IMAGE STEGANOGRAPHY USING IMPROVED LSB AND EXOR ENCRYPTION ALGORITHM

Dissertation submitted in partial fulfillment of the requirements for the award of degree of

Master of Technology
in
Computer Science and Applications

Submitted By
Sandeep Kumar
(Roll No. 601203024)

Under the supervision of
Ms.Vineeta Bassi
Assistant Professor
(SMCA)

SCHOOL OF MATHEMATICS AND COMPUTER APPLICATIONS
THAPAR UNIVERSITY
PATIALA – 147004
JULY 2014

CERTIFICATE

I hereby certify that the work which is being presented in the dissertation entitled, "**Image Steganography Using Improved LSB and EXOR Encryption Algorithm**", in partial fulfillment of the requirements for the award of degree of *Master of Technology in Computer Science and Applications* submitted in School of Mathematics and Computer Applications, Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of **Ms. Vineeta Bassi** and refers other researcher's work which are duly listed in the reference section.

The matter presented in this dissertation has not been submitted for award of any other degree of this or any other University.

(Sandeep Kumar)
601203024

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Ms. Vineeta Bassi)
Assistant Professor
SMCA

Countersigned by

(Dr. Rajesh Kumar)
Head
School of Mathematics and Computer Applications
Thapar University, Patiala

(Dr. S.K Mohapatra)
Dean (Academic Affairs)
Thapar University, Patiala

Abstract

Steganography is a technique to secure the information by just pushing information into information or information behind information. Many formats or types of steganography are being used in modern such as text, image, audio/video and protocol but digital images are the most widely used because of their frequency on the internet such as hiding/pushing secret information binary code in images binary code due to which image may slightly be changed. There are many steganography algorithms in which each has its own strength and weakness in terms of security and complexity. Some of which provides invisibility of information while some provides a large secret message to be hidden. This dissertation provides an overview of steganography specially image steganography and its uses. It attempts to design and develop the good steganography algorithm and briefly describes about the Least Significant Bit image steganography algorithm and also provides a improved version of LSB. It also uses an improved version of XOR encryption algorithm named Extended XOR with Improved LSB image steganography algorithm and analyzes the combined effects of these two algorithms.

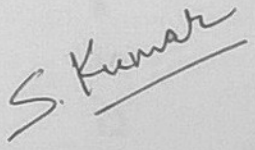
Acknowledgement

First of all I would like to thank the Almighty, who has always guided me to work on the right path of the life. This work would not have been possible without the encouragement and able guidance of my supervisor **Ms. Vineeta Bassi**. I thank my supervisor for her time, patience, discussions and valuable comments. Their enthusiasm and optimism made this experience both rewarding and enjoyable. I am equally grateful to **Dr. Rajesh Kumar**, Associate Professor and Head, School of Mathematics and Computer Applications, for motivation and inspiration that triggered me for the dissertation work.

I will be failing in my duty if I don't express my gratitude to **Dr. S. K. Mohapatra**, Senior Professor and Dean of Academic Affairs, Thapar University, for making provisions of infrastructure such as library facilities, computer labs equipped with net facilities, immensely useful for the learners to equip themselves with the latest in the field.

I am also thankful to the entire faculty and staff members of School of Mathematics and Computer Applications for their direct-indirect help, cooperation, love and affection, which made my stay at Thapar University memorable.

Last but not least, I would like to thank my parents for their wonderful love and encouragement, without their blessings none of this would have been possible. I would also like to thank my close friends for their constant support.



Sandeep Kumar

(601203024)

List of Contents Page No.

List of Figures Page No.

List of Tables Page No.

List of Abbreviations

COS	Closure of Sets
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
GEFR	Gradient Energy Flipping Rate
LSB	Least Significant Bit
MSB	Most Significant Bit
OPAP	Optimal Pixel Adjustment Process
PSNR	Peak Signal to Noise Ratio
RRS	Resist Random Scattered
RS	Random Scattered

CHAPTER 1
INTRODUCTION

1.1 Motivation

The motivation behind developing image steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage. The main goal of using the steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message.

One of the most common reasons that intruders can be able to gain unauthorized access of information and they can use this information for their own purpose, to harm someone, modify and attack . As the technologies are continuously growing due to possibilities of information to be hacked or unauthorized are also growing and in modern era communication need special kind of protection from intruders. It's not only limited up to information or communication, it also applies on computer network because internet is only the medium to exchange the message. So, providing more security to computer network is more important because most of the information is transferred over the internet. The main reason to provide is to maintain the confidentiality, integrity, availability and also to stop the unauthorized use of information. This can only be stopped either hiding existence of the information or keeping the information secret. Most common ways to stop this are steganography and cryptography. Both are complementary to each other and provide better security, confidentiality and authenticity. Image steganography is becoming an important area in the field of steganography. As the demand of security and privacy increases, need of hiding their secret information is going on. If a user wants to send their secret information to other persons with security and privacy he can send it by using image steganography.

1.2 Steganography

Steganography is a technique of hiding information within the information or hiding one form of information into another form of information [1]. Steganography word is the combination of two Greek word “stegos” and “grafia”. Stego means “cover” and grafia means “writing” whereas Steganalysis is a technique to detect the existence of steganography. Steganography is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data [2]. In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which supposed to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques.

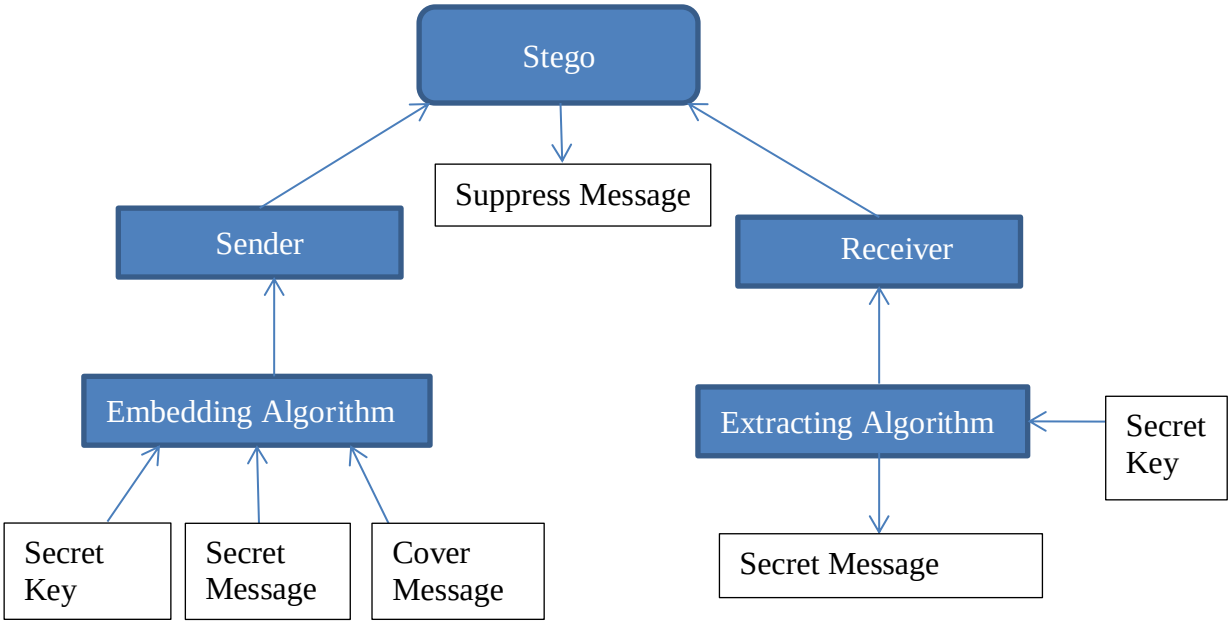


Figure 1.1 Steganography System Scenario [2]

The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the

same password used by the sender . The Steganography system scenario is shown above in the Figure 1.1.

"Steganography is the ancient art of embedding a secret message into a seemingly harmless message. This art, in contrast to cryptography, does not use ciphers or codes to scramble a message, and therefore is not obvious. U.S. and foreign officials suspect that Osama bin Laden is using steganography to pass embedded maps and photographs of terrorist targets through chat rooms and pornographic Web sites"[3].

1.2.1 History of Steganography

Steganography is being used over a long time to exchange, communicate in a secure manner. Some examples are:

i. In ancient time, this technique is first time used in Greece from 5^{th} century. Greece people used to hide information on the head of their slave. First, slave was selected and saved his head then a message was written on his head. They waited until the hair grew black and message was hidden. That slave was send to another place where his head was shaved again to get secret message [3].

ii. In the same time of Greece, Steganography technique is used by Spartans. This method uses another form called employed and Demerstus. Spartans was using this technique against their enemy Xerxes. Secret message was written on a wood wax tablet and covered be a new plane layer of wax due to this wax looked like blank [4].

iii. In 1600s, steganography technique is used by Sir Francis Bacaon in a face variant encoding.

iv. When World War 2 was going on, steganography technique is used to hide the existence of the information. Information was written on paper using invisible ink and due to this paper looked like blank to a normal person in normal light. Finally, information was read out using liquids such as water, fruit juices and vinegar. First, the wet paper in liquid was heated due to which they became dark and information written using invisible ink made visible to eyes [5].

v. During the World War 2, a new steganography technique was discovered by Germans and it is call microdots in which a secret message was hidden in a innocent message in such a manner so that the letter at every particular position in the message represented as the letter of secret message [6].

vi. In 1945, Morse code was concealed in a drawing, see Figure 1.2. The hidden information is encoded onto the stretch of grass alongside the river. The long grass denoted a line and the short grass denoted a point. The decoded message read: "Compliments of CPSA MA to our chief Col Harold R. Shaw on his visit to San Antonio May 11th 1945" [7].

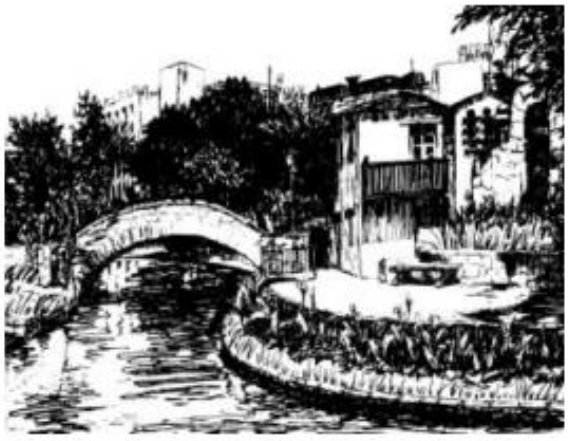


Figure 1.2 Concealment of Morse code, 1945 [7]

1.2.2 The Digital Era of Steganography

With the boost in computer power, the internet and with the development of digital signal processing, information theory and coding theory, steganography has gone "digital". In the realm of this digital world steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed. Cyber-crime is believed to benefit from this digital revolution. Hence an immediate concern was shown on the possible use of steganography by criminals, following a report in USA TODAY. Cyber-planning or the "digital menace" as Lieutenant Colonel Timothy L. Thomas defined it as being difficult to control. Provos and Honeyman scrutinized three million images from popular websites looking for any trace of steganography [2]. They have not found a single hidden message. Despite the fact that they attributed several reasons to this failure it should be noted that steganography does not exist merely in still images. Embedding hidden messages in video and audio files is also possible.

1.2.3 Types of Steganography

Based upon the condition, there are many technique of steganography in which image steganography is most popular technique. Almost all digital file formats can be used

for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. It can be divided mainly into four categories:

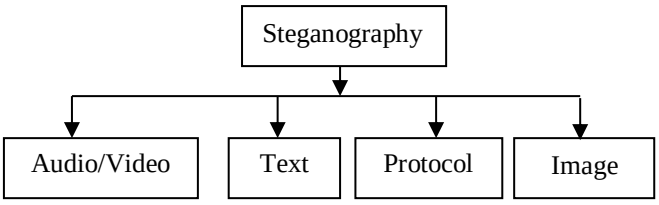


Figure 1.3 Categories of steganography

1. Audio/Video steganography
2. Text steganography
3. Protocol steganography
4. Image steganography

1.2.3.1 Audio/Video Steganography

In Audio/Video steganography, a secret message is hidden in audio/video file. The binary sequence of audio/video file is slightly differ from original file which cannot be easily be detected by human eyes [8]. Least Significant Bit is most commonly used in this category. Some types of Audio/Video steganography are:

i. Phase coding
ii. Spread Spectrum
iii. Echo hiding

1.2.3.2 Text Steganography

Hiding information in text is historically the most important method of steganography. In this type of steganography, secret message is hidden in a text. There many techniques are used such sequencing in which each character of secret message is hidden a fix position of text or the binary value of secret message is hidden in binary value of text [8]. Microdots and use of extra white space are the example of text steganography.

1.2.3.3 Protocol Steganography

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

This type of technique is used in network level to hide the secret message because there a field in IP header in TCP/IP suite or internet for data hiding due to which datagram becomes undetectable. Flag, identification fields are used for Protocol Steganography [9].

1.2.3.4 Image Steganography

Image steganography is a technique which is used to hide secret message within an image. The binary bits of secret of message are hidden in the binary of image and this slightly affects the intensities of colour or brightness which is not detectable by naked human eyes [8]. There are many algorithms which are used for image steganography but some of them are very complex while some of them are simple.

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist.

A simple image steganographic model contains an original image, called cover (I) image in which secret component secret message/image (M) is hidden and a stego key (K) which is used to hide the information as well as to extract. The purpose of using stego key is to provide security. Finally, after the steganographic process, an

image is obtained called stego-image (S) in which pixel value is different from the pixel value of original image but these changes is so minor that it cannot be easily detect by human eyes.

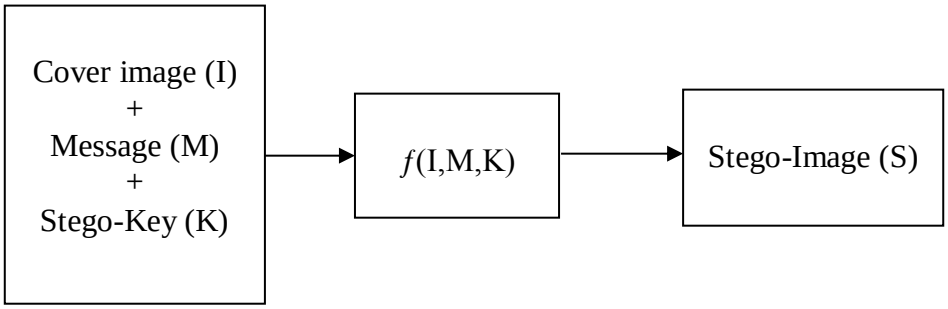


Figure 1.4 Simple Steganographic Model

In the above model, function f indicates any image steganographic algorithm. LSB image steganography algorithm is used which is used to replace the Least Significant Bits (LSB) of the image in which secret message is to be hidden called cover image with the Most Significant Bits (MSB) of secret message to be hidden without changing the statistical property of the cover image significantly.

1.3 Steganalysis

Steganalysis works as an attack on steganography. Basically, it is a process of detecting of the existence of secret message into text/image [10]. It compares the message and tries to find the secret hidden message. As we know when any message is hidden in an image, the intensity may be slightly decreased and color may be slightly faded. So, this helps in detecting the existing the hidden message. As we know steganalysis helps in attacking on steganography. Some important types of attacks are:

i. Known carrier attack
ii. Steganography only attack
iii. Known message attack
iv. Known steganography attack

Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message by using certain cryptographic algorithms for converting the

secret data into unintelligible form [10]. On the other hand, Steganography hides the message so that it cannot be seen.

In the other words, we can say that steganography is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party.

1.4 Cryptography

Cryptography is the combination of two Greek words Crypto which means "Secret" and Graphy which means "writing". So, Cryptography is a way to changing the message/information from one form to another secret form which is differ from the original with the help of a secret key and this process is called Encryption [11]. However, we use the term Cryptography to refer to the science and art of transforming messages to make them secure and immune to attacks. The changed value of secret message is called cipher and to get original message from cipher is called Decryption.

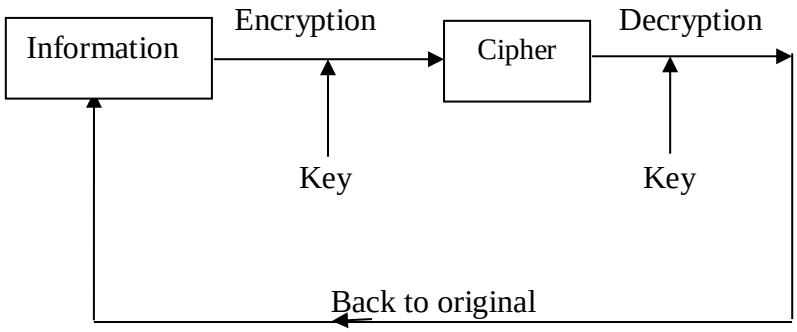


Figure 1.5 Encryption / Decryption process

1.4.1 History of Cryptography

i. About 4000 years ago, cryptography was used by Egyptians on the tomb of their master Nobleman Khunmhotep to write his life story on his tomb. They used symbol instead of words/characters and technique was called substitution method [11].

ii. In 500 BC, a machine named Scytale was developed by Spartans. This machine uses a cylinder to hide the secret message. The message was written in the encrypted form on a tape in such a manner so that if this tape is

wounded on the cylinder, the secret message can get easily [12]. This method is called transposition method.

iii. About 2000 years ago, cryptography was used by Roman army. Julius Ceasar was the commander of Roman army and he wanted to find a way of secure communication. A substitution method is also developed by Ceasar in which a letter is replaced by another symbol. In this method, letter was shifted by fixed position or changed by other symbol and Ceasar took a lot of advantage of this method during the war [13].

iv. In 1500's, Bliase De Vigenere developed a new cryptosystem which was based on Alberti's cipher disk. In Vigenere method, a square was used in which there are 26 alphabets of English language was on both axis, X and Y axis. If someone wanted to encrypt the message then one's had to find the corresponding letter when finding plaintext on row and key alphabets on column [13].

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

Figure 1.6 Vigenere Cipher Method [13]

According to key, cryptographic algorithms can be divided into two types:

i. **Secret Key Cryptography:** The key used for encryption and decryption process are same. It is also termed as symmetric key cryptography such as AES and DES [14].

ii. **Public Key Cryptography:** Two different keys are used, one for encryption and another for decryption. It is also known as asymmetric key cryptography such as RSA [14].

There are many cryptography algorithms have been already developed such as XOR, RSA, AES, DES, TDES and BLOWFISH etc. every one of these has its own advantages and disadvantages.

1.4.2 Cipher

The intermediate results after encrypting plaintext is called cipher text. It is totally differs from plaintext. It may be in readable form or not. According to the cipher cryptographic algorithms can be divided into two parts:

i. **Stream Cipher –** In stream cipher, encryption and decryption are done typically on one symbol (such as a character or a bit) at a time. In stream cipher, each binary digit is processed individually one bit at a time with the help of key such as XOR encryption algorithm. It takes less time and space then block cipher but it is not easy to implement correctly [15, 16].

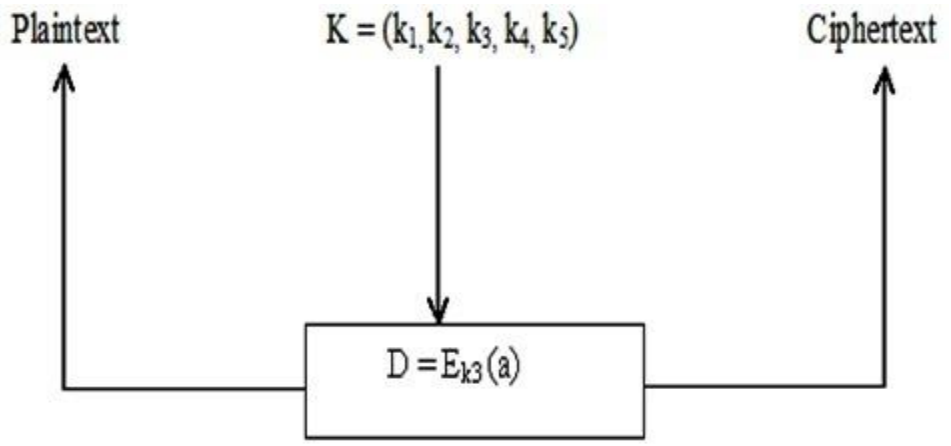


Figure 1.7 Stream Cipher

ii. **Block Cipher -** In block cipher, a chunk or block of data is processed at a time unlike stream cipher such as Blowfish and DES. It takes more time and space then stream cipher but as we are not working on individual bit so it is easier to implement than stream cipher [15, 16]. In block cipher, a group of plaintext symbols of size m (m>1) are encrypted together creating a group of cipher text of same size. Based on the definition, in a block cipher, a single key is used to encrypt the whole block even if the key is made of multiple values.

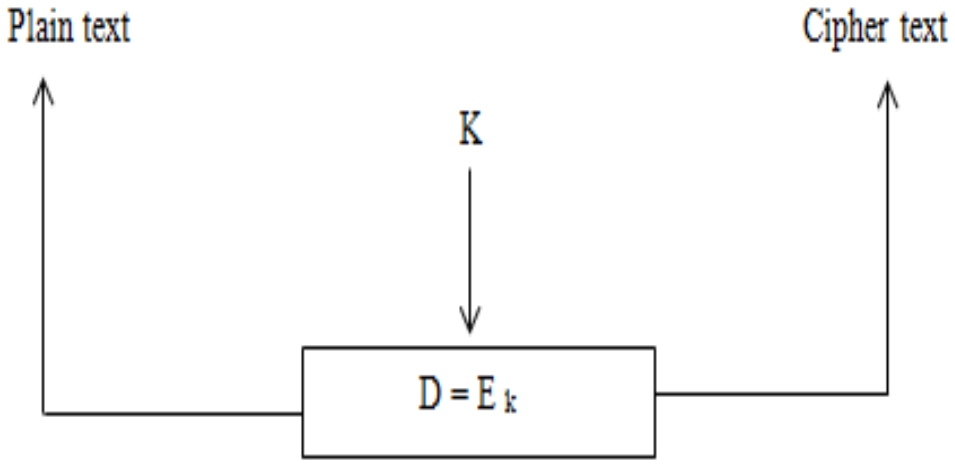


Figure 1.8 Block Cipher

- **Types of Cipher**

In past, simple pen and paper cipher method was used which was also known as classical cipher. But some important types of cipher are:

i. **Substitution Cipher –** A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another. For example, we can replace letter B with letter E, and letter S with Y [16]. Each unit or group of units is replaced by some other predefined symbol or character such as Caesar cipher and one time pad cipher.

ii. **Transposition Cipher –** Transposition Cipher does not substitute one symbol for another, instead it changes the location of the symbols. A symbol in the second position of the plaintext may appear in the eighth position of cipher text. A symbol in the seventh position of the plaintext may appear at the first

position of cipher text. It is simply permutation of plaintext such as Rail fence cipher[17].

iii. **Polyalphabetic Substitution Cipher –** In this, each occurrence of a character may have a different substitute. The relationship between a character in a plaintext to a character in the cipher text is one-to-many, for example "a" could be enciphered as "E" in beginning of the text, but as "M" in the middle. Substitution methods are used such Vigenere method and Enigma machine [18].

1.5 Cryptanalysis

It is the technique to find the true meaning of encrypted plaintext**.** It tries to detect the way of working of system such as used encryption algorithms and secret key. It can simply be called an attack on cryptography [18]. It can also be termed as code breaking or cracking of code. It can be of following types:

i. Cipher text only
ii. Known plain text
iii. Chosen plain text attack (Batch and Adaptive)
iv. Chosen cipher text (Adaptive and Indifferent)

i. **Cipher text only:** In this type of attack, attacker has access to only some cipher text. He tries to find the corresponding key and the plain text.

ii. **Known plain text:** In this type of attack, attacker has access to only some plain text/cipher text pairs in addition to the intercepted cipher text that he wants to break.

iii. **Chosen plain text:** Chosen plain text is similar to the known-plain text attack but the plain text/ cipher text pairs have been chosen by the attacker himself.

iv. **Chosen cipher text:** Chosen cipher text is similar to the chosen plain text attack, except that attacker choose some cipher text and decrypts it to form a Cipher text/ plain text pair [19].

1.6 Research Objective

The main purpose of this dissertation is to design and develop an efficient image steganography algorithm which is made more secure with the help of newly

developed cryptographic algorithm named Extended XOR. EXOR is an enhanced version of existing XOR encryption algorithm. Here, we will enhance and improved existing LSB image steganography algorithm and try to make a more secure combined approach of these two cryptography algorithm named EXOR and image steganography algorithm named Improved LSB. Results of these algorithms will be compared with existing algorithms and analysis the combined approach of cryptography and steganography.

1.7 Dissertation Outline

Based on the research contribution, the dissertation is segmented in following chapters.

Chapter 1 is Introduction.

Chapter 2 examines various research papers that are related to steganography and cryptography algorithms. It discusses previous works that form the roots of subsequent research in both areas.

Chapter 3 indicates the problem definition and justification to the problem statement.

Chapter 4 explains the proposed Work.

Chapter 5 explains the Results.

Chapter 6 contains the last section, in which we conclude this dissertation and point out some future work

CHAPTER 2

LITERATURE SURVEY

Steganography technique is most commonly used in hiding the existence of information whereas cryptography is a technique which is used to keep the content of information secret. Both are complement to each other. Same as steganography and cryptography, steganalysis and cryptanalysis are complementary to each other and considered as an attack on steganography and cryptography. Steganography can be used as both legal and illegal. Good citizen uses it for secure communication while hacker and terrorists use it in illegal way to gain unauthorized access or to attack.

2.1 Digital Image Steganography

The concept of "What You See Is What You Get, WYSIWYG" which is encountered sometimes while printing images or other material is no longer precise and would not fool a steganographer as it does not always hold true. Images can be more than what can be seen with the Human Visual System, HVS, hence, they can convey more than merely 1000 words. For decades people strove to develop innovative methods for secret communication. Three techniques are interlinked, steganography, watermarking and cryptography. The first two are quite difficult to tease apart especially for those coming from different disciplines [20].

Drawing a line between these techniques is both arbitrary and confusing [21]. Therefore, it is necessary to discuss briefly these techniques before a thorough review is provided. Figure 2.1 and Table 2.1 may eradicate such confusion. The work presented here revolves around steganography in digital images and does not discuss other types of steganography, such as linguistic or audio. Table 2.1 summarizes the differences and similarities between steganography, watermarking and cryptography, figure 2.2 shows that media TV channels usually have their logos watermark for their broadcasting. The term "cover image" is used throughout this dissertation to describe the image designated to carry the embedded bits. An image with embedded data, payload, is described as "stego-image" while "steganalysis" or "attacks" refer to different image processing and statistical analysis approaches that aim to break steganography algorithms.

Table 2.1 Comparison of Steganography, Watermarking and Cryptography

Criterion/Method	Steganography	Watermarking	Cryptography
Carrier	any digital media	mostly image/audio files	usually text based, with some extensions to image files
Secret data	payload & no changes to the structure	watermark & no changes to the structure	plain text & changes the structure
Key	Optional	Optional	Necessary
Input files	at least two unless in self-embedding	at least two unless in self-embedding	One
Detection	Blind	usually informative, i.e., original cover or watermark is needed for recovery	Blind
Authentication	full retrieval of data	usually achieved by cross correlation	full retrieval of data
Objective	secret communication	copyright preserving	data protection
Result	stego-file	watermarked-file	cipher-text
Concern	delectability/ capacity	Robustness	Robustness
Type of attacks	Steganalysis	image processing	cryptanalysis
Visibility	Never	sometimes, see Figure 2.2	Always
Fails when	it is detected	it is removed/replaced	de-ciphered
Relation to cover	not necessarily related to the cover. The message is more important than the cover.	usually becomes an attribute of the cover image. The cover is more important than the message.	N/A

Flexibility	free to choose any suitable cover	cover choice is restricted	N/A
History	very ancient except its digital version	modern era	modern era

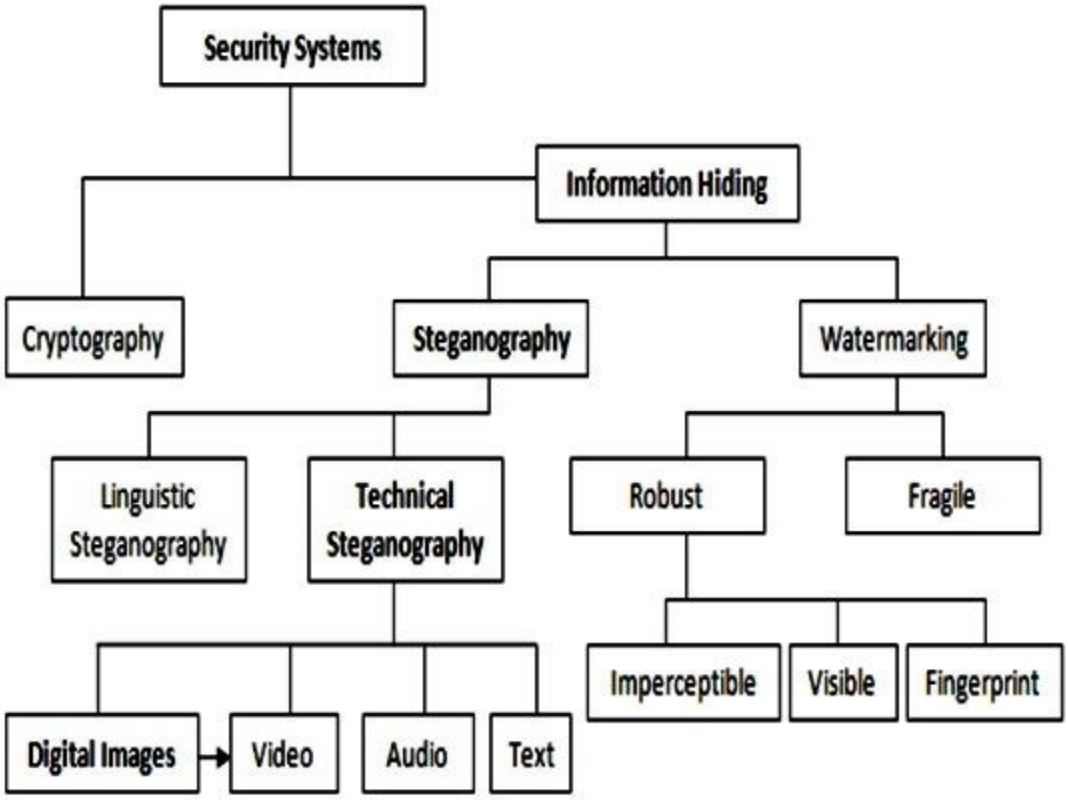


Figure 2.1 The different embodiment disciplines of Information Hiding.

Figure 2.2 Media TV channels usually have their logos watermark.

Steganography techniques aimed at secretly hiding data in a multimedia carrier such as text, audio, image or video, without raising any suspicion of alteration to its contents. The original carrier is referred to as the cover object. In this work, we will mainly focus on image steganography. Therefore, the term cover object now becomes cover image. Figure 2.3 illustrates a basic information hiding system in which the embedding technique takes a cover image and a secret image as inputs and produces as output a stego image, which is the seemingly unchanged cover image with the embedded data. The stego image may be sent over the communication links to the receiver who can carry out the extraction procedure to retrieve the secret message from the stego image.

2.2 Data Hiding Techniques

There are three different approaches that can be used to hide information in a cover object:

- Injection,
- Substitution and
- Generation

2.2.1 Injection

The data can be hidden in sections of a file that are ignored by the processing application using injection technique [22]. Therefore file bits that are relevant to an end-user are not modified—leaving the cover file perfectly usable. For example, we can add additional harmless bytes in an executable or binary file. Because those bytes don't affect the process, the end-user may not even realize that the file contains additional hidden information. However, using an insertion technique changes file size according to the amount of data hidden and therefore, if the file looks unusually large, it may arouse suspicion.

2.2.2 Substitution

Substitution technique is used to replace the least significant bits of information that determine the meaningful content of the original file with new data in a way that causes the least amount of distortion. The main advantage of this technique is that the cover file size does not change after the execution of the algorithm. On the other

hand, this approach has at least two drawbacks. First, the resulting stego object may be adversely affected by quality degradation—and that may arouse suspicion. Second, substitution limits the amount of data that you can hide to the number of insignificant bits in the file.

2.2.3 Generation

Unlike injection and substitution, generation techniques [23] do not require an existing cover file. This technique generates a cover file for the sole purpose of hiding the message. The main flaw of the insertion and substitution techniques is that people can compare the stego object with any pre-existing copy of the cover object (which is supposed to be the same object) and discover differences between the two. We will not have that problem when using a generation approach, because the result is an original file, and is therefore immune to comparison tests.

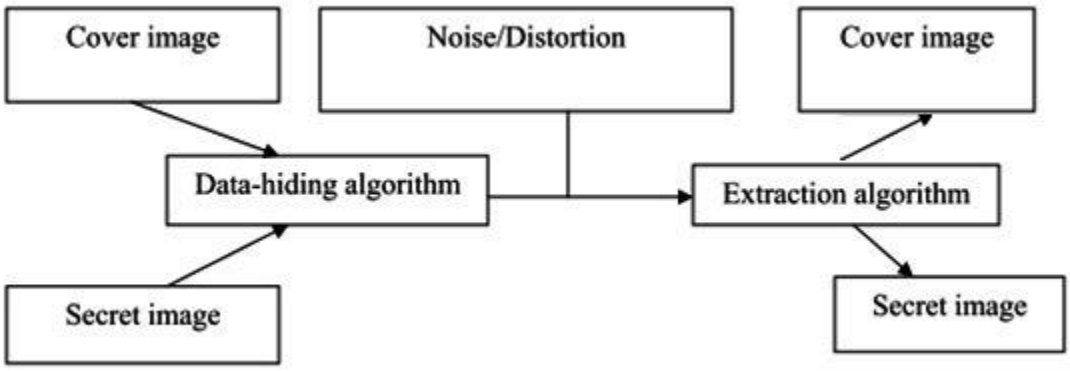


Figure 2.3 Image Steganography System

2.3 Substitution Algorithms

There is an increased interest in using digital images as cover objects for the purpose of steganography because of the proliferation of digital images over the Internet and given the high degree of redundancy present in a digital representation of an image (despite compression). There has been a number of image steganography technique algorithms based on the substitution approach. They can be categorized into two types:

- Spatial Domain Techniques and
- Transform Domain Techniques.

2.3.1 Spatial Domain Techniques: In the spatial domain approach, the cover image pixels are directly used to describe bits of the secret data whereas in the frequency domain, the cover image first undergoes a transformation into its frequency domain and then its transformed coefficients are altered to embed the secret information.

- **Spatial Domain Algorithm**

Spatial domain algorithms embed data by substituting carefully chosen bits from the cover image pixels with secret message bits. LSB-based techniques are the most widely known steganography algorithms, which work by replacing the least significant bits of an image pixel. These modifications could be interpreted as random noise, which should not have any perceptible effect on the image. That is usually an effective technique in cases where the LSB substitution does not cause significant quality degradation, such as in 24-bit bitmaps. Some algorithms change LSB of pixels visited in a random walk, others modify pixels in certain areas of images, or simply increment or decrement of the pixel value [24]. Our proposed technique is based on LSB technique. For example, to hide the letter "a" (ASCII code 97 that is 01100001) inside eight bytes of a cover, we set the LSB of each byte like this:

10010010
01010011
10011011
11010010
10001010
00000010
01110010
00101011

The application decoding the cover reads the eight Least Significant Bits of those bytes to re-create the hidden byte—that is 01100001—the letter "a."

2.3.2 Transform Domain Technique

Transform domain techniques [25] hide data in mathematical functions that are in compression algorithms. DCT technique is one of the commonly used transform domain algorithm for expressing a waveform as a weighted sum of cosines. The data is hidden in the image files by altering the DCT coefficient of the image. Specifically, DCT coefficients which fall below a specific threshold are replaced with the secret

bits. Taking the inverse transform will provide the stego image. The extraction process consists in retrieving those specific DCT coefficients.

The LSB technique is used to hide the secret image bits in the cover image to obtain the stego image. The stego image is transformed from spatial domain to the frequency domain using DCT. And finally quantization and run length coding algorithms [25] can be used for compressing the stego image to enhance the security.

Steganography is a best technique to hide secret message into digital media specially in image which is called image steganography because image has many redundant bits so secret information can be hidden by replacing the bits of secret message with redundant bits.

Image steganography uses many methods for information hiding such as Least Significant Bit and Scrambling. Image scrambling is based on transposition cryptography which is a password replacement method with the change in location not in content of secret message. In image scrambling, the location of image pixels is changed and then re-arranged. Image scrambling can be one dimensional or two dimensional [9, 10]. Basically image scrambling is of three types:

i. Image hash scrambling
ii. Magic transformation
iii. Shape transform

Least Significant Bit image steganography is most commonly used algorithm in which least bit is replaced with MSB of secret message. It can be used with wavelet transformation [9]. As we know that image has contrast levels and small pieces of secret information can be hidden at every contrast level and it slightly changes the contrast. LSB also uses lifting wavelet transform. Lifting wavelet transformation can be considered as a technique having the properties of wavelet transform such image transformation, multi resolution and image restoration.

As technology is going to increase, improvements are also being done on LSB. A randomized LSB algorithm is also developed in which secret message is embedded randomly in RGB plane with the help of random generator. As we know the range of red colour is 0-85, range of green is 86-170 and range of blue is 171-255. If the integer value which is generated by random generator lies between 0-85, then it is

embedded into red colour range, if it lies between 86-170 then it is embedded in green colour range otherwise it is in blue colour range.

2.4 Algorithms in Spatial Domain

LSB Image steganography algorithm can be used in spatial domain. In spatial domain, it is used as LSB substitution. In spatial domain, a permutation is performed before embedding the bits and it has distributed effect only due to which hardly half of the bits are changed in LSB. But some algorithm based on random walk in which they choose random pixels in selected parts of image. These algorithms do not change least bit sequentially. Some important categories of algorithms in spatial domain are:

i. Non Filtering Algorithms
ii. Randomized Algorithms
iii. Filtering Algorithms

2.4.1 Non Filtering Algorithms

It consists of sequential insertion of message bits with image least significant bits due to this it is considered the simplest one. This method causes only a small modification in the intensity level of colours.

2.4.2 Randomized Algorithms

As we know that the non-filtering algorithms are simple and easy to detect the presence of secret message and also to access the secret message. So, randomized algorithm provides the better solution by inserting the concept of random number generator. It is also called the pseudo random generator which provides the access of password and well distribution of message bits over pixels of image.

2.4.3 Filtering Algorithms

In these types of algorithms, a filtering process which uses a default filter is performed on cover image and areas of image which has better rate is found to hide secret message.

2.5 Related Literature

Zhi and Fen [26] proposed method of LSB image steganography, which was used a method called detection of random LSB. They use passive steganalysis method for detection of secret message in stego image. This method used the concept

of RS in which secret message was inserted in selected part of image randomly not in fixed or predefined manner due to this steganalysis becomes difficult. In this method, gradient energy of image is analysed theoretically based on steganalysis detection method called GEFR. To hide a secret message, a pixel can be detected easily because gradient energy level varies from pixel to pixel.

Khosravirad *et al.* [27] proposed a new LSB technique which can be applied in both spatial domain as well as transform domain. This technique uses the concept of COS which is high order statistical property. They try to find a subset of secret message in the pixel set of an image due to which less of bits are changed in image which results less change in the bits of image. They also introduced the concept of vector of features. These features help in the classification of stego image. This method is more accurate than the method proposed by Harmsen which uses second order vector feature. In Harmen's method, false alarm was about to 14.75 % while in this method, the false alarm is reduced about to 1.5 %.

Zhang *et al.* [28] introduced a new method of LSB steganalysis which is based on statistical distribution of pixel difference in spatial domain. Can be done on high resolution images. Based on the difference of zero and non-zero values of pixels and also finds the error which is used to determine the steganographic features. It also uses Laplacian distribution. As we know that pixels are highly correlated to each other in image and zero, non-zero values occur frequently. If change in the some neighbour's pixel value then it may slightly change the intensity level of colours.

Luo *et al.* [29] introduced a more appropriate LSB technique. They developed an improved Random scattered method called RRS method over RS. In RRS, the value of pixels is adjusted slightly in the embedded image. Firstly, the secret message is embedded in cover image using LSB and then a compensation is done dynamically on the stego image due to this RS steganalysis is decreased near the value to 0 cause inappropriate steganalysis. In this method, one is added to the pixel value of secret message which is called compensation and then uses the RS method to adjust the pixels value in image. Basically, this method provides more resistance to RS steganalysis.

Cvejic and Seppanen [30] presented modification to standard LSB algorithm in which embedding is done four bit per sample due to which capacity of storing secret information is increased by 33 present. They tried to decrease the SNR value within silent parts and where the value of audio changing slowly using modified error diffusion as well as adjustment of LSB with the help of error replacement method. In this method, closed level of audio is found and then secret message is inserted into audio. After that, minimum error replacement is calculated and maximum error replacement is tried to decrease to 2^{k-1} caused the LSB performance improvement.

Thenmozhi and Chandrasekran [31] presented a novel approach for building a secure data hiding technique of Steganography using integer wavelet transform along with cropping. Employed frequency domain to increase the robustness of the proposed steganography method. cropping function and OPAP has been utilised to obtain an optimal mapping function to reduce the difference error between the cover and the stego-image and to increase the hiding capacity with low distortions respectively. Simulation results showed that the novel scheme outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity.

Balakrishana *et al.* [32] proposed single digit sum (SOS) based image steganography. Proposed technique controlled the amount of change in pixel. Determined the base for computing SOS by using upper limit of pixel. Ensured that the stego image does not degrade beyond the degradation in the compressed image.

Martin *et al.* [33] investigated whether stego-images, bearing a secret message, are statistically "natural" or not. Utilized recent results on the statistics of natural images and investigated the effect of some popular steganography techniques. Found that these fundamental statistics of natural images were, altered by the hidden "nonnatural" information. Considered the class of natural images, for which the change generally falls within the intrinsic variability of the statistics, and didn't allow for reliable detection, unless knowledge of the data hiding process is taken into account.

Thenmozhi and Chandrasekran [34] presented a novel technique for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. Discussed the chaotic system, and its advantages for achieving the encryption of data. Applied the henon

mapping (chaos) on the secret image and performed the two dimensional Discrete Wavelet Transform (2-D DWT) on the cover image of size M × N. improved the Image quality by preserving the wavelet coefficients in the low frequency sub band. Experimental results showed that the algorithm has a high capacity and a good invisibility.

Prabhakran and Bhavani [35] proposed secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Performed Arnold transformation to scrambles the secret image. Also performed Discrete Wavelet Transform (DWT) is performed in both images, followed by Alpha blending operation. Applied the Inverse Discrete Wavelet Transformation (IDWT) to get the stego image. Investigated the performance of the proposed scheme by comparing various qualities of the stego image and cover image. Results showed that the proposed algorithm for steganography is highly secured with certain strength in addition to good perceptual invisibility.

Das and Tuithung [36] presented the technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q were used as cover image and secret image respectively. Performed Huffman Encoding over the secret image/message before embedding and each bit of Huffman code of secret image/message was embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, so that the Stego-Image became standalone information to the receiver. Experimental result showed that the algorithm had a high capacity and a good invisibility. Proposed technique showed better result in comparison with other existing steganography techniques.

Keshari and Modani [37] proposed an innovative technique for image Steganography based on Weighted fractional Fourier Transformation (WFRFT). The secret image was embedded in the intermediate domain of the cover image. Window size of 2 x 2 was selected from the cover image and converted into its intermediate domain between spatial and frequency by using WFRFT. Performed the inverse WFRFT to convert back from intermediate domain into spatial domain to generate the stego image. Secret image was received at recipient side through the reverse procedure of adopted at transmitter. Experimental results were demonstrated and discussed through histogram analysis for verifying the proposed technique.

Sethi and Sharma [38] proposed a new method to develop secure image-encryption techniques using a logistics-based encryption algorithm. Utilized a Haar wavelet transform technique to decompose the image and decorrelate its pixels into averaging and differencing components. Demonstrated the validity of the proposed scheme by using the test images. Performed the tests like NPCR, UACI, PSNR etc on the sample images to prove the results.

Ramaiya *et al.* [39] presented a unique technique for Image steganography based on the Data Encryption Standard (DES) using the strength of S-Box mapping & Secret key. Carried out the preprocessing of secret image by embedding function of the steganography algorithm using two unique S-boxes. Also proposed the scheme, capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption.

Zhiwei *et al.* [40] discussed image steganography combined with pre-processing of DES encryption. When transmitting the secret information, firstly, encrypt the information intended to hide by DES encryption was encrypted, and then was written in the image through the LSB steganography. Improved the Encryption algorithm lowest matching performance between the image and the secret information by changing the statistical characteristics of the secret information to enhance the anti-detection of the image steganography. Experimental results showed that the anti-detection robustness of image steganography combined with pre-processing of DES encryption was found much better than the way using LSB steganography algorithms directly.

Karim *et al.* [41] introduced a best approach for Least Significant Bit (LSB) based on image steganography that enhanced the existing LSB substitution techniques to improve the security level of hidden information. The new security conception stored the hidden information into different position of LSB of image depending on the secret key. Result showed that it was difficult to extract the hidden information knowing the retrieval methods. utilized the Peak Signal-to-Noise Ratio (PSNR) to measure the quality of the stego images. Proposed method changes very small number of bits of the image and hence gives the better result. Result showed that the proposed method results in LSB based image steganography using secret key which provides good security issue and PSNR value than general LSB based image steganography methods.

Moon and Kawitkar [42] utilized the least significant bit substitution method [2]. Implemented the method for color bitmap images (24 bit and 8 bit i.e. 256 color palette images) and wave files as the carrier media. proposed algorithm can hide the file of any format in an image and audio file. Then send the image via e-mail attachment or post it on the web site and anyone with knowledge that it contains secret information, and who is in possession of the encryption password, will be able to open the file, extract the secret information and decrypt it.

Li *et al.* [43] proposed LSB Information Hiding algorithm which could Lift wavelet transform image. Furthermore, made the objective evaluation of image quality by the PSNR and normalized cross correlation coefficient. Achieving the purpose of information hiding with the secret bits of information to replace the random noise, using the lowest plane embedding secret information to avoid noise and attacks, utilized redundancy to enhance the sound embedded in the way nature to be addressed. Results showed that the proposed algorithm has a very good hidden invisibility, good security and robustness for a lot of hidden attacks.

Shejul and Kulkarni [44] proposed a DWT based approach for steganography using biometric features. Here, the secret data embedded in skin region of image that provides secure location for data hiding. They hide Secret data in one of the high frequency sub band of DWT by tracing skin pixels. All the steps of data hiding are applied on the cropped image. This provides security to the method and PSNR is used to determine the quality of stego image after embedding the secret data.

2.6 Overview of XOR Algorithm

The combined approach of steganography and cryptography play an important role in information security because if someone detect the presence of secret message in any media file, he cannot use this information directly due to in encryption form. So, neither steganography nor cryptography is alone better. Cryptography provides security to information. Many algorithms have been already developed some of these take more space and some of these take less time such as XOR, AES, DES, TDES, Blowfish and RSA [14]. XOR algorithm is simple one and it takes less space but slightly more time than other. So, we can use XOR algorithm for enhancement because it has less time complexity. XOR encrytion algorithm is simple algorithm

because it performed only XOR operation between the bit of key and plaintext. It first convert plaintext and key to their equivalent binary value, then XOR operation is performed between binary value of key and plaintext, called encryption. Decryption is same as encryption and it is performed again XORing of the binary value cipher text and key. In it, cipher text takes equal space as original plaintext. XOR algorithm can work only binary signals or values and encrypts each pixels separately because image is made up of a lot of pixels and each element (character, symbol, number etc) of information can be converted into binary value.

XOR algorithm is also suitable for multimedia data such audio, video and image but pixels are in multimedia are highly correlated [12]. Pixels values can be redistributed to different location by using affine transformation with XOR operation. Scrambling of plain text/image can be performed using XOR encryption with Modulo-256 addition operations for two round independent of chaotic map and no iteration method is used in any choatic map for scrambling [12].

2.7 Least Significant Bit Image Steganography Algorithm

LSB is simple and most commonly used image steganography algorithm. LSB is basically follow insertion process in which last bit is simply replaced by the bit of secret message [29].

At first, original image called cover image (I) is converted into 8-bit stream but if we are using a 24-bit image then it can also be divided into 3 block of 8-bit of red, green and blue colour component [26]. Then LSB or last bit of each 8-bit block is replaced with the bit of secret message/image sequentially or randomly using a pseudo-random generator with the help of stego-key [27].

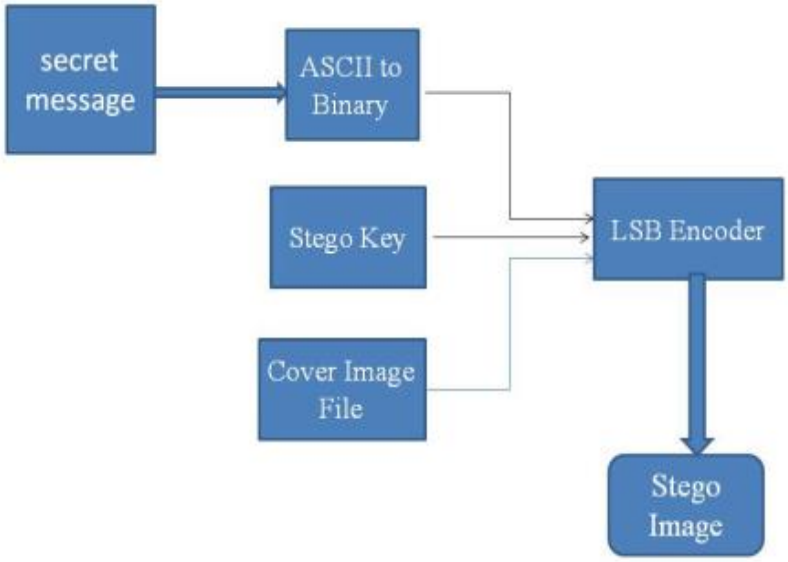


Figure 2.4 LSB Insertion Mechanism

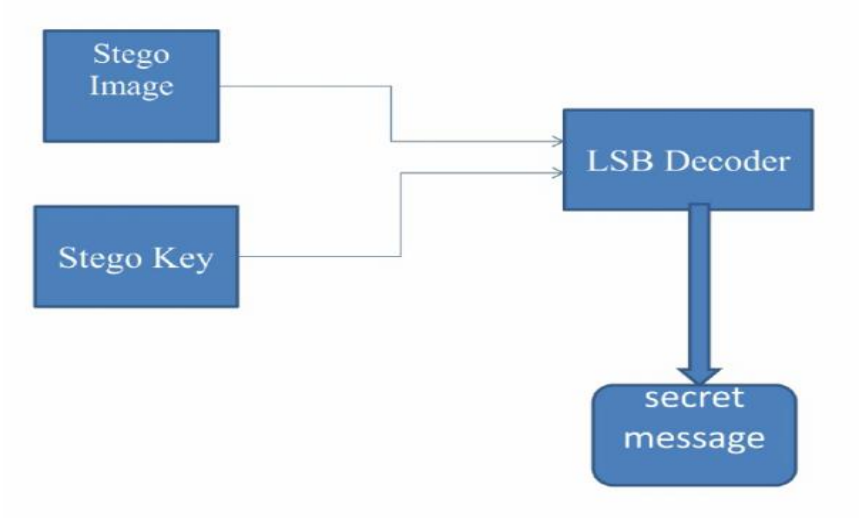


Figure 2.5 LSB Extraction Mechanism

Suppose, we have a 24-bit image, then three pixels of the image are

11010011 01100101 00111010

01110101 10101100 11011001

10010001 10101001 10110011

When we want to hide the secret message which ‘A’ and the 8-bit equivalent value of A is 01000001 then resulting value of above pixels are

11010010 01100101 00111010

01110100 10101100 11011000

10010000 10101001 10110011

Here we need to change only 4 bits. As we know that primary colour intensities are from 0 to 256 (Red 0-85, Green 86-170, Blue 171-255) [28] and only 4 changes may only result a small change in intensities which cannot be easily detected by human eyes.

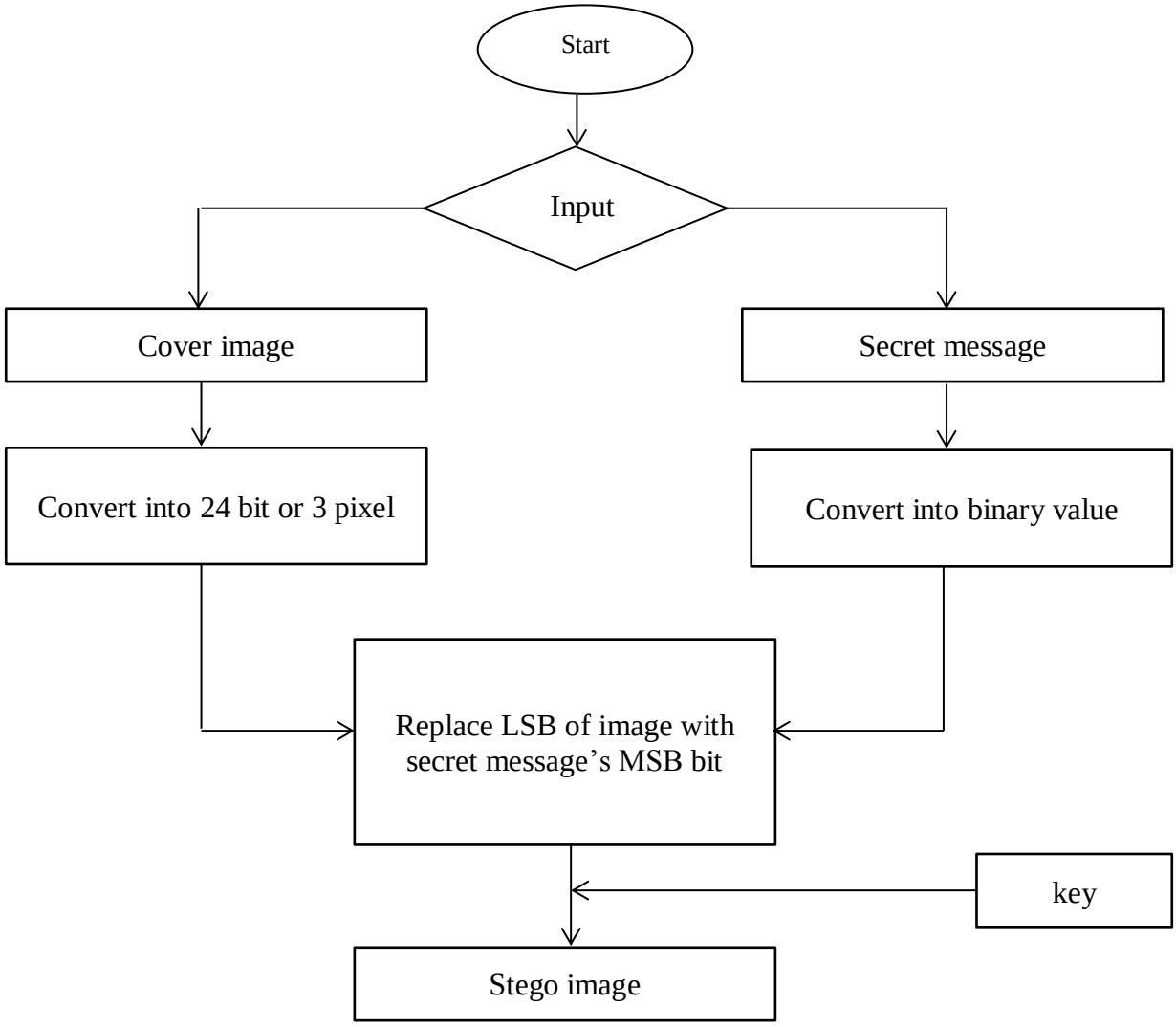


Figure 2.6 Flow chart of LSB

CHAPTER 3

PROBLEM STATEMENT

In modern era, unauthorized access of information increasing day by day due to this we need to secure information and this can be done using cryptography or steganography technique. There are many image steganography and cryptography algorithms has been already developed such as Least Significant Bit (LSB), Random Scattered (RS), Most Significant Bit (MSB) but LSB is most frequently used because it simply inserts the bit of secret message with the least significant bit of image. LSB is very simple due to this detection of secret message is also easy, so we need to develop an improved version of LSB algorithms which is more secure than LSB.

CHAPTER 4

PROJECT DESIGN AND IMPLEMENTATION

4.1 Cryptography Vs Steganography

Cryptography and Steganography differ to each other because cryptography is used to keep the contents of the message secret while steganography is used to hide the existence of secret message. Both techniques are used to protect information from the unauthorized use but sometime it is used in illegal means and neither cryptography is alone perfect nor steganography. Both approaches can be used with each other, to provide better security because cryptography makes the message secret and steganography make existence of message invisible. If someone try to find the existence of secret message and finds but that message would not be understood because it would be encrypted due to the use of cryptography. So, by combining these two approaches, information can be made more secure.

4.2 United approach of steganography and cryptography

In united approach, first we use EXOR encryption algorithm and then Improved LSB image steganography algorithm. First the secret message is encrypted using EXOR and then it is embedded in any media using Improved LSB.

Steps used in combined approach-

Hiding process:

i. Input secret message or text
ii. Input key
iii. Encrypt secret message using EXOR
iv. Embedded this encrypt message using Improved LSB

Extraction process:

i. Extract message using Improved LSB
ii. Decrypt that message using EXOR with same key

In this united approach, two algorithms are used one is image stenographic algorithm called Improved LSB and another is cryptographic algorithm called Extended XOR (EXOR).

4.3 Proposed Algorithms

In this dissertation, we are using two algorithms in which one is Improved LSB steganography algorithm and second is Extended XOR cryptography algorithm.

4.3.1 Improved LSB Algorithm

In LSB Algorithm, only least significant bit is replaced by information bit but in Improved LSB, least significant bit is not directly changed. It will change with the help of second least significant bit and the information bit. There are four rules based upon which value of least significant bit is calculate and then replaced.

Rules-

Table 4.1 Operation for Improved LSB

2^{nd} least significant bit of image	Bit of information to be hidden	Resultant Least significant bit to be replaced
0	0	1
0	1	0
1	0	0
1	1	1

These operations are used for both to hide and to extract the information.

Steps used in proposed Improved LSB:

Hiding process:

1. find the pixel value of cover image

2. find the value 2nd LSB of each pixels of cover image
3. find the binary value of message to be hidden
4. perform the operation with the help of rules between the value 2nd LSB of each pixels and bits of message
5. find the resultant value of LSB

Extracting process:

1. find the pixel value of stego image
2. find the value 2nd LSB and LSB of each pixels of stego image
3. perform the operation with the help of rules between the value 2nd LSB and LSB of each pixels of stego image
4. find the resultant bits of hidden message

Suppose value of three pixels of cover image is:

11010011 01100101 00111010

01110101 10101100 11011001

10010001 10101001 10110011

Suppose we want to hide 'A'. Binary value of a is 01000001

Table 4.2 Hide Message and Calculation of LSB

2nd least significant bit of cover image	Bit of information to be hidden (A)	Resultant LSB to be replaced with LSB of cover image
1	0	0
0	1	0
1	0	0
0	0	1
0	0	1

0	0	1
0	0	1
1	1	1

Table 4.3 Extraction of Hidden Message

2^{nd} least significant bit of stego image	Least significant bit of stego image	Bit of information to be extracted
1	0	0
0	0	1
1	0	0
0	1	0
0	1	0
0	1	0
0	1	0
1	1	1

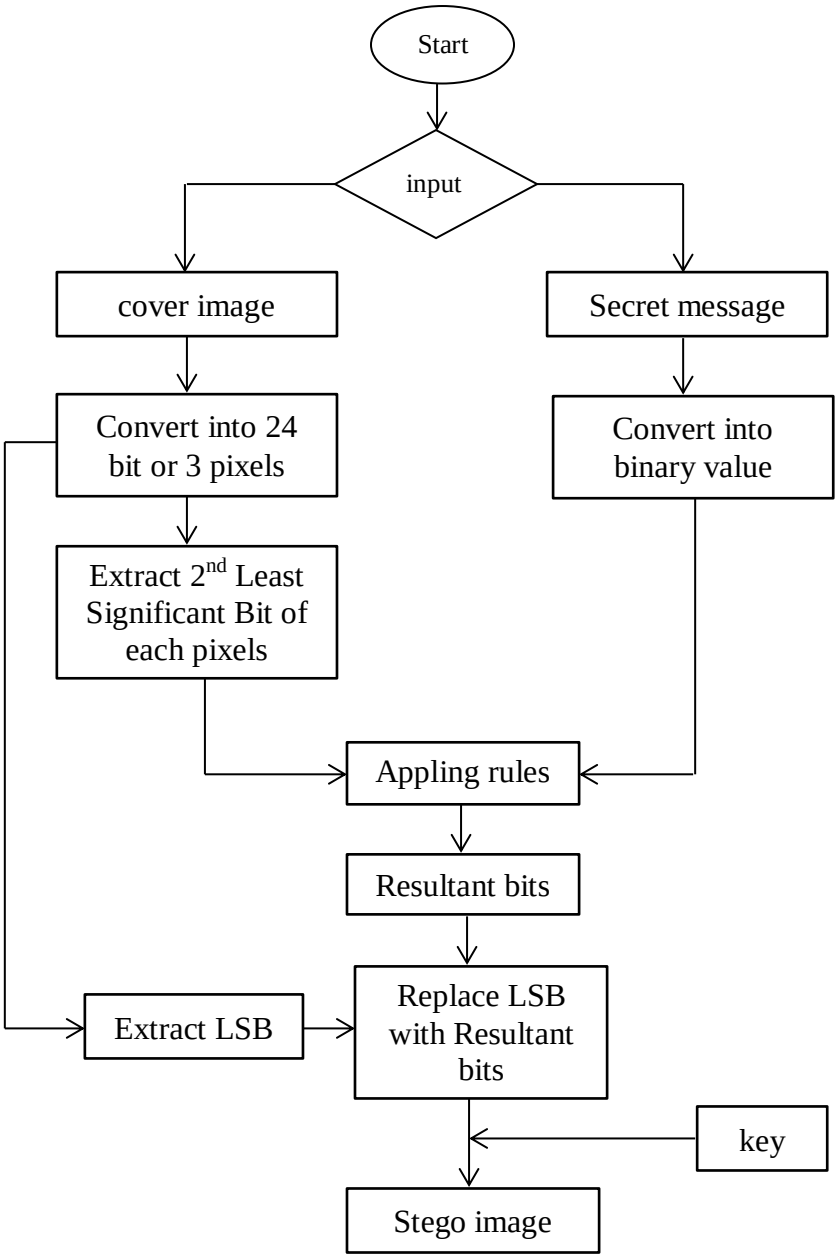


Figure 4.1 Flow chart of Improved LSB

4.3.2 Extended XOR Encryption System

Extended XOR (EXOR) is an enhanced version of XOR encryption algorithm. It is a symmertic key algorithm means same key is used to encrypt and decrypt.The length of key is 64 bit. It is a block cipher algorithm which takes block of bit as input which makes encryption faster. It is an iterative version with the concept of modulo. This algorithm is using divide and conquer approach because first it divides the information into blocks then encrypt/decrypt each block and finally, it merge the

encrypted/decrypted block. Each block is processed in parallel which makes it faster then simple XOR encryption.

This algorithm can be divided into three parts namely

i. Calculating the value of variables like F, L, M, N, n and I.

ii. Encryption

iii. Decryption

i. Calculating the value of variables

Modulo is based on the ASCII value of key means that ASCII value of the first and last character/digit/number/symbol are used to compute the modulo. The value of first charatcter, called 'F', is divided by the value of last character, called 'L' and The value of modulo is stored in a variables represented by 'M'. If key has only one character then ASCII value of this charater contains two digits and than M is computed by dividing the decimal value of first digit by the decimal value of second digit. If the value of F and L are same then do F=F+1 means the value of next element which is second element is considered as F but if all the units of key are same then we assume only first unit of key and find the modulo assuming first digit of unit as 'F' and second digit as 'L'. Then the binary value of the key is computed and find the number of 1s in the binary value of key and store in a varible called **'n'**. The value of modulo of 'M' and 'n' is stored in an another variable named 'I'. There is also an another varible called **'N'** which stores the binary value of plaintext or information.

ii. Encryption

The value of modulo M is used to divide the plain text into block. If the value of M is not multiple of eight then the value of M is divided by eight and remainder R is added in the value of M. The purpose of making M as multiple of eight is as we know each character is represented in binary form by one byte or eight bits. So, the value of bit in the information is always multiple of eight. If the value of N is not divisible by M then find the modulo of M and N, then make remainder **S** bits (last S bits of N) as a separate block and finally divide N-S into M blocks due to this the value of total blocks become M+1.

The value of I is used to change the I^{th} bit of the block defined from 1 to 0 or 0 to 1 then XOR operation is performed between binary value of key and binary value of each changed blocks. Then again, the value of I^{th} bit in the block obtianed from previous stage is changed from 0 to1 or 1 to 0. Again, XOR operation is performed between the binary value of each block obtained from previous stage and binary value of key. This step or iteration is performed according to the value of **n** or equal to the value of **n** (n<=64). Finally, changed block are combined which is called cipher text 'C'.

iii. Decryption

Decryption process same as encryption. In decryption, first according to the value of modulo constant M, cipher text is divided into blocks. If the value of block may be M+1 because cipher text may not be divisible by M then we have to make a separate block of remainder bits. Then according to the value of I, the value of I^{th} bit in each block is changed from 0 to 1 or 1 to 0 and XOR operation is performed between the binary value of key and binary value of each block of cipher text. Again, the value of I^{th} bit is changed and XOR operation is performed between the key and binary value block obtained from previous stage. This process is continused equal to the value of **n** then only Xoring of Binary value of key and obtained block from previous stage is done. Finally, after combining the binary value of each block obtain one can easily get the origional plain text.

The EXOR encryption algorithm can be written in following steps-

1. Find the ASCII value of key
2. Find the ASCII value of '**F**' and '**L'**
3. while (F=L)
4. do
5. {
6. Then F= F+1
7. }
8. Calculate the value of **M**

9. **{**
10. M = F mod L
11. }
12. Calculate the value of **n**
13. Calculate the value of **I=** n%M
14. Find the binary value of Plain text called **N**
15. If (M % 8 !=0)

    {

    Then R= M%8

    R=8-R

    M=M+R

    }

//Divide binary value of plaintext into blocks //

16. If (N % M =0)

    {

    Divide N into M blocks

    }

    Else

    {

    S= N%M

    Make separate block last S bits

    Divide (N-S) into M blocks

    }

17. Perform XOR operation parallelly between the value of binary valued blocks and Key
18. For i=0 to i<=n (n<=64)

i. Change the value of I^{th} bit of each block

ii. performe XOR operation parallelly between obtained changed value of block from previous stage

19. Combined the value of blocks and obtained Cipher text.

// *Steps used in decryption are as followed*//

20. Repeat step 1 to 11

21. For i=0 to i<=N

i. Perform the XOR operation between key and changed value of block

ii. Change the I^{th} of the each block

22. Finally, perform the XOR operation between the key and output of previous stage block.

23. Convert binary to plaintext.

Here,

- Steps 1-14 come under the calculation of variables phase.
- Steps 15-19 come under the encryption phase.
- Steps 10-13 perform parallelly which makes EXOR algorithm faster and secure.
- Steps 20-23 come under the decryption phase.

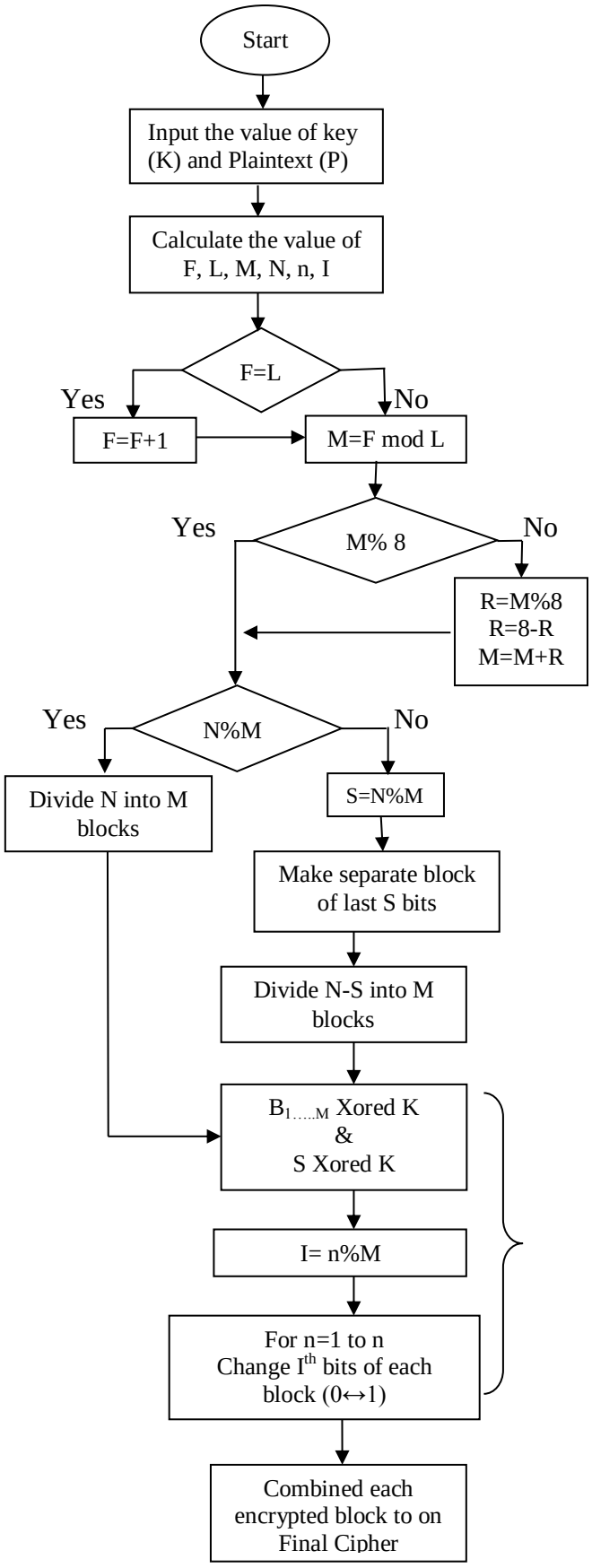


Figure 4.2 Flow Chart of EXOR

CHAPTER 5

RESULTS

If we encrypt a file by EXOR encryption algorithm, then we find that cipher text takes same space as original text. Comparison between XOR and EXOR algorithm can be done on the basis of time complexity, space complexity and security.

Table 5.1 Comparison of Space and Time Taken

Algorithm		Size of original file (in kb)	Size of Cipher Text (in kb)	Time in encryption (in ms)	Time in Decryption (in ms)
XOR		1	1	64	64
		18	18	1397	1132
		86	86	5800	4443
EXOR		1	1	236	211
		18	18	4985	4828
		86	86	22164	21679

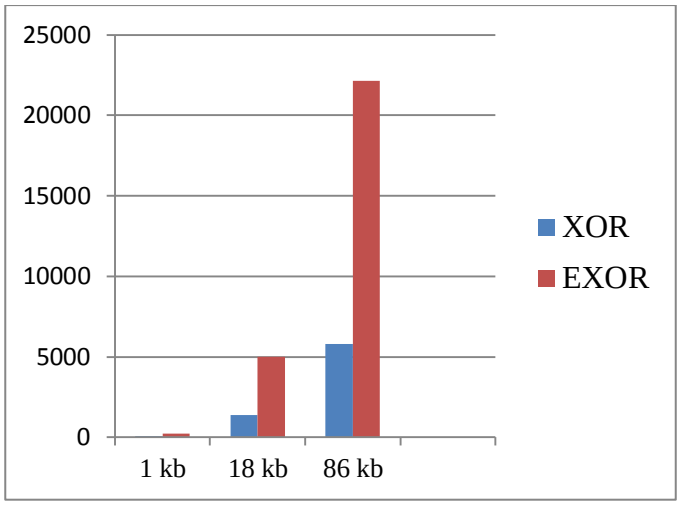


Figure 5.1 Time taken to Encrypt

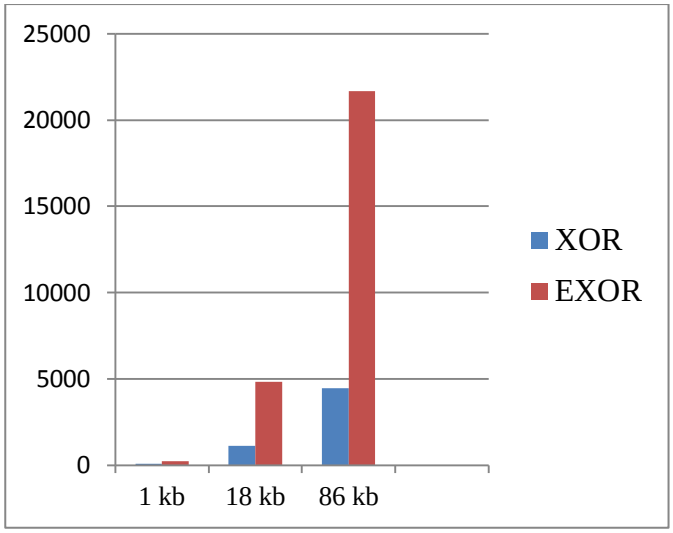


Figure 5.2 Time taken to Decrypt

In this dissertation, 24-bit bitmap file named dalia is taken and a message "improved Least Significant Bit algorithm" is being hidden using both algorithm which are existing LSB and improved LSB with the help of key "wish".

Figure 5.3 Original Image of Dalia

Figure 5.4 Image After Embedding Message Using Existing LSB

Figure 5.5 Image After Embedding Message Using Improved LSB

206 pixels are different in original image and image after embedding message in original image using improved LSB while 320 pixels are different in original image and image after embedding message in original image using existing LSB. But if we compare image after embedding message in original image using improved LSB and existing LSB, then 766 pixels are different.

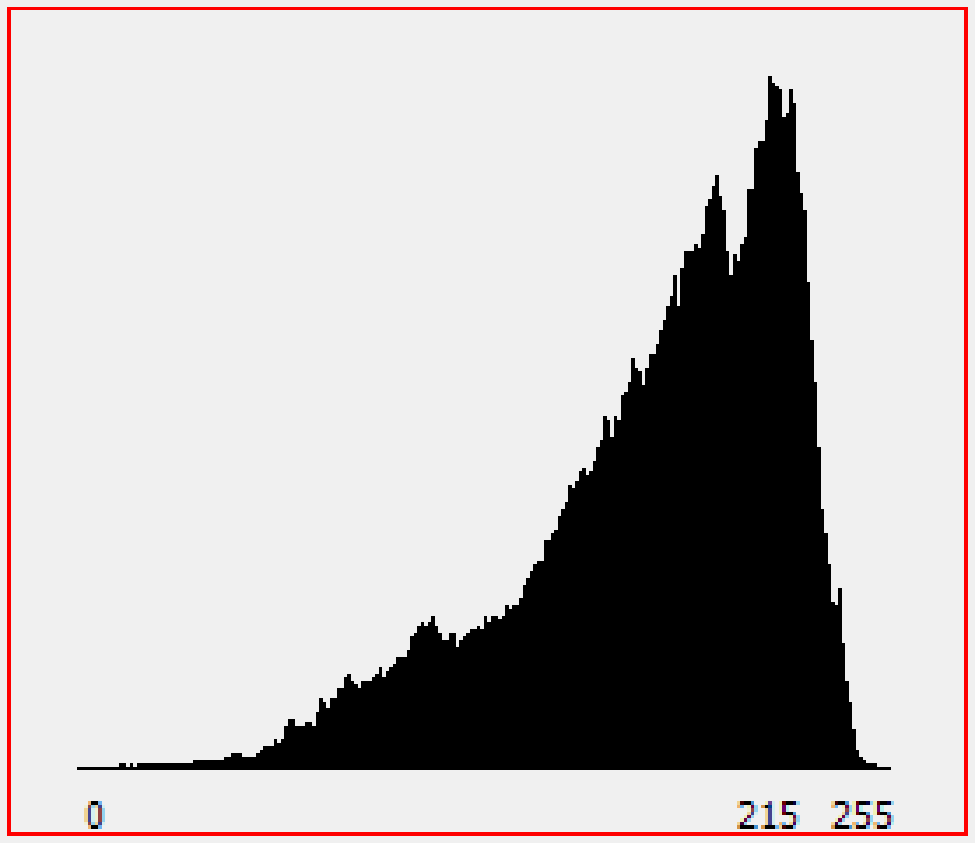


Figure 5.6 Histogram of Original Image

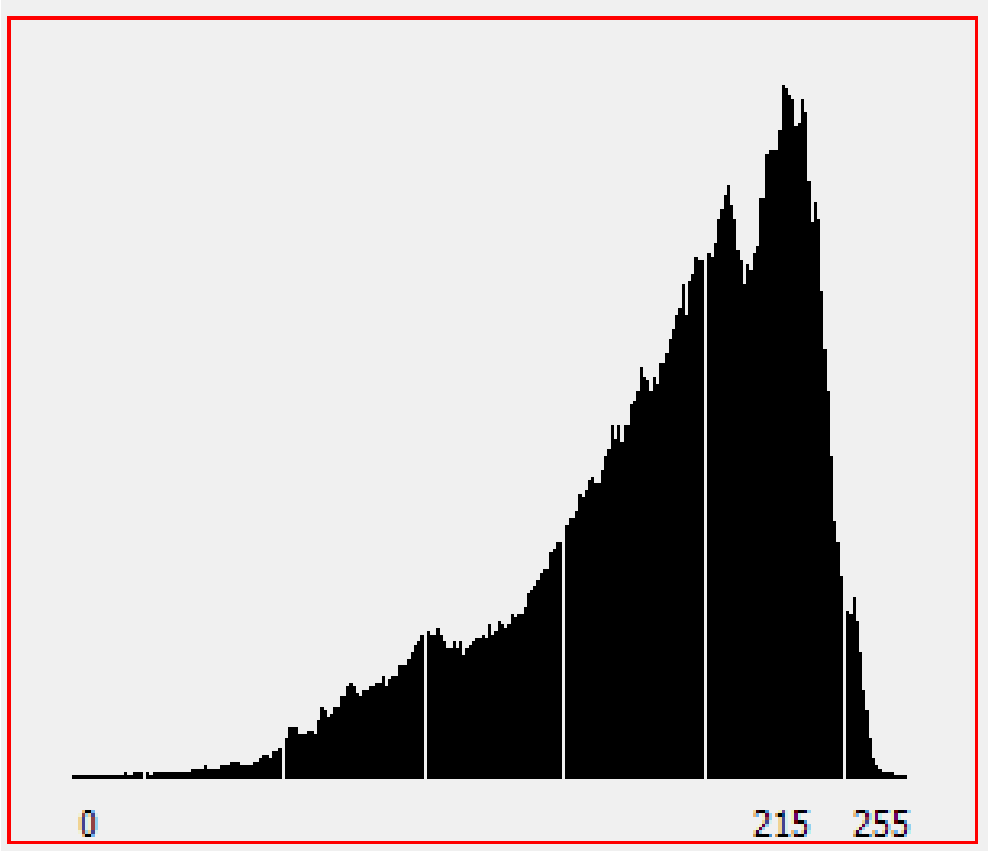


Figure 5.7 Histogram of Image after Embedding Message using Existing LSB

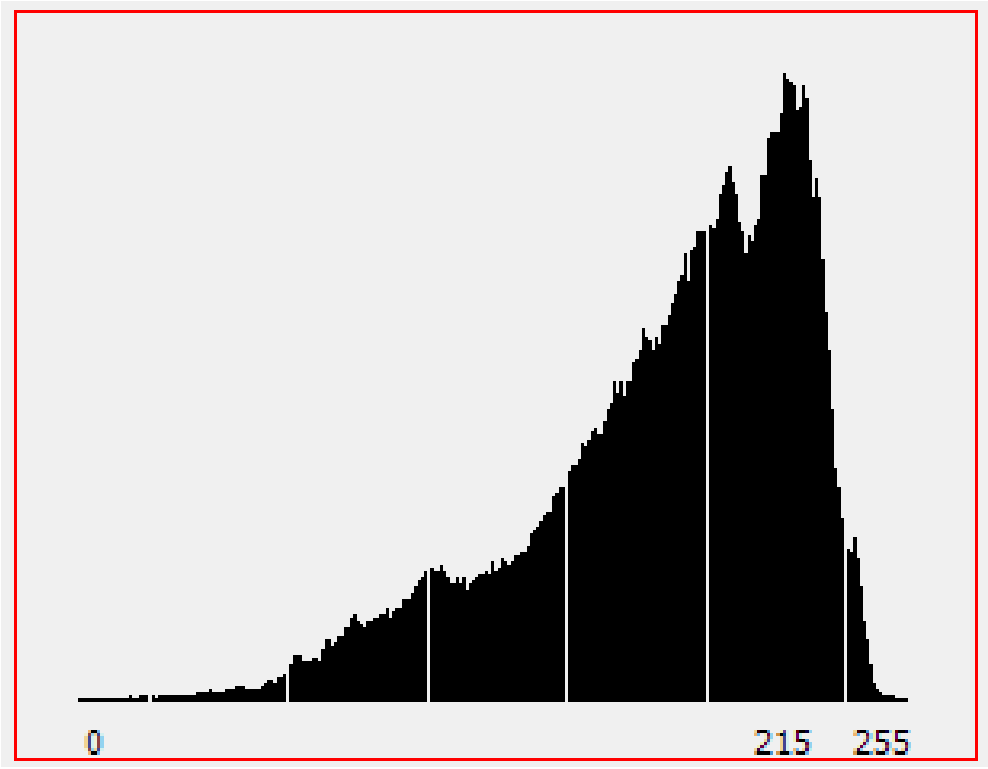


Figure 5.8 Histogram of Image after Embedding Message Using Improved LSB

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

In this dissertation we focus our concern in image because of it's widely used in Internet and also in mobile system. Improved LSB algorithm can easily be implemented and do not visually degrade the image to the point of being noticeable. It would appear that Improved LSB is good algorithm of Stegnography due to its security. Using Improved LSB algorithm we can exchange secret messages over public channel in a safe way. On the basis of above results, we can see that XOR and EXOR both the algorithm take same space after encryption and decryption. EXOR is more secure than XOR because it is an iterative version of XOR and iteration is totally dependents on the numbers of 1's in the equivalent binary value of the key. EXOR also uses modulo concept which makes it more secure but EXOR takes more time then XOR because encryption is done in one by one iterative process. Basically, it is working for documents, so it can be further enhanced to encrypt image, audio, video and other formats of information.

On the basis of above results, it can be seen that most of the time in improved LSB insertion operation less number of bits are changed in comparison of existing LSB algorithm, due to which the process of detecting existence of hidden information becomes difficult and if someone is able to find then he cannot be able to use because it would be in encrypted form due to EXOR encryption algorithm. So, combined approach of cryptography and steganography provides more security to information.

6.2 Future Work

Now a days, image steganography is broadly used in steganography field. So there is lot to do as per research is concerned. Time Complexity of EXOR can be reduced. We can use both the algorithm, EXOR and improved LSB with other cryptographic algorithms and steganographic algorithms which can reduce the space and time complexity and increase the level of security.

REFERENCE

[1] Fabien, A. P., Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G. ; "Information Hiding — A Survey", *Proceedings of the IEEE*, Vol. 87, No. 7, pp.1062-1078, 1999.

[2] Provos, N. & Honeyman, P. ;"Hide and Seek: An introduction to steganography", *Security and Privacy*, Vol.1, pp.32-44, 2003.

[3] Shirali-Shahreza, S. and Shirali-Shahreza M. ; "Steganography in Textiles", *4th International Conference on Information Assurance and Security* , pp.56-61, 2008.

[4] Singh, K. M., Singh, L. S., Singh, A. B. and Devi, K. S. ; "Hiding Secret Message in Edges of the Image", *International Conference on Information and Communication Technology* (ICICT), pp.238-241, 2007.

[5] Rahate, N. D. and Rothe, P. R. ; "Data Hiding Technique for Security by using Image Steganography", *International Conference on Industrial Automation and Computing* (ICIAC),pp 33-36, 2014.

[6] Caldwell, J., "Steganography using the technique of orderly changing pixel componenet", *International Journal of Computer Applications*, Vol.58, No.6, 2014.

[7] Delahaye, J. P. ; "Embeddeed Information, Information Hiding", *Scientific American*, pp.142-46, 1996.

[8] Morkel, T., Eloff, J. H. P. and Oliver, M. S. ; "An Overview of Image Steganography", *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA)*, 2005.

[9] Bo, X., Jia-zhen, W. and De-yun, Peng. ; "Practical Protocol Steganography: Hiding Data in IP Header", *the First Asia International Conference on Modelling & Simulation (AICMS)*, pp. 584-588, 2007.

[10] Avcibas, I., Memon, N., and Sankur, B. ; " Steganalysis Using Image Quality Metrics", *IEEE Transactions on Image Processing*, Vol. 12, No. 2, pp 221-229, 2003.

[11] Sethi, N. and Sharma D., ; "A New Cryptology Approach for Image Encryption", *2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, pp.905-908, 2012.

[12] Nag, A., Singh, J. P., Khan, S., Ghosh, S., Biswas, S., Sarkar, D. and Sarkar, P. P. ; "Image Encryption Using Affine Transformation and XOR Operation", *International Conference of Signal Processing, Communication, Computing and Networking Technologies (ICSCCN)*,pp.309-312,2011.

[13] K.Senthil, K., Prasanthi, and K., Rajaram, R. ; "A Modern Avatar of Julius Ceasar and Vigenere Cipher", *International Conference on Computational Intelligence and Computing Research*, pp.1-3, 2013.

[14] Mandal, A. K., and Parakash, C. ; "Performance Evaluation of Cryptographic Algorithms: DES and AES ", *Students' Conference on Electrical, Electronics and Computer Science*, pp.1-5, 2012,

[15] Dhull, S., Beniwal, S. and Kalra, P. ; "Polyalphabetic Cipher Techniques Used For Encryption Purpose", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol.3, No.2,2013.

[16] Stalling, W. ; "Network Security Essentials (Applications and Standards)", *Pearson Education*,2004

[17] Kahate, A. ; " Cryptography and Network Security", *2nd edition, McGraw-Hill*, 2009.

[18] Stallings, "Cryptography and Network Security", *2nd edition, Prentice Hall*, 1999.

[19] Stallings, W. ; "Cryptography and Network Security", *3rd edition, Pearson Education*, 2003.

[20] Johnson, N.F. and Katzenbeisser, S.C. ; "A survey of steganographic techniques", *International Journal of Computer Applications*, 2004.

[21] Wayner, P. ; " Disappearing cryptography", *2nd ed. Morgan Kaufmann Publishers*, 2002.

[22] Mastronardi, G.,and Castellano, M. M ; "Intelligent Data Acquisition and Advanced Computing Systems", Proceeding of IEEE on Computer Science and Security, Vol.87,No.7, pp.1179–1107, 1999.

[23] Shirali-Shahreza, M. and Shirali-Shahreza, M.H. ; "An Improved Version of Persian/Arabic Text Steganography Using "La" Word", *Proceedings of the 6th National Conference on Telecommunication Technologies 2008 (NCTT 2008)*, pp.26–28, 2008.

[24] Vishal, Wilson and Bryon ; "Linear, color separable human visual system model for vector diffusioning system", *Journal of Electronic Imaging*, Vol.1, pp.277-292, 1992.

[25] Wang, Y. and Moulin, P. ; "Statistical Signal Processing", *IEEE*, Vol.56 No.11, pp.339-342, 2003.

[26] Zhi, L. and Fen, S.A. ; "Detection of Random LSB Image Steganography", *Vehicular Technology Conference IEEE*, Vol. 3, pp.2113-2117, 2004.

[27] Khosravirad, S. R., Eghlidos, T. and Ghaemmaghami S. ; "Higher-order statistical steganalysis of random LSB steganography", *International Conference on Computer Systems and Applications*, 2009.

[28] Zhang, T., Li, W., Zhang, Y. and Ping, X. ; " Detection of LSB Matching Steganography Based on Distribution of Pixel Difference in Natural Images", *International Conference on Image Analysis and Signal Processing (IASP)*, pp.629-632, 2010.

[29] Luo, X., Liu, B. and Liu, F. ; "Detecting LSB Steganography Based on Dynamic Masks", *5th International Conference on Intelligent Systems Design and Applications*, pp. 251 – 255, 2009.

[30] Cvejic, N. and Seppanen, T. ; "Increasing the Capacity of LSB-based audio Steganography", *IEEE Workshop on Multimedia Signal Processing*, pp.336-338, 2002.

[31] Thenmozhi, S. and Chandrasekran, M., "Novel Approach for Image Stenography Based on Integer Wavelet Transform", *International Conference on Computational and Computing Research*, 2012.

[32] Balakrishana, C., Chandra, V. N. & Pal, R., "Image Steganography Using Single Digit Sum with Varying Base", *International Conference on Electronics, Computing and Communication Techonologies (CONECCT)*, pp.1-5, 2014.

[33] Martin, A., Sapiro, G. and Seroussi, G. ; "Is Image Steganography Natural", *IEEE Transactions on Image Processing*, Vol.14, pp.2040-2050, 2005.

[34] Thenmozhi, S. and Chandrasekran, M. ; "A Novel Technique for Image Steganography Using Nonlinear Chaotic Map", *7th International Conference on Intelligent Systems and Control (ISCO)*, pp. 307-311, 2013.

[35] Prabhakran, G. and Bhavani, R. ; "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", *International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, pp.1096-1100, 2012.

[36] Das, R. and Tuithung, T. ; "A Novel Steganography Method for Image Based on Huffman Encoding", *3rd International Conference on Emerging Trends and Application in Computer Science (NCETACS)*, pp. 14-18, 2012.

[37] Keshari S. and Modani, S.G. ; "Weighted Fractional Fourier Transformation Based Image Steganography", *International Conference on Recent Trends in Information Systems*, pp. 214-217, 2011.

[38] Sethi, N. and Sharma D. ; "A New Cryptology Approach for Image Encryption", *2nd International Conference on Parallel, Distributed and Grid Computing*, pp.905-908, 2012.

[39] Ramaiya, M.K., Hemrajani, N. and Saxena, A.K. ; "Security Improvisation in Image Steganography using DES", *3rd International Advance Computing Conference (IACC)*, pp.1094-1099, 2013.

[40] Zhiwei, Z., Ren-er, Y., Shun, T. and Shilei, C. ; "Image Steganography Combined with DES Encryption Pre-processing", *Sixth International Conference on Measuring Technology and Mechatronics Automation, IEEE*, 2014.

[41] Karim, S.M., Rahman, M.S. and Hossain, M.I ; "A new approach for LSB based image steganography using secret key", *Computer and Information Technology (ICCIT)*, pp.286-291,2011 .

[42] Moon, S. K. and Kawitkar, R. S. ; "Data Security using Data Hiding", *International Conference on Computational Intelligence and Multimedia Applications*, Vol.4, pp.247-251, 2007.

[43] Li, C., Xu, W., Meng, L., Liu, B., Wang, Y. and Wu, L. ; " Realization of a LSB Information Hiding algorithm Based on Lifting Wavelet Transform Image", *International Conference on Mechatronic Science, Electric Engineering and Computer*, pp.1015-1018, 2011.

[44] Shejul, A.A. and Kulkarni, U.L. ; "A DWT based Approach for Steganography using Biometric", *International Conference on Data Storage and Data Engineering*, pp.39-43, 2010.