981254536]$ to create an encrypted image. Now, equate with the encrypted image they are much identical in form of visual appearances and histograms. Reference image plays a significant part in the format or visual appearance of encrypted images. Visual quality of encrypted images can be effected by only changing the security key.

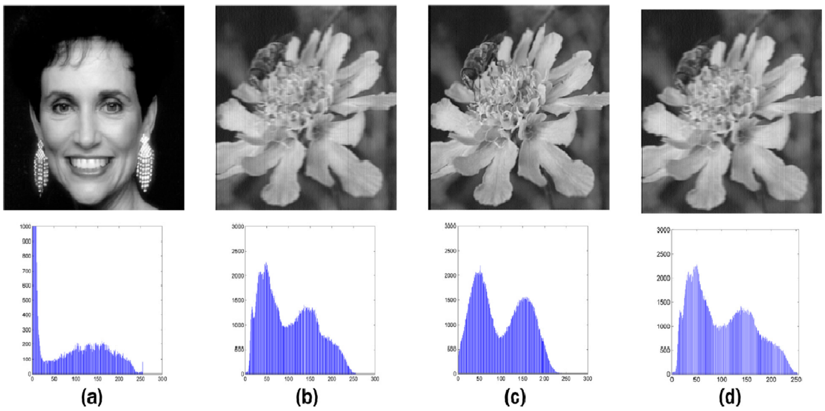


FIGURE 5.1: Key Sensitivity Encryption Test (a) Original Image (b) Encrypted Image with Key (c) Encrypted Image with K_1(d) Encrypted Image with K_2

However, in image decryption the security key plays an important role. In pre-encryption process, select $Key_3 = [K_{p3}, K_{t3}]$, where

$$K_{p3} = [77554332805586554485261598 1254537] \quad \text{and} \quad K_{t3} = db1$$

to encrypt the plain image. Then use Key_4, Key_5 and Key_3 in image decryption to obtain the decrypted image. Here, $Key_4 = [K_{p3}, K_{t4}]$ and $Key_5 = [Kp_5, K_{t3}]$ where $K_t4 = db3$ and $K_{p5} = [78554332805586554485261598 1254537]$. From the decrypted results, the original image can be recreated only when the exact key (Key_3) is being apply. Any change in the key will give in return unrecognized recreated image. NIES is highly sensitive to its security key changes in both image encryption and decryption.

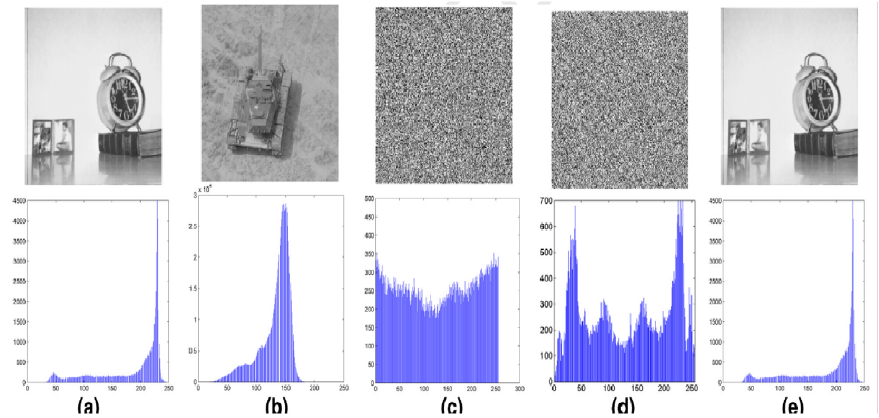
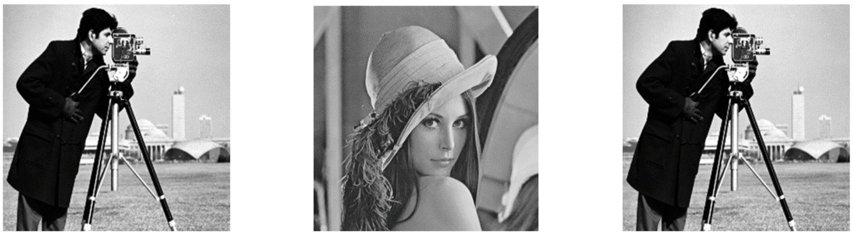


FIGURE 5.2: Key Sensitivity Decryption Test(a) Original Image and Histogram (b) Decryption with K_3 (c) Decryption with K_4 (d) Decryption with K_5 (e) Decryption with K_3

5.1.3 Data Loss and Noise Attack

During the transmission of sensitive a data loss can be expected. A successful system of encryption should resist attack on data loss. Figure 5.3 shows the effects of the data loss attack on simulations. Using the modified piecewise linear chaotic map algorithm [6] in the pre-encryption process. NIES encrypts the original image in the pre-encryption process and a statue image as a reference image to get the final encrypted image.



Original image Reference image Original image

Figure 5.3: Data Loss

There is a possibility that the images can potentially distorted during processing, amplification and detection may also occure by different types of noise. Obviously, for real applications an image encryption algorithm with the ability to resist noise attack would be appropriate.

In order to test the proposed NIES against noise attack,we apply salt and paper noise on the visually meaningful encrypted image. DWT will filter it and remove the reference image in decryption phase. The cipher image will not be distorted and show clear decryption results. Through these reconstructed images the original meaning of the image is clearly visible. Which show that the proposed NIES will withstand against the noise attacks.

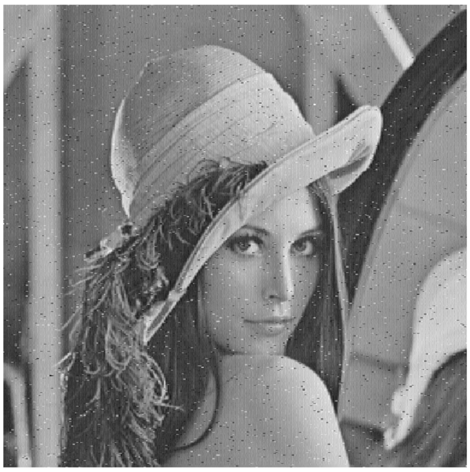


Figure 5.4: Gaussian Noise

5.2 Summary

There exist image encryption schemes whose noise like or texture like encrypted images may brings a lot of attacked. Now in this research we introduced a newly DWT based image encryption idea to accomplished visually meaningful encrypted image, That mainly considered as normal image rather then encrypted ones. The concept makes huge problem for the attacker to distinguish among correction and locating the encrypted images from all normal images. Therefore, the proposed idea is capable to save the originality of image with a high level security as compared to the other existing encryption algorithms.

It enhance the security of encrypted data and saves the real contents of image. More efficient DWT based content generates visually meaningful encrypted images with many different visual appearances. The proposed concept shows outstanding encryption and improve the security of existing image encryption algorithms with a low computation cost. The proposed concept have potential application and strength for privacy and copyright protection in network.

Bibliography

[1] A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone, and R. L. Rivest, "Handbook of applied cryptography," 1997.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2010.

[3] D. Coppersmith, "The data encryption standard (des) and its strength against attacks," *IBM J. Res. Dev.*, vol. 38, no. 3, pp. 243–250, May 1994. [Online]. Available: http://dx.doi.org/10.1147/rd.383.0243

[4] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*. Alpha Press, 2009.

[5] G. J. Simmons, "Symmetric and asymmetric encryption," *ACM Comput. Surv.*, vol. 11, no. 4, pp. 305 – 330, Dec. 1979. [Online]. Available: https://doi.org/10.1145/356789.356793

[6] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps." *I. J. Bifurcation and Chaos*, vol. 15, pp. 3119–3151, 10 2005.

[7] S. Som and A. Kotal, "Confusion and diffusion of grayscale images using multiple chaotic maps," in *2012 National Conference on Computing and Communication System*, 2012, pp. 1–5.

[8] W. Ditto and T. Munakata, "Principles and applications of chaotic systems," *Commun. ACM*, vol. 38, no. 11, pp. 96 – 102, Nov. 1995. [Online]. Available: https://doi.org/10.1145/219717.219797

[9] D. Jakobovic, S. Picek, M. S. R. Martins, and M. Wagner, "A characterisation of s-box fitness landscapes in cryptography," in *Proceedings of the Genetic and Evolutionary Computation Conference*, ser. GECCO '19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 153 – 157. [Online]. Available: https://doi.org/10.1145/3321707.3321850

[10] C. H. Skiadas and C. Skiadas, *Handbook of applications of chaos theory*. Independence, MO: CRC Press, 2016. [Online]. Available: https://cds.cern.ch/record/2197392

[11] Y. Zhou, L. Bao, and C. Chen, "A new 1d chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172– 182, 04 2014.

[12] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, no. 1, pp. 153 – 157, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0375960105011904

[13] M. A. Al-Khasawneh, S. M. Shamsuddin, S. Hasan, and A. A. Bakar, "An improved chaotic image encryption algorithm," in *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, pp. 1–8.

[14] L. Bao and Y. Zhou, "Image encryption: Generating visually meaningful encrypted images," *Information Sciences*, vol. 324, pp. 197–207, 12 2015.

[15] M. Lakshmi, J. Senthilkumar, and Y. Suresh, "Visually lossless compression for bayer color filter array using optimized vector quantization," *Appl. Soft Comput.*, vol. 46, no. C, pp. 1030 – 1042, Sep. 2016. [Online]. Available: https://doi.org/10.1016/j.asoc.2015.12.025

[16] A. Mousa and A. Hamad, "Evaluation of the rc4 algorithm for data encryption."

[17] R. Davis, "The data encryption standard in perspective," *IEEE Communications Society Magazine*, vol. 16, no. 6, pp. 5–9, November 1978.

[18] W. Diffie, "The first ten years of public-key cryptography," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 560–577, May 1988.

[19] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proceedings of CRYPTO 84 on Advances in Cryptology*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 10–18. [Online]. Available: http://dl.acm.org/citation.cfm?id=19478.19480

[20] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978. [Online]. Available: http://doi.acm.org/10.1145/359340.359342

[21] Z. Su, G. Zhang, and J. Jiang, *Multimedia Security: A Survey of Chaos-Based Encryption Technology*, 03 2012.

[22] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989. [Online]. Available: https://doi.org/10.1080/0161-118991863745

[23] A. Masmoudi, M. S. Bouhlel, and W. Puech, "Image encryption using chaotic standard map and engle continued fractions map," in *2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 2012, pp. 474–480.

[24] R. K. Sinha, N. San, B. Asha, S. Prasad, and S. S. Sahu, "Chaotic image encryption scheme based on modified arnold cat map and henon map," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, 2018, pp. 1–5.

[25] C. Fu, W. Li, Z. Meng, T. Wang, and P. Li, "A symmetric image encryption scheme using chaotic baker map and lorenz system," in *2013 Ninth International Conference on Computational Intelligence and Security*, 2013, pp. 724–728.

[26] L. Singh and K. Singh, "Visually meaningful multi-image encryption scheme," *Arabian Journal for Science and Engineering*, vol. 43, pp. 1513 – 1517, 02 2018.

[27] L. Chen, J. Chen, G. Zhao, and S. Wang, "Cryptanalysis and improvement of a chaos-based watermarking scheme," *IEEE Access*, vol. 7, pp. 97 549–97 565, 2019.

[28] Y.-q. Xu, M. Sun, and J.-h. Shen, "Shannon wavelet chaotic neural networks," 10 2006, pp. 244–251.

[29] C. S. Bertuglia and F. Vaio, "Nonlinearity, chaos, and complexity: The dynamics of natural and social systems," 2005.

[30] G. L. Baker and J. P. Gollub, *Chaotic Dynamics: An Introduction*, 2nd ed. Cambridge University Press, 1996.

[31] J. Peng, Shangzhu Jin, Yongguo Liu, Zhiming Yang, Mingying You, and Yangjun Pei, "A novel scheme for image encryption based on piecewise linear chaotic map," in *2008 IEEE Conference on Cybernetics and Intelligent Systems*, 2008, pp. 1012–1016.

[32] Y. Hu, C. Zhu, and Z. Wang, "An improved piecewise linear chaotic map based image encryption algorithm," *TheScientificWorldJournal*, vol. 2014, p. 275818, 01 2014.

[33] X. Wang and C. Jin, "Image encryption using game of life permutation and pwlcm chaotic system," *Optics Communications - OPT COMMUN*, vol. 285, pp. 123 – 137, 02 2012.

[34] G. Bhatnagar, Q. J. Wu, and B. Raman, "Discrete fractional wavelet transform and its application to multiple encryption," *Inf. Sci.*, vol. 223, pp. 297 – 316, Feb. 2013. [Online]. Available: https://doi.org/10.1016/j.ins.2012.09.053

[35] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, "Designing an efficient image encryption-then-compression system via prediction error clustering and

random permutation," *IEEE Transactions on Information Forensics and Security*, vol. 9, pp. 39–50, 2014.

[36] M. Shan, J. Chang, Z. Zhong, and B. Hao, "Double image encryption based on discrete multiple-parameter fractional Fourier transform and chaotic maps," *Optics Communications*, vol. 285, no. 21-22, pp. 4227–4234, Oct. 2012.

[37] C. Guo, S. Liu, and J. T. Sheridan, "Optical double image encryption employing a pseudo image technique in the Fourier domain," *Optics Communications*, vol. 321, pp. 61–72, Jun. 2014.

[38] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*. Alpha Press, 2009.

[39] L. Bao and Y. Zhou, "Image encryption," *Inf. Sci.*, vol. 324, no. C, pp. 153 – 167, Dec. 2015. [Online]. Available: https://doi.org/10.1016/j.ins.2015.06.049

[40] C.-K. Chen, C.-L. Lin, C.-T. Chiang, and S.-L. Lin, "Personalized information encryption using ecg signals with chaotic functions," *Inf. Sci.*, vol. 193, pp. 125 – 140, Jun. 2012. [Online]. Available: https://doi.org/10.1016/j.ins.2012.01.016

[41] Y. Zhou and S. S. Agaian, "Image encryption using the image steganography concept and plip model," *Proceedings 2011 International Conference on System Science and Engineering*, pp. 699–703, 2011.

[42] R. Naskar and R. S. Chakraborty, *Reversible Digital Watermarking: Theory and Practices*, 2014.

[43] P. Chaovalit, A. Gangopadhyay, G. Karabatis, and Z. Chen, "Discrete wavelet transform-based time series analysis and mining," *ACM Comput. Surv.*, vol. 43, no. 2, pp. 153 – 187, Feb. 2011. [Online]. Available: https://doi.org/10.1145/1883612.1883613

[44] L. An, X. Gao, Y. Yuan, and D. Tao, "Robust lossless data hiding using clustering and statistical quantity histogram," *Neurocomput.*,

vol. 77, no. 1, pp. 1 – 11, Feb. 2012. [Online]. Available: https://doi.org/10.1016/j.neucom.2011.06.012

[45] I. Dragoi and D. Coltuc, "On local prediction based reversible watermarking," *IEEE Transactions on Image Processing*, vol. 24, no. 4, pp. 1244–1246, 2015.

[46] X. Gao, C. Deng, X. Li, and D. Tao, "Geometric distortion insensitive image watermarking in affine covariant regions," *Trans. Sys. Man Cyber Part C*, vol. 40, no. 3, pp. 278 – 286, May 2010. [Online]. Available: https://doi.org/10.1109/TSMCC.2009.2037512

[47] J. Franco-Contreras, G. Coatrieux, F. Cuppens, N. Cuppens-Boulahia, and C. Roux, "Robust lossless watermarking of relational databases based on circular histogram modulation," *IEEE Transactions on Information Forensics and Security*, vol. 9, pp. 397–410, 2014.

[48] Y. Shi, X. Li, X. Zhang, H. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades," *IEEE Access*, vol. 4, pp. 3210–3237, 2016.

[49] L. An, X. Gao, X. Li, D. Tao, C. Deng, and J. Li, "Robust reversible watermarking via clustering and enhanced pixel-wise masking," *IEEE Transactions on Image Processing*, vol. 21, pp. 3598–3611, 2012.

[50] L. Bao and Y. Zhou, "Image encryption," *Inf. Sci.*, vol. 324, no. C, pp. 156 – 157, Dec. 2015. [Online]. Available: https://doi.org/10.1016/j.ins.2015.06.049

[51] X. Gao, L. An, X. Li, and D. Tao, "Reversibility improved lossless data hiding," *Signal Process.*, vol. 89, no. 10, pp. 2053 – 2065, Oct. 2009. [Online]. Available: https://doi.org/10.1016/j.sigpro.2009.04.015

[52] Y. Zhou, L. Bao, and C. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Process.*, vol. 93, no. 11, pp. 3039 – 3052, Nov. 2013. [Online]. Available: https://doi.org/10.1016/j.sigpro.2013.04.021

[53] X. Liao, S. Lai, and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," *Signal Processing*, vol. 90, pp. 2714–2722, 09 2010.