ADAPTIVE METHOD OF DATA HIDING USING EDGE DETECTION

A Dissertation Submitted in Partial Fulfillment of the Requirement for the Award of the Degree of

MASTER OF ENGINEERING

in

Wireless Communication

Submitted By

Harpreet Kaur

Roll no: 801563007

Under Supervision of

Dr. Ajay Kakkar

(Assistant Professor, ECED)

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY, PATIALA, PUNJAB

JULY, 2017

DECLARATION

I, Harpreet Kaur hereby declare that the work presented in this thesis entitled "***Adaptive Method of Data Hiding using Edge Detection***" in partial fulfillment of the requirement for the award of degree of Master of Engineering (Wireless Communication) submitted at Electronics and Communication Engineering Department, Thapar University, Patiala is an authentic record of work carried out under supervision of **Dr. Ajay Kakkar** (Assistant Professor, ECED, Thapar University) from July 2015 to July 2017. The matter presented in this has not been submitted either in part or full to any other university or institute for the award of any other degree.

Date: 24/8/17

Harpreet Kaur
Roll No: 801563007

It is certified that the above statement made by the candidate is correct to the best of my knowledge and belief.

Date: 24/8/17

Dr. Ajay Kakkar
Assistant Professor, ECED

CERTIFICATE

It is certified that the work contained in the thesis titled "***Adaptive Method of Data Hiding using Edge Detection***" being submitted by **Ms. Harpreet Kaur** to the **Department of Electronics and Communication Engineering, Thapar University, Patiala** in the fulfillment of the requirements for the award of the degree of **"Master of Engineering"** has been carried out under my guidance and supervision. The matter presented and the results contained in this thesis have not been submitted in part or full to any other institute or university for the award of any other degree.

Dr. Ajay Kakkar
Assistant Professor,
Department of ECE
Thapar University
Patiala

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to **Dr. Ajay Kakkar**, Assistant Professor, Electronics and Communication Engineering Department, Thapar University, Patiala for his patient guidance and support throughout the thesis. I am truly very fortunate to have the opportunity to work with him. I found this guidance to be extremely valuable. I am also thankful to our Head of Department, **Dr. Alpana Agarwal** and P.G. Coordinator, **Dr. Hem Dutt Joshi**. I would like to thank the entire faculty and staff of Electronics and Communication Engineering Department and then friends who devoted their valuable time and help me in all possible ways towards successful completion of this work. I thank all those who have contributed directly or indirectly to this work.

Lastly, I would like to thanks my parents for their years of unyielding love and encourage they have always wanted the best for me and I admire their determination and sacrifice.

Harpreet Kaur

ME-WC

801563007

ABSTRACT

Data security is of utmost importance for an institution, organization and many government sectors to maintain the confidential information protected from different competitors. It will help to make sure that the security of user's data is maintained. In today's time most of the information is first received, then processed and finally is get saved within the computers and further transmitted across different networks, therefore, it is required to preserve the data in order to maintain confidentiality. The thesis work covers the introduction, need and type of cryptography in data communication. It also deals with the various techniques employed for the data security and the goals and applications of steganography. Difference between steganography and the process of image encryption is also discussed. Then, the various methods or techniques given by different scholars in the realm of cryptography and steganography are discussed in literature review. On the basis of literature survey, observations and the objectives are also drawn. After studying the various techniques of cryptography and keeping in mind the importance of steganography for transmission of secret data, the proposed work incorporates the use of encryption keys, LSB substitution method, edge detection and clustering process for data hiding. Data hiding efficiency among various image formats with different pixel sizes are found with the help of LSB algorithm. To ensure triple security of data process of encryption is combined with steganography. This is done by generating keys from data and then hiding back the encrypted data in the cover image. At last, the outcomes of the proposed data hiding algorithms which are based on detection of edges of the pixels of the image and clustering them in a group are compared. Thus, it has been concluded that the results of proposed algorithms show good value of PSNR as well as an acceptable quality of the stego image which makes it hard to discover any existence of embedded data in the cover image and hence, make it secure for transmission.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

AES	Advance Encryption Standard
BREA	Byte Rotation Encryption Algorithm
CCA2	Adaptive Chosen-Ciphertext Attack
CED	Concurrent Error Detection
CMD	Clustering Modification Direction
COA	Ciphertext-Only Attack
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DWT	Discrete Wavelet Transform
FED	Fuzzy Edge Detection
FHE	Fully Homomrphic Encryption
FRT	Fractional Fourier Transform
FT	Fresenlet Transform
HVS	Human Visual System
IEEE	Institute of Electrical and Electronics Engineers
JPEG	Joint Photographic Experts Group
KPA	Known-Plaintext Attack
LSB	Least Significant Bit
LZW	LempelZiv–Welch
MSE	Mean Square Error
PKE	Public Key Encryption
PVD	Pixel-Value Differencing
PSNR	Peak Signal To Noise Ratio
QT	Quantization Table

RSA	Rivest Shamir Adleman
SA	Simulated Annealing
SHE	Somewhat Homomorphic Encryption
SED	Sobel Edge Detection
SPD	Steganography Pattern Discovery
TDES	Triple Data Encryption Standard
TIF	Tagged Image File Format
UED	Uniform Embedding Distortion
UERD	Uniform Embedding Revisited Distortion

CHAPTER 1
INTRODUCTION

This chapter deals with the role of cryptography in field of information security and describes the various key parameters to keep the data protected from various kinds of attacks. A brief account of image encryption and decryption has been provided. Further, the need, goals and various applications of image steganography have been discussed. Comparison between image encryption and stegenography has also been done.

1.1 CRYPTOGRAPHY

Cryptography is the analysis of scientific algorithms associated with features of data security, for instance, privacy, data trustworthiness, entity validation and data origin verification [1]. Basic cryptographic model is shown in figure 1.1. It composes of the original intelligible message or data before encryption, known as Plaintext. Key is a word or value that is utilized to scramble the plain text or decode the cipher text. Cipher text is the encoded content. The content acquire with the performance of encryption process which is performed with the assistance of a key is said to be cipher text [2]. The process of encryption is used for different replacements and changes on the plaintext. It is a method to hide the information, so that, any unauthorized person will not be able to read it and that can be accessed with the help of a certain key. This process is usually performed at the transmitter end. Decryption is a process of changing the encoded data back into its original form. Decryption is done at the receiver side [2]. Some of the basic stream ciphers used in cryptography are: a) Transposition ciphers and b) Substitution ciphers.

a. TRANSPOSITION CIPHERS

Each letter of the data signal that has to be securely transmitted are disorganized, i.e. written in a certain pattern, and after that it has to be transmitted in some different order from its original form. The letters of the data that will be secretly communicated are mixed, that is, modified in some way, and is then transmitted in an alternate form, from its initial form [4]. For example, transpositions write messages horizontally into rectangular arrays, reading out the transposed text vertically. The recipient reverses the process to recover the original text:

Plaintext: MY-NAME-IS-HARPREET

I-AM-PURSUING-M.E.,

FROM-THAPAR-VARSITY

Ciphertext: MIFY-R-AONMMA-MPTEUH-RAISPSUA-IR HN-AGVR-

APMRR.SEEIE.TT,Y

b. SUBSTITUTION CIPHERS

These ciphers are made by substituting one symbol, for example, a letter of a message, with any other symbol or letter in a designed way. Keep the alphabet side by side with any other alphabet that is dislocated by a small numbers of letters to the right:

A B C D E F G H I J K L M

D E F G H I J K L M N O P

N O P Q R S T U V W X Y Z

Q R S T U V W X Y Z A B C [4]

Using a displacement of three letters to the left, one can obtain the following substitution:

Plaintext: MY NAME IS HARPREET

I AM PURSUING ME FROM THAPAR VARSITY

Ciphertext: JV KXIB FP EXOMOBBQ

F XI MROPRFKD JB QEXOPFQV

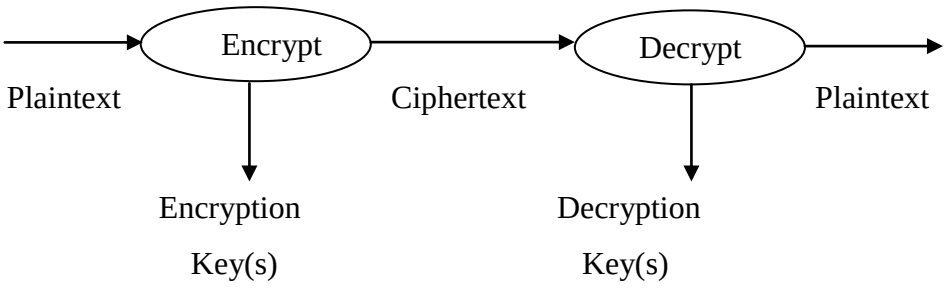


Figure 1.1 Cryptographic Model [1]

1.2 CRYPTOGRAPHIC GOALS

In data and telecommunications, cryptography is vital when we have to convey any information over any un-confided channel, which incorporates any network, especially the web [3]. For a particular application like communication we have a few certain security prerequisites which are given as:

- **Authentication:** The way toward verifying one's personality. The important kinds of host-to-host validation on web nowadays are may be address based or name based but both of them are not so solid [2].
- **Privacy/Secrecy**: This is necessary as it will keep the access of the data to only the authorized users but not everyone. Privacy is similar to the terms confidentiality and secrecy. Apart from physical security there are many methods to provide secrecy [3].
- **Integrity**: Making sure that the message received by the receiver is not in any modified form from the original one [2]. Usually utilized strategies to secure information integrity incorporate hashing the information you get and comparing it with the hash of the initial message.
- **Non-repudiation:** A method assuring against a party denying a data or a communication that was initiated by them. In other words we can say that it is a way to verify that the sender has truly sent the message or not [4].
- **Data Integrity**: It is a job to address the unauthorized change of data. To guarantee information uprightness, one must be able to recognize data control by unauthorized parties. Data manipulation incorporates things, like inclusion, cancellation and substitution [1].

1.3 TYPES OF CRYPTOGRAPHIC SCHEMES

There are two types for cryptography which depends upon the use of keys and are as follows:

a. Private Key Cryptography (Symmetrical): This deploys a single key for both encryption and decryption [3].
b. Public Key Cryptography (Asymmetrical): This employs a single key for encryption and some different key for decryption [3].

a) Symmetric Key Cryptography

In symmetric secret writing there is a same key which is used for performing both secret writing and decoding. This can be conjointly referred to as secret key secret writing as only one key is utilized to code and decode data. It changes plaintext into cipher text by employing a secret key and the key should be best-known to each the sender and the receiver. Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) and Blowfish are the examples of symmetrical key cryptography [3]. AES was adopted as a standard for secret writing by National Institute of

Science and Technology. The major problem with this approach is the distribution of the key.

b) Asymmetric Key Cryptography

Asymmetric encryption is that kind of encryption system where the encryption and decryption are performed using two various keys: one is public key and the other is a private key. Public key is used for encryption process and private key is used for decryption process. This cryptography scheme is also known as public key encryption. RSA is the most commonly used public key cryptosystem [4]. There is no need for distributing them prior to transmission. This form of cryptography provides many benefits like simplify key distribution and durable encryption [3].

1.4 CRITERIA FOR THE SELECTION OF A CRYPTOGRAPHIC ALGORITHM

The security of the cryptographic model can be analyzed on the basis of the encryption algorithm and the key management scheme. For highly secured model one can make use of DES or AES having more number of round functions [5]. The following section describes how to select a particular cryptographic algorithm on the basis of various parameters. The parameters selection is based on a particular application.

i) Level of Security

It is an important parameter in the cryptographic algorithm and is further dependent upon various factors such as (a) CPU time required by a machine for a specific processing speed to create the key, scramble and unscramble the information, (b) the amount of storage needed to carry the information in encryption process, (c) number of client indulged in the model. (d) time needed by the model to recoup the information if there arises an occurrence of key crash and (e) time accessible to an unauthorized person to create different sorts of assaults [6].

ii) Overheads

Cryptography needs consistent endeavors to accomplish security; at first endeavors are needed for the creation of keys. When the keys were produced the subsequent stage is to scramble the information and deliver it via internet [3]. Also, different overheads related to cryptography and are as per the following:

- **Financial overheads:** A considerable measure of money must be contributed to place the documents secured from hackers. The use of multiple key lengths always increases the budget of the model [6].

- **Power Consumption:** The effective processors devour greater power in the key making process subsequently node capacitance, charge sharing and leakage current remains in the design [6].

1.5 THE SIGNIFICANCE OF KEY LENGTH

The larger the key the more it is difficult to crack. It has been observed that to crack a block of encrypted data, the amount of probable key values twice over each time when a distinct bit is summed up to the key length. The large keys offer more protection; as we are aware that with the use of strong computational tools, that computer is easier to assault cipher text by brute force schemes rather than by the hacker [33].

1.6 TYPES OF ATTACKS

Attacks are the actions taken against a target with the intention of doing harm. These are the random threats generated by the hacker.

- **Ciphertext-only attack (COA)**

The COA is a kind of attack in which we presumed that the cryptanalyst has access to the ciphertext, but not to the plaintext. This kind of assault has been most frequently occurred in practical world cryptanalysis, yet is the poor assault and thus owning to the cryptanalyst's deficit of knowledge [33].

- **Known-plaintext attack (KPA)**

This kind of attack is one in which we presumed that decipherer has way in to at list a restricted range of pairs of plaintext and therefore the relative enciphered text. A motivating illustration is the World War II, in which the Allies utilized known-plaintexts in the thriving cryptography of the Enigma machine cipher [27].

- **Adaptive chosen-ciphertext attack (CCA2)**

Hacker will go for a chain of ciphertexts and view the ensuing plaintexts, and there will be chance at each stride to investigate the preceding ciphertext-plaintext pairs and then the next ciphertext is selected [26].

1.7 INTRODUCTION TO IMAGE ENCRYPTION

Information security has become necessary for its proper storage and safe transmission. Information may involve images and when they are shared from one user to another through internet, there is a risk of its hacking by the hackers. As we are aware that everything is becoming wireless; therefore, the security during these data sharing is definitely required [10]. The security of image information from unapproved client is imperative. Image

encryption has a vital function in area of data hiding. Image encryption technique arranges data in such a way no one will be capable to understand it. Consequently, no programmer or unauthorized person, including server user and others, can approach unique message or some other sort of transmitted data through open systems, for example, web [9]. An image contains at least one color channels that characterize the intensity or color at the specific pixel area I (m, n). In a general case, every pixel area contains a solitary numerical value representing the signal level at that point in the image [19-21]. The change from this arrangement of numbers to a genuine image is accomplished using a color map. A color map gives a particular shade of color to each numerical value in the picture to impart a visual portrayal of the information. The most widely recognized color map is the grayscale which allots all shades of gray from black (0) to white (greatest) as per signal level [8]. The process of image encryption and decryption are very important in the field of data security. Further the basic need is felt, when the data has to be transfer from one user to another via a channel or medium such as internet.

Requirements of image encryption and decryption are:

• It helps to attain the pixels of the original picture.

• It makes image secured by strong encryption process and prevention from hacking [7].

• The encryption process should be fast enough, so that, it can be transferred in less time.

• Decryption will allow getting back the original image without any quality decay [9].

(a) Original image (b) Encrypted image (c) Decrypted image

Figure 1.2 Image encryption and decryption

The figure 1.2 shows the process of image encryption and decryption. Figure 1.2 (a) represents the original image which has to be encrypted with the help of a key. The figure 1.2 (b) represents the encrypted image which is obtained after applying encryption algorithm on the original image. It is analyzed that the encrypted image is useless as the picture content is in hidden form [10]. With the help of a suitable key or algorithm the encrypted image can be decrypted which is shown in figure 1.2 (c). This is known as image decryption [36].

1.8 IMPORTANCE OF IMAGE ENCRYPTION

Image encryption technique is useful in mobile and multimedia communication. As we have seen the biometric images of fingerprints have replaced the individual user password codes. So, when images are sent over a channel, there is a chance that a hacker may get access to the information. With the help of encryption, the data to be transfer will become safer [11]. Also using encryption of non-critical images, an unauthorized user will not be able to distinguish between a necessary or non necessary details or data. Image encryption can also be used to maintain confidentiality and privacy. Fields like medical imaging uses the application of image encryption to provide secrecy in the images that they used and worked on. Nowadays, to decrease the price and to enhance the services, the medical reports are being transferred from the laboratories to doctors, offices or to medical centers in electronic forms only [12]. In accordance with medical science rule, medical data or documentation, which may contain multiple pictures, would not be revealed to any unknown fellows. So, it is mandatory to encrypt the medical images before sending them over a network [20].

1.9 IMAGE DECRYPTION

Decryption is the reverse process of encryption. When the receiver obtains the encrypted image, extractions of the numbers from the encrypted image are to be done [13]. This extraction of numbers from image is considered as the highlighting factor of this work. The process of extracting numbers from the encrypted image by methods like using various key algorithms, mathematical transformations or different mapping techniques is known as the image decryption process [16]. Image decryption may be based on cryptographic algorithms such as AES, DES, RSA etc. or it may be performed using different operations such as ORing, Xoring etc. of the encrypted data sequence and the valid key sequence which was used in the process of encryption [18].

1.10 ENCRYPTION V/S STEGANOGRAPHY

Encrypting any data is a popular approach which provides privacy. Encryption technique, deals with changing of data, so that, gatecrashers can't get access of that data [5]. Be that as it may, amid encryption, the secret data is altered, subsequently it is in unclear form and a gatecrasher can effectively associate the nearness with secret data. Steganography is another method for securing mystery data [7-8]. The word steganography is acquired from the Greek words "stegos", signifying "cover", and "grafia", signifying "composing", characterizing it as "secured composition" [60]. Steganography is the art and science of concealing communication; a steganographic framework in this way, hides secret information with the

help of a cover media, so that, a hacker or an unauthorized user may not will feel the presence of the secret data. Steganography is a process of concealing different types of content such as text, image, audio or any video in some other multimedia file like audio, image or video [60]. Steganography can be distinguished by cryptography in the viewpoint that in case of steganography, the key point is that the secret data is covered up and no one can think that there is some implanted information, while in cryptography, anyone can realize that there is a hidden message. It incorporates an immense range of secret communications strategies that hide the message's extremely presence [56-57]. It can be stated that steganography is a workmanship and investigation of imparting in a way which hides the nearness of the correspondence while in cryptography, the unapproved client is permitted to find and change the information but he/she does not have the potential to destroy particular security without having the capacity to damage certain security sites provided by the cryptosystem. The aim of steganography is to shroud data in other cover data in such a way that cannot enable any unauthorized person to seek and differentiate, if there is a presence of any secondary message [23]. Image steganography, is a method in which secret information is inserted inside a picture, as a cover media which is generally examined amid the most recent decades. Content flexibility, visual versatility, small dimension of pictures and furthermore the shortcomings of the human visual system (HVS) make it a great conveyer to transfer confidential information through the web [60].

1.11 HISTORY OF STEGANOGRAPHY

According to a historian Herodotus the technique of steganography was initially used in 440 BC. He gave two examples in which the steganography was exercised. It was when Histiaeus made a notification on his vassal, Aristagoras, by snipping off the head of his most trustworthy worker, "denoting" the notification onto his scalp, then sending him out the door once his hair had regained, with the direction, “When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon." Moreover, Demaratus sent a notice about an expected assault to Greece by composing it specifically on the wooden backing of a wax tablet before using its beeswax surface. Wax tablets were in like manner utilized then as reusable composition surfaces, now and again utilized for shorthand [4].

1.12 KEY ISSUES RELATED TO STEGANOGRAPHY

Picture quality, security against attack and geometric undiscoverabilty are the key issues associated to steganography methods. Steganography process has the above said parameters are the important key points to be considered which will decide the efficiency of the

steganography algorithm [44]. So, for using steganography optimally the following key issues are to be clearly understood:

a. **Imperceptibility:** Steganography framework ought to have high installing limit and ability to bear up against stego assaults. The stego picture ought not to have extreme visual artifacts. More the trustworthiness of the stego picture, the superior would be its image quality [44].
b. **Security against assault:** The steganographic framework may experience the ill effects of various sorts of stego assaults, enabling busybody to recover secret message bits implanted in cover media [48].
c. **Payload limit:** It is characterized regarding quantity of undisclosed bits that can be implanted in each pixel. In a perfect world it ought to be as high as would be prudent while keeping up the satisfactory quality of the stego image. It is otherwise called embedding capacity or concealing limit or hiding ability and is calculated regarding bits per pixel or bits per transform coefficient [44].

So, for using any steganographic technique the above key issues have to be kept in mind. The system should be enough strong, so that, the picture quality and statistical undetectability may be optimized [45]. For this a secured and high capacity steganography system should be designed. We have three distinctive ways to deal with security of design, large limit image steganography framework: (a) Select appropriate cover picture from the database, (b) Choose suitable embedding areas and (c) Utilize encrypted version of secret information hiding. Accordingly, these reasonable methodologies will bring about secure, high limit steganography framework that may crush a few factual assaults [54, 57].

1.13 CLASSIFICATION OF IMAGE STEGANOGRAPHY

The process of image steganography may be divided in spatial domain, transformation domain, spread spectrum and model based steganography. Some other methods such as invisible inks, digital signatures and covert channels may also be exercised [53]. In case of spatial domain, secret information is hidden in pixel value straightforwardly though transformation domain techniques accomplish inserting by initially changing over the image from spatial to frequency space [54]. The spatial to frequency change might be finished with the assistance of any of the changes strategies, for instance, discrete cosine transform (DCT), discrete wavelet transform (DWT), double density double tree DWT (DD DT DWT), ridgelet or curvelet transform, et cetera. At that point embedding is finished utilizing reasonable transform coefficients [60]. Different procedures like soft computing devices can be utilized

to ideally pick the transform coefficients to conceal information in it. As transformation domain strategies are more invulnerable to image processing operations and are less helpless to stego assaults, these are generally favored over spatial domain techniques [62]. Picture restoration and error control methods can be utilized in spread spectrum method, while taking off the information at the decoder end. It is a visually impaired technique as the initial picture is not necessary amid extraction [50, 51]. This plan outflanks others as far as payload limit and imperceptibility. It is otherwise called statistics aware embedding. Prior to choosing the areas for information embedding in a cover picture, geometric global elements of the picture are considered. Further, the genuine information embedding procedure is done as required [56]. Therefore, it gives an extra layer of security to steganography.

Additionally, two primary ways for attaining embedding in spatial space are classified as Least-Significant-Bits (LSB) substitution, and Pixel-Value-Differencing (PVD). LSB substitution is the most normally utilized strategy specifically substituting the LSBs of pixels in the cover picture with secret bits to get the stego picture. PVD technique gives great imperceptibility by figuring variation of two sequential pixels to choose the deepness of the hidden bits [28, 42]. In the presented method, we have used LSB method of data hiding.

1.14 GOAL OF STEGANOGRAPHY

Information exchange in the just about any cluster of computer has to be more secure in the era of cloud computing and big data. Steganography helps to prevent illegal attention through covering the secret message in a number of digitally electronically representative media, without hurting the accessibility of secret message [38-40]. Image steganography methods are recently been helpful to send any secret message in the protected image carrier to prevent threats and attacks whereas it does not give any kind of opportunity to hackers to find out the secret concept. Inside a steganographic system secrets information is embedded inside of a cover file, to ensure that no one will suspect that anything perhaps there is inside carrier. The cover file could be image, audio or video. To really make it safer, the secret information might be encrypted embedded then, it will be decrypted at the receiver [41, 43].

1.15 APPLICATIONS OF STEGANOGRAPHY

Steganography has various applications in different areas of science and technology. Some of the main areas of applications are given as:

a. Use in present day printers

A few present day PC printers utilize steganography, for example HP and Xerox company's color laser printers. The printers put on small yellow spots to every page. These visible spots comprise encoded printer serial numbers, time stamps and date [3].

b. Example from present day rehearse

The bigger the cover message with respect to the shrouded message, the less difficult it is to conceal the last mentioned. Consequently, computerized pictures are utilized to conceal messages on the Internet and on other correspondence media. Expressed fairly more formally, the target for making steganographic encoding hard to identify is to guarantee that the progressions to the bearer because of the infusion of the payload are outwardly insignificant; that is to state, the progressions are unclear from the noise floor of the transporter. Also the use of technology is to embed maximum data in minimum number of pixels of the image. Presently, many medical science centers use steganography for hiding the records in cover images [3].

c. Digital Watermarking

Digital water marking is the most important application of steganography. This is the process of replicating a picture, symbol, or content on paper stock, such that, the origin of the archive may be in some event mostly confirmed. An advanced watermark can finish a similar capability; a visual craftsman, for illustration, X upload test pictures on her website and finish with an embedded initials so that she could shortly exhibit her proprietorship on the off chance that others endeavor to represent her work as their own [3].

d. Alleged use by knowledge administrations

During 2010, the Russian foreign intelligence service was charged for using modified steganography software for embedding encoded instant messages in picture files for communicating something with "unlawful operators" which were located abroad [3].

e. Distributed steganography

Some certain dispersed steganography strategies, including schemes that disseminate the payload using various transporter documents in different areas to cause discovery more troublesome [3].

1.16 ORGANIZATION

In the beginning of the thesis the basics, goals and use of cryptography along with the importance of steganography have been discussed. Further, the approaches which have been used by various researchers in the field of cryptography and steganography are studied. After

that, the presented technique which is based on the limitation of the existing techniques has been designed. The outlines and the main content of each chapter are briefly given as following:

- Chapter1 briefly discussed the introduction of cryptography, image encryption/decryption, various attacks, encryption algorithms and differences between encryption and steganography.
- In Chapter 2, literature review has been done; which consists the work carried out by the different research scholars in the area of cryptography and steganography. From the literature review, few observations have been drawn, and gaps and problem formulation have also been stated. It also involves the objectives drawn out from the literature reviews.
- In Chapter 3 the various proposed algorithms for different applications are discussed. The various parameters and the description of the algorithm have been given.
- Chapter 4 deals with the simulation results of the proposed scheme. Different comparison factors are used for the discussion of the obtained results.
- Finally, in Chapter 5 the conclusion and the recommendations of the proposed work have been given.

CHAPTER 2
LITERATURE REVIEW

This chapter deals with the work carried out by the different research scholars in the domain of cryptography and steganography in information security. From the literature reviews many interpretations have been drawn. Problem formulation and objectives have also been drawn from these observations and enlisted in the end.

2.1 LITERATURE SURVEY

Maniccam SS *et al.* [5] presented a new method which could perform both lossless compression as well as the encryption of both binary as well as gray-scale pictures. Both processes of compression and encryption are grounded on SCAN patterns which are created by the SCAN methodology. The authors also gave basic idea about SCAN, compression and decompression methods, encryption and decryption procedures, and examine the outputs of the methodology.

Chang CC *et al.* [6] presented a technique to break the scheme that was proposed by Chung and Chang few years back and was about a method to encrypt binary images with few pairs of plain image and cipher image. When compared to other researchers, their method could actually obtain better compression ratio by placing various scan patterns at the identical level in the scan tree structure and exploiting the two-dimensional run-encoding method. However, their scheme seems to be quite vulnerable to attacks, if it utilizes similar key to encrypt various images.

Wu DC *et al.* [7] presented a novel technique for embedding confidential information into a gray-scale cover image. Firstly, a secret message and a cover image were divided into non-overlapping blocks of two consecutive pixels during the process of embedding. At that point the distinction value is computed from the estimations of the two pixels in each block. The quantity of bits which could be hidden in a pixel pair is chosen by the width of the range that the distinction value has a place with. This strategy gives a simple approach to deliver a more indistinguishable outcome than those yielded by basic least-significant-bit substitution techniques.

Chang CC *et al.* [8] proposed a technique which could give more hiding capability and to reduce the deformation of the stego-image, by using a steganographic scheme which was

done by side information. This technique used the connection between neighborhood pixels to discover the level of effortlessness or contrast of pixels. On the off chance that the pixel was available in edge territory, then it could insert more changes as contrast with smooth zones. The two-sided, three-sided, and four-sided side match plans are utilized as a part of this work. The simulation outcomes demonstrate that the strategy gives a huge embedding limit without making detectable distortion.

Munoz-Rodriguez JA *et al.* [9] framed a scheme based on optical operations for image encryption and decryption and verified simulation experimentally. This technique would take an image as input and is encrypted by a fringe pattern. The output of the encryption process was a fringe pattern deformed in accordance with the reflectance map of image. The decryption process is performed with the help of moire fringe pattern. For retrieval of the envelope of the final image, a low pass filter is applied on the moire pattern.

Shin CM *et al.* [10] presented an encryption technique which was based on phase wrapping scheme and modified exclusive-XOR algorithm. Then, the combination of XORed images and the bipolar random images was taken and then it is transformed to full phase images, which is known as encrypted image and a key image, by a phase-wrapping method and phase-encoding technique. The decryption process was performed using a simple phase-visualization system.

Lukac R *et al.* [11] put forward a new secret sharing technique which could secure the content of image by coding it by β bits per pixel. The presented input-agnostic encryption scheme constructs β-bit shares by incorporating bit-level breakdown or assembling with a {ƙ, η}-threshold sharing strategy. The reassembling was done with the help of decryption process using easy consistent operations in the decomposed bit-levels without using any post processing operations. This research work provided a cost effective cryptographic image processing of β-bit images via web.

Wang RZ *et al.* [12] proposed a new image steganography technique which deploys a two-way block-matching approach to probe for the utmost similar block for each block of the important image. A hop scheme was used to record bases and indexes which were acquired jointly with few not well matched blocks in least significant bits of the cover image. A high data payload, that would minimize the memory and transmission-time necessities, was

utilized in this method. Furthermore, it gave a strategy which could stop a user from selectively obstructing the transmission of the imperative image.

Mao Y *et al.* [13] discussed the significance and utility of utilizing a joint signal processing and cryptographic way to deal with media encryption, keeping in mind the end goal to address the access control problems unique to multimedia applications. The frameworks thought of two atomic encryption processes that could keep up regular consistence and were well disposed to delegate processing. Quantitative testing for these operations was done to uncover that a good trade off could be made amongst security and bit rate overhead.

Wang CM *et al.* [14] presented a novel image steganographic scheme that was able to produce a secret-embedded image and the obtained image was fully indistinct by the original image by the human eye. Furthermore, this novel scheme prevented the falling-off-boundary issue as it incorporates both modulus function as well as the pixel-value differencing. In presented method, a revised procedure to revamp the remainder was used which could minimize the image distortion created due to concealing of secret message. The estimations of the two back to back pixels were barely modified after the way toward embedding of the secret data by the presented optimal alteration algorithm was carried out. Experimental outcomes indicated that the presented technique was secure against the RS detection assault.

Kekre HB *et al.* [15] presented a novel modified form of Least Significant Bit (LSB) technique. This work proposed a viewpoint which was easy to implement as compare to Pixel value Differencing (PVD) scheme and thus attained a large embedding limit and imperceptibility. The presented scheme could also be applied on twenty four bit color images, therefore, it could attain embedding limit much greater than PVD.

Joshi M *et al.* [16] proposed a technique for encoding of twin color images deploying fractional Fourier transform (FRT). Firstly, the colored pictures which were to be encoded were transformed into the indexed image formats earlier than they were fed to twin image encryption scheme grounded on the concept of FRT. This scheme utilized one arbitrary code in the image domain and one arbitrary phase code in the FRT domain to accomplish twice image encryption. Various fractional orders, arbitrary masks in image and FRT domain were the solutions to intensify the safety of the presented technique.

Zhang Z *et al.* [17] presented a novel two-description image coding algorithm using steganography, making every portrayal by concealing the coarsely coded part into the finely coded in view of least-significant bit (LSB) steganographic method. In this way, the bit budget for the coarsely coded part in each portrayal could be held with little remaking of decay for the finely coded part in case the hiding procedure was appropriately modeled. The experimental outputs validate the benefit of the presented strategy.

Liu Z *et al.* [18] proposed a new image encryption method derived from the commutation and anti-commutation protocols. Enciphering of a picture into two different pictures by superposing its two one-dimensional sections Fourier transforms or fractional Fourier transforms in horizontal and vertical directions. The picture obtained with commutation rule was known as the encrypted image while the image obtained with anti-commutation rule was known as decryption key. To execute the presented algorithm an optical setup was also modeled.

Singh M *et al.* [19] discussed picture encryption by blending pictures with different matrices formed using letters or numbers and then positioned in the input plane of a double random phase encoding (DRPE) scheme. Addition or multiplication of different such matrices with an input picture gives a changed picture pattern that was encoded in a DRPE scheme using the 4-f geometry. Simulation results showed the reliability of the scheme as the MSE between the decrypted and original image was very less.

Liu Z *et al.* [20] presented a triple image encryption technique employing fractional Fourier transform in it. In this technique, the original image was encoded in amplitude section and left two images were encoded in phase information. The difference between the last image and the outcome phase of transform gave the formula for encryption. In presented method, normally random phase encoding technology was not needed. If the picture is decoded with the help of right keys, mostly all the information of the picture was retained.

Yang H *et al.* [21] presented a fast image encryption and validation strategy. A 128 bit hash value with help of plain image and the secret hash keys was created after initiating a keyed hash function. The purpose of key for encryption and decryption was served by the hash value and the verification of decrypted image was done with the assistance of secret hash keys. The speed capability was thus revamped.

Luo W *et al.* [22] did expansion of the LSB matching revisited image steganography along with proposed adaptive edge technique that would choose the embedding areas in accordance to the size of undisclosed information and the deviation between two continuous pixels in the cover image. For lesser embedding rates, only sharper edge areas were used and smoother areas were kept same. The simulation outputs were analyzed on 6000 natural images with three particular and four universal steganalytic methods exhibit that this novel algorithm could improve the reliability distinctly in comparison with typical LSB-based techniques. Thus, their edge adaptive ones, such as pixel-value-differencing-based algorithms while visual quality of stego images were well maintained.

Lin GS *et al.* [23] presented a new closed-loop computing work which iteratively explores actual moderations of coefficients to increase a base steganographic technique accompanied by high superiority of image and improved anti-steganalysis capacity. For attaining desired aim, an anti-steganalysis tester and an embedding controller-depend on the simulated annealing (SA) method accompanied by a perfect cost function-were used into the processing loop to run the convergence of probes. Simulation outputs display that the base techniques could be increased with better exhibitions in image PSNR, file-size differentiation, and anti-steganalysis pass-rate.

Guo JM *et al.* [24] showed that the quality factor in a JPEG image be an embedding space, and furthermore talked about the capability of inserting a message to a JPEG picture by altering JPEG quantization tables. In collaboration with a few permutation schemes, the presented algorithm was utilized as a mechanism for secure information exchange. This technique might have attained adequate decoded outputs accompanied by the easy JPEG double compression approach.

Zhang J *et al.* [25] presented a logical steganalyzer that uses the key point that the noise residuals in the DCT domain were either concentrated on zero or very sensitive to LSB matching. Simulation outcomes exhibits case of almost ideality at embedding rate 0.5 bpp and also with a correctness of 90.9% at 0.1 bpp while a precision of 44.6% using WAM steganalyzer. Nevertheless, this presented detector serves only since the accurate JPEG decompressor was investigated.

Wang X *et al.* [26] offered a new image encryption technique based on a skew tent map. Some faults of the proposed technique were found out and then a chosen plaintext attack

against it was suggested. Simulation outputs showed that the plain image could be retrieved as it was from the cipher image not having the use of secret key. Thus, it has been viewed that this method was not much safe to be implemented in network communication.

Wua CC *et al.* [27] presented a new secret image sharing algorithm by implementing optimal pixel adjustment procedure for improving the picture standard under various payload capacity and different validation bits constraints. Simulation outcomes exhibited that the presented technique enhanced the picture standard of stego pictures by a good percentage in comparison to techniques lately presented by Yang *et al.* [38], Chang *et al.* [8], and Lin and Tsai [23]. This scheme preserves the secret image sharing and validation capability and also improves the image quality.

Liao X *et al.* [28] worked to enhance the hiding limit while yielding an undetectable optical standard, and proposed a new steganographic technique which depends on four-pixel differencing and modified least significant bit substitution. The mean difference value of a four-pixel block was used to categorize the block as a smooth region or an edge region. Confidential information was embedded into every pixel using k-bit modified LSB substitution algorithm, here value of ƙ could be determined by the extent where the mean difference value jumps into. By showing how readapting approach serves, a hypothetical confirmation was provided for verification of this technique which got success both in process of embedding as well as retrieving of data.

Hou CL *et al.* [29] worked on a significant problem in steganography which was to reduce distortion between the cover and stego image. Due to ease of the tree based parity check technique, it was used to embed a secret data in the cover picture. The tree-based parity check technique was an well-organized method for embedding a message on image data because of its effortlessness. On the basis of this method, a majority vote scheme which gives minimized distortion for locating a stego object was proposed. The lesser hiding capability of the proposed technique make it more optimum as compare to the previous works when the embedded message length was comparatively high.

Roy S *et al.* [30] proposed and advanced steganography scheme for concealing text messages inside RGB images. The motive of the research was to enhance the protection level and to get better the storage capability whereas incurring nominal degradation of the picture. The safety level is improved by distributing the message over the complete picture in its place of

clustering inside definite picture portions, as also by including a password verification method to make sure that the message can be retrieved only by the projected receiver. Simulation outcomes which are done for analyzing the storage capacity and quality degradation, establish the superiority of the proposed approach.

Satir E *et al.* [31] talked about limit and privacy problems of content steganography and to revamp it a new another strategy was presented. Lempel–Ziv–Welch (LZW) data compression technique was chosen because of its rehashed utilization in the writing and noteworthy compression proportion. Secret message was embedded in the chosen content from the already made content base that comprises of naturally produced writings. Simulation outcomes display that the proposed conspire gave a great addition as far as embedding capacity was concerned.

Kakkar A *et al.* [32] worked on a novel technique which could create keys from the given message. Different times, for example encryption, decryption, key setup, processing, and key shifting times, were calculated and analyzed. The time taken to exchange the error key or the key with flaws with new/fresh keys was very less, in the presented model. The security also enhanced, if the key size was extended and the key shifting time was minimized; the given combination was used for secure transmission. This work could be further expanded, if more number of S-Boxes would be used for the similar task, and the key length would be minimized with normal processing time.

Ma K *et al.* [33] presented new concurrent error detection (CED) method to tackle fault-based attack against RSA which was done by deploying its multiplicative homomorphism characteristic. The presented CED method requires continuous messages for sharing the key, so that, it could attain better performance. The CED technique provides various other benefits, such as solid defiance for fault assaults and less time overhead.

Bhati S *et al.* [34] presented novel encryption algorithm “Byte Rotation Encryption Algorithm (BREA)” which also includes “Parallel Encryption Model” this improved both privacy and time of the encryption technique. The BREA works on different pieces of plaintext and complete in parallel way utilizing multithreading thought of single processor improves the speed of encryption system. This proposed framework disregarding the front end could be used in any system applications for system security.

Pareek NK *et al.* [35] presented an encryption scheme which was valid on the grayscale pictures utilizing a confidential key of size 128-bits. Right off the bat, visual nature of picture was rotted by the blending procedure. Acquired picture was isolated into key ward dynamic pieces and after that these blocks/pieces were gone through key based diffusion and substitution procedures. Introduced plan was anything but difficult to execute and has enhanced encryption rate.

Pakshwar R *et al.* [36] focused on the various types of image encryption and decryption schemes and basically a investigation on already existing various picture encryption and decryption algorithms was done. This work also focused on the functionality of picture encryption and decryption schemes.

Juneja M *et al.* [37] reviewed different steganography schemes LSB substitution, LSB matching, Adaptive LSB and Pixel-Value Differencing (PVD), Edge detection filter based, Pixel Indicator methods, component based LSB and texture based algorithms. This survey infers that the requirement of improved steganography scheme for color pictures all imperceptibility, robustness and capacity were considered to be equal parameters for meeting the required criteria.

Yang C *et al.* [38] presented a pixel group trace design. Based on the design as well as on few geometrical features of imagery, the authors presented two novel quantitative methods for steganalysis. The presented methods were designed for two particular MLSB steganography paradigms. Simulation of MLSB hiding using exclusive or operation was performed using the pixel group trace model. It also traces the transition connection between the feasible structures of the pixel group's value by several trace pixel group subsets. After that approximation equations of embedding proportion were acquired from the transition probability matrix amongst trace subsets and the regularity of standard and singular pixel group sets. At last, the sequence of simulation outcomes particularly for triple pixel group exhibit that the presented steganalysis schemes could evaluate less embedding ratio with lesser inaccuracy, specially, for certain cases, the interquartile extent for errors of approximation was lesser than the best one of the variants by greater than 45%.

Chakraborty S *et al.* [39] proposed a safe and undisclosed picture sharing technique, which carries least computational intricacy. The presented technique was a substitution in case of encryption, and it diversifies the data which was to be hidden into various matrices. The

hidden data is entrenched into cover picture with the help of bit by bit EX-OR process. The payload was a basically a form of grayscale representation which was further categorized into three matrices namely sign matrix, error matrix, and frequency matrix. Down scaling of frequency matrix was made by means of a mapping procedure resulting in the construction of a matrix named Down Scaled Frequency (DSF) matrix. These three matrices are embedded in a variety of cover imagery with the application of bit by bit EX-OR procedure among the cover imagery and their individual bit planes obtained from these matrices. Examination of the presented technique confirmed the usefulness of the presented method in hiding the payload even with least computational complexity.

Tang M *et al.* [40] presented a large capacity steganography deploying multilayer embedding (CRS), which could improve the operation of information embedding system. The simulation outcomes presented that the designed CRS technique has more desirable output as compare to the others. Additionally, the presented CRS scheme presents the benefits of high standard picture and less complcation while computation.

Sarreshtedari S *et al.* [41] presented a novel scheme for the least significant bit (LSB) imagery steganography in spatial domain provided the ability of one bit per pixel. In comparison to the lately introduced picture steganography methods, this novel technique known as one third LSB embedding decreases the possibility of converting per pixel to one-third without leaving any effect on the embedding capacity. Another benefit of the presented scheme was to nullify maximally, if there were any changes in the histogram of the image. It was observed t/hat 33% likelihood embedding performs better than histogram compensating version of the LSB matching in terms of maintaining the image histogram unaltered.

Kekre HB *et al.* [42] introduced a new hybrid scheme to secure digital images. The presented framework was a mixing of information embedding and image encryption. For information embedding, four different methods of Multiple LSB's schemes were exploited and evaluated. A number of parameters were also used to estimate the proposed framework. Experimental results show a fine performance in terms of PSNR.

Kanan HR *et al.* [43] proposed an adjustable visual picture superiority as well as information lossless practice in spatial domain which depends on a genetic algorithm (GA). The basic key point of the presented scheme was designing the steganography difficulty as a exploration and optimization task. Simulation outputs, as compare to other recently well known

steganography methods, show that the introduced technique which could attain high hiding capacity in addition to this also improves the PSNR of the stego image.

Subhedar MS *et al.* [44] discussed about only picture steganography. The work in the paper provides an analysis of basic concepts, estimation procedures and safety points of steganography scheme, different spatial and transform domain hiding techniques. Additionally, picture superiority metrics which were utilized for analyzing stego pictures and cover choice procedures which offer an added security to hiding method were also underlined. Prevailing study trends and guidelines to revamp the prevailing techniques were advised.

Agrawal V *et al.* [45] discussed the way of execution of processes like encryption and decryption, if one could use symmetric key and public key cryptography with the help of Advance Encryption Standard (AES) and Data Encryption Standard (DES) algorithms and modified Rivest Shamir Adleman (RSA) algorithm. Using this technique both color and black and white picture of every size saved in TIF was encoded and decoded with the help of blowfish algorithm. Modified RSA Encryption Algorithm (MREA) algorithm was utilized to encode files as well as transfer encoded documents to further ending where it was decoded. Important characteristic of the presented algorithm was that it fulfills the properties of confusion and diffusion in addition to this the ultimate estimate of encryption key makes decryption process unfeasible.

Cheon JH *et al.* [46] introduced a hybrid technique on homomorphic encryption which integrates public-key encryption (PKE) with somewhat homomorphic key (SHE) in order to optimize the storage needs of most somewhat or fully homomorphic encryption (FHE) applications**.** In this design, messages were encoded by a PKE and calculations on encoded information were done with SHE or FHE subsequent to homomorphic decryption.

Zhang Y *et al.* [47] proposed a novel image encoding technique for instantaneous encryption plus compression importance, and which depends on random convolution along with random subsampling. The presented technique, process one image and attains a strong restoration. This presented technique through the structural design of double random masks was somewhat identical to double random phase encoding.

Ahani S *et al.* [48] discussed the role of sparse representation which could safely conceal any information inside non-overlapping blocks of a specific color picture in the wavelet domain. A new improved was introduced by which the bit error rate of embedded data extraction was decreased to nil. The simulation outputs showed that the hidden facts were indistinguishable perceptually. The value of average PSNR of the proposed scheme was nearly 40 and 11 dB greater than the mean values of PSNR the MPSteg-colour technique as well as the wavelet domain 2-LSB embedding technique, correspondingly.

Sun Y *et al.* [49] presented a new compression-encryption technique using a fractal dictionary and Julia set algorithms. In the presented method, for compression purpose, fractal dictionary encoding reduced the time usage and also a good quality of image for reconstruction was obtained. The process of encryption in the method, the key had high key space and large sensitivity, even to small perturbation. Also, the stream cipher encryption and the diffusion process used in the given work help spread perturbation in the plaintext, attaining better plain sensitivity and also gave an efficient resistance to chosen-plaintext attacks.

Feng B *et al.* [50] presented a binary picture steganographic technique which focused for improving the embedding deformation on the texture. Initially extraction of the complement, rotation, and mirroring-invariant local texture patterns (crmiLTPs) is done from the binary picture. The weighted summation of crmiLTP was changed if flipping one pixel is then engaged to calculate the flipping deformation subsequent to that pixel. The steganographic technique creates the cover vector by separating the scrambled image into super pixels. After then, the syndrome-trellis code was generated to reduce the intended embedding distortion. Simulation outcomes had shown that this steganographic method attains geometric protection without corrupting the picture superiority or the embedding capability.

Maheswari SU *et al.* [51] proposed a frequency domain steganography based data embedding scheme deploying Fresnelet transform (FT). By using the technique, the QR coded secret message was hidden using Fresnelet coefficients of the Least Significant Bit (LSB) which was performed at high frequency subbands. The proposed technique provides a high PSNR value which was around 45 dB in addition to this an embedding capability of 352,332 bits was also achieved. The obtained outputs authenticate the realistic viability of the introduced technique for safety employments.

Farhat F *et al.* [52] investigated steganalysis of least significant bit (LSB) hidden pictures in spatial domain as well as most familiar LSB steganography techniques were revealed to be visible. The presented technique was implemented to the image in spatial domain using image clouding; relative auto-decorrelation features extraction and quadratic rate evaluation were the major steps of the introduced investigation approach. The researchers also presented and used novel geometric characteristics, Clouds-Min-Sum as well as Local- Entropies-Sum, both had enhanced the revealing precision along with the hiding rate evaluation. Their experimental results demonstrated that the presented method surpasses some popular, strong LSB steganalysis methods, in terms of true and false detection rates and mean squared error.

Guo L *et al.* [53] refined the homogeneous hiding by considering the respective changes of geometrical design for digital pictures, focusing to create the embedding reconstruction to be relative to the coefficient of deviation. The effectiveness of the presented technique was confirmed with the proof acquired from the exhaustive experiments by means of a well-known steganalyzer by rich models on the BOSSbase catalog. The presented Uniform Embedding Revisited Distortion (UERD) obtains a considerable performance enhancement in field of safe hiding capability in comparison to the original Uniform Embedding Distortion (UED), and rivals the existing state of the art with a decreased calculations difficulty.

Li B *et al.* [54] displayed a technique which could utilize the interactions among inserting changes with a specific end goal to diminish the possibility of location by steganalysis. It utilizes another plan, named as clustering modification directions (CMDs), which depends on the supposition that while implanting alterations in greatly finished areas were locally making a beeline for a similar heading, the steganographic safety was revamped. To actualize the technique, a cover picture was decomposed into a few subimages, and in these subimages portions of secret data were inserted through easily understood techniques utilizing additive distortion functions. Exploratory outcomes demonstrate that the presented CMD technique, joined into existing steganographic plans, could successfully conquer the difficulties that were faced by the current steganalyzers with high-dimensional elements.

Wu J *et al*. [55] proposed an optical multiple image encryption plot in view of computational ghost imaging by means of the position multiplexing. During encryption procedure, every plain picture was encoded into an intensity vector by utilizing the complicational ghost imaging with an alternate diffraction space. The concluding cipher content was produced by superimposing all the intensity vectors collectively. Experimental outcomes demonstrated the

authenticity as well as safety of the presented multiple-image encryption technique. The multiplexing limit of the planned strategy was additionally examined.

Shihua ZS *et al.* [56] presented another secret key generation scheme in light of some functions on the DC as well as AC values in YUV (color representation) space. Using discrete cosine transformation which was performed on the data after image color space change the above discussed two values are taken. A color image in YUV and RGB space using multi-chaotic maps could be scrambled using combination of new secret key and the given secret key jointly.

Jain M *et al.* [57] reviewed some digital image steganographic techniques depending on LSB (least significant bit) and LSB array concept. This paper covers and gives importance to the discussion on the major methods, techniques and algorithm of digital image steganography determined by LSB and LSB array which was used particularly in image domain.

Sedighi V *et al.* [58] discussed an option approach in light of a locally assessed multivariate Gaussian cover image design which was adequately easy to infer a closed-form phrase for the authority of nearly all capable indicator of content-adaptive least significant bit coordinating but, in the meantime, sufficiently complex to catch the non-stationary feature of natural images. Specifically, the authors believed that a new detect ability restricted correspondent as well as gauge the protected payload of every image.

Sajedi H [59] proposed a procedure for steganography Pattern Discovery (SPD) to have high recognition precision. The proposed technique utilizes a evolutionary strategy to take out the signature of stego pictures against clean pictures by using fuzzy if–then rules. In view of the found information, suitable prepared models for steganalysis were utilized and stego images would be distinguished with high precision. The outcomes show that the example of a steganography strategy was extracted well and the kind of steganography technique used to make a stego image could be anticipated with high exactness.

Dadgostar H *et al.* [60] proposed a steganography technique by utilization of interval valued intuitionistic fuzzy edge identifying strategy and in addition the modified LSB substitution strategy which makes it possible to standardize the picture quality and also to enhance the capacity. This proposed technique gave satisfactory equilibrium among embedding limit as well as nature of the stego picture.

Mahato S [61] *et al.* proposed a new scheme to hide secret information in the game, "Minesweeper". This method generated a minesweeper grid that was visually impossible to differentiate by humans from other minesweeper games which are presently there online. The game has a number of properties, utilizing which, steganography could be performed. Here, the authors had utilized position of mines which are in the minesweeper grid to conceal the covert data. The process of concealment begins with the player's first click on the minesweeper grid. The geometric analysis of various properties also shows similarity of the proposed game to other online and offline minesweeper games. The game simulator was given with embedded message within it.

Malik A *et al.* [62] considered the capacity and security issues of text steganography by employing LZW compression technique and color coding based approach. The proposed technique used the advance dispatch policy for concealing the confidential information. This algorithm first compresses secret data and then concealed the compressed confidential information into the electronic mail addresses and also in the cover message of the email. Experimental outputs demonstrate that the presented strategy creates a large embedding limit as well as lessens computational complexity. In addition, the security of the presented technique was fundamentally enhanced by utilizing stego keys.

2.2 OBSERVATIONS

From the literature survey carried out in above section, few observations have been drawn which are as follows:

- Most ciphers can be easily broken with enough computational effort by brute force attack. A single key with variable length provides more secure communication than the fixed one. Also a key with shorter length has high chances of getting hacked easily but it is simpler and faster, on the other hand key with larger length is highly secured but it has high complexity.
- Some proposed algorithms in the above section have a major flaw of file size limit i.e. some proposed algorithms are valid for a file or image of some specific size or a defined range. Some proposed methods are providing a highly secured data transmission but the time consumed for the encryption/decryption process is very large, therefore, they are not useful in real time applications. So, these are the basic key points that have been observed.

- It also has been observed that embedding secret data in an image deteriorates the image quality and embedding capacity is also less.
- It has been analyzed that the edge areas of an image can bear more number of secret message bits as compare to smooth areas, as edge pixels are considered as noisy pixels as their intensities are either greater or lesser than their adjacent pixels because of sudden change in the coefficient gradient.
- To retrieve the secret data at receiver side, it is to be noted that during steganography process i.e. the edges of the cover image and the stego image should not change before or after embedding data.

2.3 GAPS AND PROBLEM FORMULATION

Based upon the above observations, it has been observed that there is a need to optimize the encryption system which takes less time to encrypt the data and provides high security. Also it is intended to optimize the available cryptographic algorithm, so, as to obtain high quality stego image. Sometimes the data to be transmitted is very large; therefore, it is also required to enhance the embedding power of the stego imagery by using some optimized methods or techniques. As it is required to obtain an image with high embedding capacity and less distortion. Therefore, comparison of various image formats with different pixel sizes is also has to be done. To minimize the processing time which depends on various factors such as the hardware used, software used, algorithm used, number of edge and smooth pixels in cover image, data length which has to be embedded, so these key points have to be carefully selected. Also, to improve the safety of the information which is to be transmitted an optimized method should be used.

2.4 OBJECTIVES

The main motive of finding the gaps and formulating the problem is to draw the objectives that are required for the improvement of the existing work. So, from the previous section, objectives have been drawn and are as follows:

- To study various types of encryption algorithms.
- To get high security using cryptography and steganography.
- To get better embedding capacity and provide an acceptable quality of image.
- To compare the embedding capacity of different image formats using steganography.
- To perk up the security of the secret information.
- To use an optimized edge detection method for large amount of data embedding.

CHAPTER 3
ANALYSIS OF LSB ALGORITHM AND EDGE DETECTION TECHNIQUES

In this chapter the proposed algorithm has been discussed. Firstly the data hiding is performed using the three bits of each pixel of cover image by using LSB method. With this various image formats hiding capacity has been obtained. Further, to enhance the security or prevent the access of the data from hackers, triple security method has also been proposed. Finally, an adaptive edge detection method for an optimized data hiding has also been proposed.

3.1 DATA EMBEDDING AND EXTRACTING ALGORITHM USING LSB

Steganography is the process of hiding any information that may be in the form of text, image, video, audio; a steganographic system thus hides secret data in unremarkable cover media so as not to attract a hacker's attention. The proposed method has been divided into two sections: a) Embedding Algorithm, and b) Extracting Algorithm.

a) Embedding Algorithm

In this, a cover image has been taken which is used to hide the data. The data which has to be hidden is known as payload. The secret information which we need to conceal is considered in the form of bits. Here, number of secret data bits depends upon the pixel size of the cover image. The flow chart of embedding algorithm has been shown in figure 3.1. The flow chart comprises of the cover image in which the data has to be embedded and the secret data. For better analysis, cover images with three different pixel sizes which are 256×256, 512×512 and 1024×1024, with three different image formats which are JPG, PNG and BMP have been considered.

In this way, we have nine cover images which are shown in table 1(a) to (i). The color images are firstly converted into gray scale images of the same size i.e. 256×256, 512×512 and 1024×1024. The LSB substitution method has been used in this scheme [60]. The three LSB's of each pixel of the grayscale cover image are replaced with zero, the image thus formed is known as the modified image. Further, to construct the stego image the zeros in the modified image are replaced by the data bits which has to be embedded. Each pixel would contain three bits of the data. This is known as the embedding procedure.

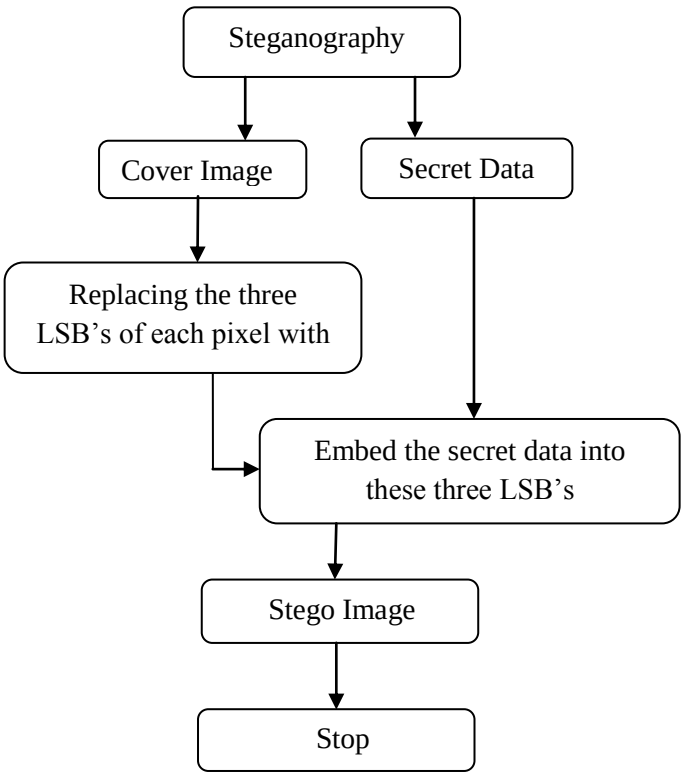


Figure 3.1 Embedding Algorithm

b) Extracting Algorithm

The extracting of the original data is the process of obtaining back the secret message from the output of embedding algorithm i.e. the stego image. The flow chart for the extracting algorithm is shown in figure 3.2.

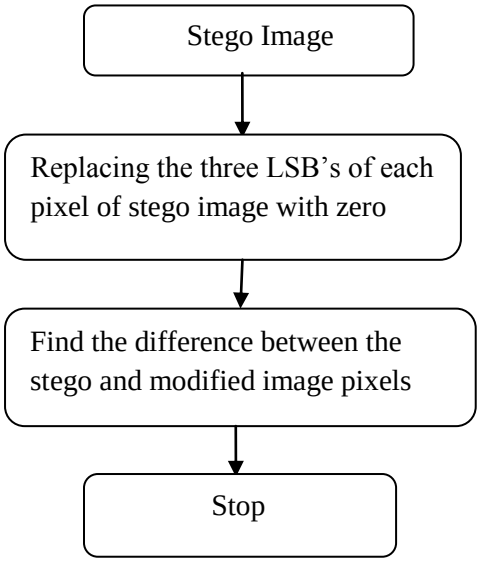


Figure 3.2 Extracting Algorithm

The input in the extracting algorithm is the stego image which is achieved after the embedding process. The extraction algorithm comprises of three steps. It is analogous to the embedding process where three LSBs of the stego image are set to zero to obtain the modified image. Then, the difference between the stego image and the modified image gives the embedded payload. The LSB of every pixel is traversed to extract the embedded data. In this way, extraction of the embedded data is done and the data is successfully achieved.

3.2 ALGORITHM BASED ON CRYPTOGRAPHY AND STEGANOGRAPHY

For enhanced security of data triple protection has been applied on the secret message which is based on two processes which are encryption using keys and image steganography. The algorithm for the same has been shown in figure 3.3.

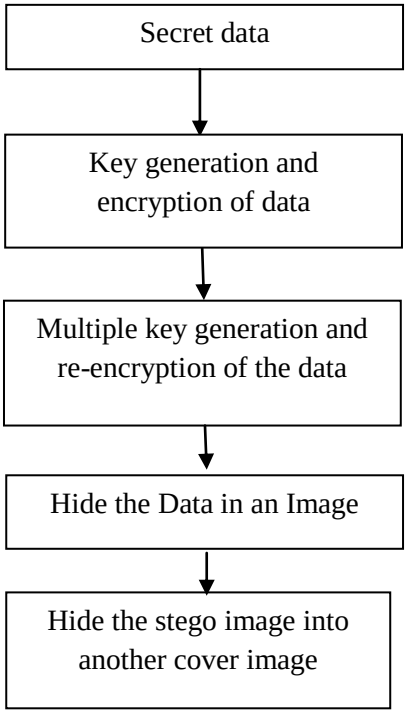


Figure 3.3 Algorithm for enhanced security of data using encryption and steganography

Firstly, we have taken two randomly generated data and on performing some operation on that data, the key has been generated. After that the data has been converted into the cipher text with the help of key. This is called the single key generation and the encryption process. The cipher text obtained after using different keys is further protected with the help of image steganography. For that a PNG image of pixel size 256×256 is taken as a cover image. It is then converted into gray scale image of same size. Now, the next step is to do embedding of the secret data in the cover image. So, for this we have used LSB substitution method of data embedding. For this, we have considered the three LSB's of the cover image which is

replaced by the data which has to be hidden. Thus, the image obtained after embedding the secret data is known as the stego image. Now, this image has become safe to be transmitted into the channel and no one would be able to know that there is some hidden data in the image. Then, for the next level of security, the stego image is further hidden into another cover image. The obtained final image is totally secured.

3.3 SCHEME FOR EMBEDDING USING EDGE DETECTION: FUZZY LOGIC METHOD

The comparison done in section 3.1 was based on the uniform embedding in all the pixels of the cover image. However this technique that we are currently using is based on variably embedding the pixels of the cover image i.e. the undisclosed message that has to be hide would be embedded variably in every pixel. The main emphasis is to get better picture quality of stego picture and also to enhance capability of data that can be hidden. This has been done by differentiating edge pixels and smooth pixels. Safety of every steganography strategy relies on upon the choice of pixels for hiding. Noisy pixels as well as pixels found in finished regions are preferred decisions for inserting on the grounds that they are hard to design. Edge pixels may be viewed as noisy pixels in light of the fact that their intensities may be higher or may be lower than their adjoining pixels because of abrupt transform in the coefficient angle. Because of these abrupt transforms in the visual and geometric properties, edges are hard to display in contrast with pixels of smoother zone. Hence a potential edge recognizing strategy is required. The flow diagram of this adaptive embedding process is shown in figure 3.4. Here, we are using fuzzy logic edge detecting algorithm. Fuzzy sets give the means to deal with imprecise information. It is based and connected intently to utilization of possibility in crisp information. Fuzzy sets gives margin for inaccuracy and its alteration probabilities in both info as well as outcome values. This technique considers full or fractional participation and connection among one value to other. A fuzzy inference system (FIS) toolbox in Matlab is used in which the input membership functions and the output membership functions are defined. Accordingly, various rules or conditions based on if, else or and rules are applied, on the basis of these rules the edge detection is done. This would separate the edge pixels from smooth pixels. Before embedding the data we have performed the clustering of the pixels of the image followed. The clustering is performed using k-means clustering that is a technique of vector quantization, originated from signal processing, and which is well-known for cluster investigation in information mining. The objective of k-means clustering is to divide η observations into k clusters. All observations belong to the cluster with the nearby mean, helping as a sample of the cluster. Following the k-mean clustering the embedding process

has to be performed. The data hiding process has performed by dividing the edge pixels in four numbers of clusters. The strong edge would contain maximum information and the smooth pixel would have less amount of information.

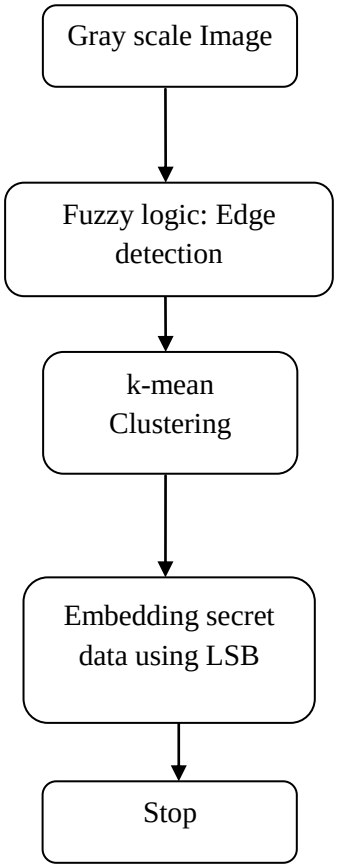


Figure 3.4 Flow chart for adaptive method of embedding

3.4 SCHEME FOR EMBEDDING USING EDGE DETECTION: SOBEL METHOD

As the data has to be embedded followed by edge detection and clustering processes, one more algorithm similar to as we discussed in the previous section has been proposed. Its flowchart is shown in figure 3.5.

The basic difference is the use of edge detection technique used. All other steps remained same. In this, the edges of grayscale image have been detected using another method of sobel edge detection. And then the k-mean clustering has been performed as explained in the previous section. The results and the comparison among both methods of edge detection are done in next chapter.

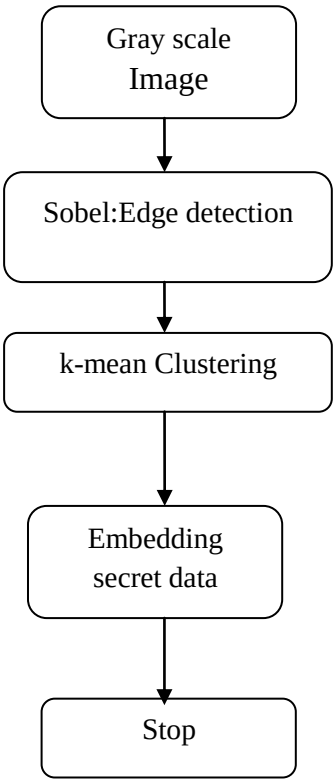


Figure 3.5 Flow chart for embedding using sobel edge detection

CHAPTER 4

RESULTS AND DISCUSSION

In this chapter, the outcomes of the proposed algorithm have been shown. This chapter is divided into four sections: a) Comparison among different image formats using LSB steganography, b) Enhanced security of data using encryption and steganography, c) Triple security using both encryption and steganography and d) Comparison between embedding using fuzzy edge detection and using sobel edge detection.

4.1 COMPARISON AMONG DIFFERENT IMAGE FORMATS USING LSB STEGANOGRAPHY

For embedding secret data, nine cover images, shown in table 4.1 (a-i) are taken. They all are of different format with different pixel sizes. Three different formats are JPG, PNG and BMP and three pixel sizes are 256×256, 512×512 and 1024×1024. Before embedding data into cover images, they are converted in to gray scale images. Then the secret data is embedded into the three LSB's of these obtained gray color images and thus nine stego images have been obtained which are shown in table 4.2, 4.3 and 4.4**.**

Type → Size ↓	JPG	PNG	BMP
256×256	 (a)	 (b)	 (c)
512×512	 (d)	 (e)	 (f)

1024×1024			
	(g)	(h)	(i)

Table 4.1 Nine different cover images

Comparison between the stego images on the basis of execution time and payload bits has been done and is shown in table 4.5. From the table 4.5, it has been observed that as the pixel size of the image increases the number of payload bits increases correspondingly. Say, for a size of 256×256 the secret data is of length around 196608 bits. Similarly, it increases to 786432 bits and 3145728 bits as the pixel size of the image is increased to 512×512 and 1024×1024 respectively. Further, it has also been analyzed that the execution time is also varying for different formats as well as with different pixel sizes. Performance of the different image formats with different pixel size has been compared by considering image quality parameters such as, PSNR and MSE and is shown in table 4.6. High PSNR value and low MSE value tells us that the image is of good quality. The value of PSNR is measured in decibel (dB). If PSNR value is more than 30 dB, image distortion is generally considered as imperceptible.

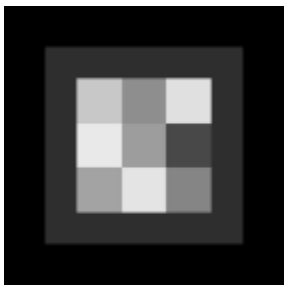
		
a) Image 01	b) Image 02	c) Image 03

Table 4.2 Stego images of size 256×256 pixels a) JPG, b) PNG and c) BMP

In table 4.2, three images of pixels size 256×256 in formats JPG, PNG and BMP are taken. On embedding the secret data in three LSB's of the pixel of these images, it has been viewed that the maximum length of data that can be embed is of 196608 bits in all the three image

formats. The PSNR and MSE values of these three images are also found. It has been observed that out of three image formats JPG, PNG and BMP the PSNR value of the PNG is the maximum while JPG has the lesser value than JPG and BMP has least PSNR value. The MSE value is least for PNG, than JPG and is maximum for BMP. The processing time is moderate for PNG, and is minimum for JPG and is maximum for BMP. So, comparing all the three formats PNG is considered as the optimum format for data hiding using steganography.

		
a) Image 04	b) Image 05	c) Image 06

Table 4.3 Stego images of size 512×512 pixels a) JPG, b) PNG and c) BMP

Similarly, if we consider the above three image formats but now with image size 512×512, so as the pixel size increase the embedding capacity is also increased from 196608 bits to 786432 bits. The PSNR value is nearly same for JPG and PNG and is more for BMP. Similarly, the MSE is approximately equal for both JPG and PNG but is less for BMP.

		
a) Image 07	b) Image 08	Image 09

Table 4.4 Stego images of size 1024×1024 pixels a) JPG, b) PNG and c) BMP

The processing time for BMP is more than JPG and less than PNG. So, for pixel size 512×512, BMP results are better than JPG and PNG. Now, we have considered three more images 7 to 9 which are shown in table 4.4 in which the pixel size of images are of 1024×1024. As the pixel size has increased, the overall capacity of the secret data is also increased from 786432 bits to 3145728 bits. On comparing the above three images, it has been observed that the processing time for BMP is 620 seconds while for JPG it is less that is 606 seconds and for PNG it is highest which is 679 seconds. The PSNR values are nearly same for all the three formats. The mean square error is least for BMP that is equal to 5.26 and which is little less than PNG and for JPG value of MSE is large which is around 7.37.

Comparing all the factors we found that the BMP image format has better optimized results than PNG and JPG.

Finally, the comparison among all three sizes of JPG images has been done, and it is observed that as pixel size increase from 256 to 512 and then to 1024, although payload increases but the processing time increases and the PSNR value also decreases. Similarly, in case of PNG image format as the pixel size of an image increases the embedding capacity increases but at a rate of increased processing time and higher value of MSE.

Factors →	Processing Time (Seconds)			Payload(Bits)		
Pixel Size ↓	JPG	PNG	BMP	JPG	PNG	BMP
256×256	41.459	44.755	47.458	196608	196608	196608
512×512	162.797	178.258	168.211	786432	786432	786432
1024×1024	606.115	679.333	620.100	3145728	3145728	3145728

Table 4.5 Processing time and payload of different image formats with different pixel sizes

Pixel Size	PSNR(dB)			MSE		
	JPG	PNG	BMP	JPG	PNG	BMP
256×256	42.1405231	45.4849798	39.3992447	4	1.85	7.53
512×512	42.9189103	42.7122022	45.5121571	3.35	3.51	1.84
1024×1024	39.4923072	40.958741	40.952108	7.37	5.27	5.26

Table 4.6 Comparison of PSNR and MSE for different images shown in table 4.1

But on comparing the case of BMP the image with pixel size 512×512 has better image quality then the stego image of 256×256 and 1024×1024.

For an M× N gray scale image, the PSNR value has been calculated using the given formula:

$$PSNR=10log_{10}(\frac{255}{MSE}) \quad (1)$$

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x(i,j)-x'(i,j)\right)\text{ ^ }2 \quad (2)$$

where $x(i, j)$ and $x'(i, j)$ are the pixel values of the cover and the stego image, respectively and MSE is the mean square error which is given in equation 2. It has been observed that in case of JPG, as the pixel size of image increases the PSNR value decreases and MSE value increases, but for pixel size 512×512 the MSE is least. In case of PNG as the size of pixel increases the value of PSNR decreases and MSE value also increases. For BMP the trends are not general, the best results have been observed for pixel size 512×512 in which we obtain

least MSE with highest PSNR. The overall results of PNG image format with different pixel size are better than that of JPG and BMP.

4.2 ENHANCED SECURITY OF DATA USING ENCRYPTION AND STEGANOGRAPHY

Figure 4.1 shows cover image of PNG format of pixel size 256×256 which is used for hiding the encrypted data. We are using three LSB's of each pixel to hide the encrypted data. Since, there are 256×256 pixels so, data which is being hidden (known as payload) is given as: Payload=256×256×3=199608 bits. Firstly, the cover image is converted into gray scale image of same size. Then the data is embedded into three LSB's of each pixel of the gray scale image shown in figure 4.1(b)**.** Finally the stego image is obtained which is shown in figure 4.1(c).

a) Original cover image01

e) Gray scale image02

c) Stego image01

d) Original cover image02

e) Gray scale image02

f) Stego image02

Figure 4.1 a,d) Cover image 01, 02, b,e) Grayscale image 01, 02, and c,f) Stego Image 01,02

Table 4.7 shows the values of PSNR and MSE of the stego image as shown in figure 4.1(c and f). For both images, it has been analyzed that value of MSE is very less and as a result a high value of PSNR is achieved. Also payload has been increased from 199608 to more bits by increasing the pixel size of the image. Further, the last step of the proposed algorithm is carried out which is to hide the stego image in another cover image.

PSNR (dB)	MSE	PAYLOAD (bits)
49.2520	0.78	199608
45.5925	1.81	199608

Table 4.7 PSNR, MSE and payload values for stego image obtained in 4.1(c,f)

Figure 4.2 Cover Image

The stego image (shown in figure 4.1 (c)) which is obtained after embedding the encrypted data now has been hidden again for achieving further security of data. For this a new cover image (shown in figure 4.2) is used to embed the stego image.

Figure 4.3 Final stego image

The cover image shown in figure 4.2 is then again embedded by the image containing the hidden data which is shown in figure 4.1(c). The hiding process which is adopted for hiding an image into another image is bit plane technique which replaces complex regions on the bit-planes of the vessel image with new complex data patterns (i.e., pieces of secret files). This replacing process is known as embedding. Now, no one will be able to observe any difference

between the cover image and the embedded image. The final image obtained after embedding the secret image is shown in figure 4.3.

4.3 FUZZY LOGIC EDGE DETECTION: ADAPTIVE METHOD OF EMBEDDING

In this section, we have discussed about the results obtained using fuzzy logic edge detection method, clustering using k-mean and the embedding process. The edge detection has been carried out on a gray scale image. First of all the grayscale image of the cover image is considered as shown in figure 4.4.

Figure 4.4 Cover image (Grayscale representation)

The edges of this image are to be found by using the fuzzy edge detection method which is based on Fuzzy inference system (MATLAB FIS toolbox). The fuzzy logic edge-detection process relies on the image gradient to locate breaks in uniform regions. The image gradients both along the x-axis as well as y-axis have been considered. The results of Ix and Iy are shown in figure 4.5 and 4.6 respectively. Now, we have to state a zero-mean Gaussian membership function for every input.

Figure 4.5 Edges along X-axis (Horizontally)

Figure 4.6 Edges along Y-axis (Vertically)

If the gradient value for a pixel is 0, it belongs to the zero membership function with a degree of 1. Similarly identify the triangular membership functions, white and black, for Iout. The final membership functions are shown in figure 4.7.

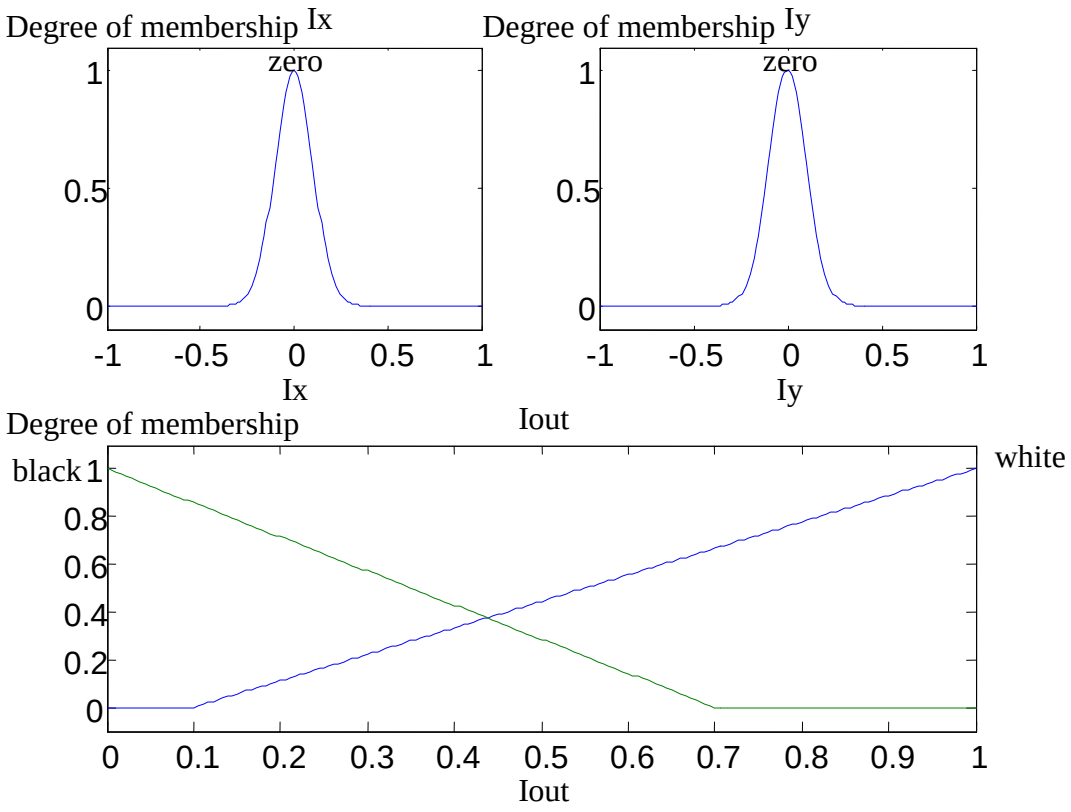


Figure 4.7 Membership functions for input and output

With the certain set of rules defined as following:

1. If (Ix is zero) and (Iy is zero) then (Iout is white) (1).

2. If (Ix is not zero) or (Iy is not zero) then (Iout is black) (1)'.

The final edge detection of the image has been shown in figure 4.8

Figure 4.8 Edge detection using fuzzy logic

After edge detection, clustering of the pixels using k-mean clustering technique has been performed. The clustered image is shown in figure 4.9.

Figure 4.9 Clustering using k-mean

Subsequent to k-mean clustering the data is embedded in the original grayscale image which is done in accordance with the pixels obtained after clustering process. The edge pixels are embedded with high number of bits and the smooth pixels are embedded with lower number of bits. This is done to achieve a high embedding capacity as well as to maintain an acceptable image quality of the stego image with a high value of PSNR and least value of MSE. The stego image so obtained is shown in figure 4.10.

Figure 4.10 Stego image

Thus, using fuzzy edge detection and k-mean clustering we have achieved new results for embedding our secret data into cover image. The PSNR, MSE and the payload values are shown in table 4.8.

Image	**PSNR**	**MSE**	**Payload**
Lena (256 × 256)	44.77	2.18	150099

Table 4.8 Value of Parameters using fuzzy logic

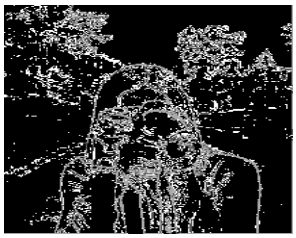
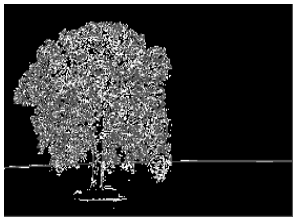
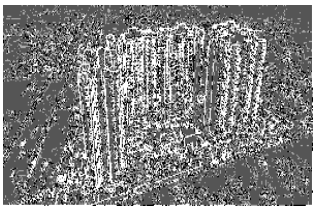
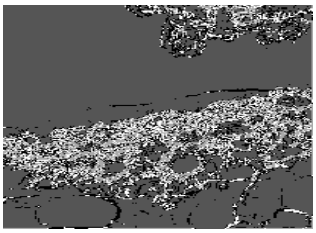
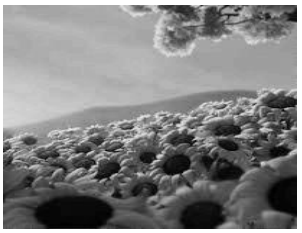
Hence, it is clear that for image 'Lena' of figure 4.4 which has a pixel of size 256 × 256 high value of PSNR i.e. 44.77 dB is achieved along with an embedding capacity of 150099 bits. Now, to analyze the proposed method a new edge method based on sobel edge technique has been also used. The results using fuzzy logic have been compared with sobel technique in the next section.

4.4 COMPARISON BETWEEN SOBEL AND FUZZY LOGIC BASED ALGORITHMS

In the last section, we have used the fuzzy logic method for edge detection. This method is tested on various images of different pixel sizes and their results are analyzed in this section. In addition, the results have been compared with another algorithm which is based on sobel edge detection.

The results are shown in table 4.9. Six different images which are house, camera girl, tree, skyscraper, sunflowers and sun are considered. The original grayscale image are shown in column one of the table 4.9 (a) to (f), the images obtained after performing edge detection

and k-mean clustering are shown from (g) to (l) and finally the stego images are shown in third column of the table 4.9 from (m) to (r).

 (a)	 (g)	 (m)
 (b)	 (h)	 (n)
 (c)	 (i)	 (o)
 (d)	 (j)	 (p)
 (e)	 (k)	 (q)

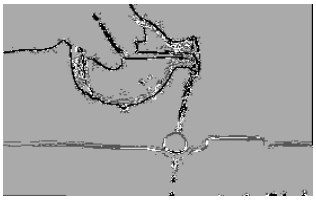
 (f)	 (l)	 (r)

Table 4.9 (a)-(f) Original Images, (g)-(l) Clustered Images and (m)-(r) Stego Images

The comparison of the results obtained using fuzzy edge detection (FED) and sobel edge detection (SED) are shown in table 4.10.

Image	**Pixel Size**	**MSE**		**PSNR(dB)**		**Payload(bits)**	
		FED	SED	FED	SED	FED	SED
House	285×177	4.5	5.10	40.949	39.9	115815	120527
Skyscraper	300×168	5.72	6.04	39.451	39.21	127871	130604
Sun	275×183	1.68	2.10	44.77	43.79	104755	108095
Tree	275×183	4.39	4.83	40.59	40.17	117658	121388
Cameragirl	212×238	2.67	4.24	42.75	40.75	110476	119941
Sunflowers	204×204	3.41	4.47	40.867	39.69	94105	99946

Table 4.10 Comparison of MSE, PSNR and Payload values using FDE and SDE

It has been observed from table 4.10 that the MSE value using fuzzy edge detection is comparatively less and as a result a high PSNR value is obtained as compare to sobel edge detection method. This provides a better image quality of the stego image, as it becomes more difficult for an unauthorized person to detect the presence of any secret data in the image. Hence, for a better quality image the FED method is more preferred for data hiding as compare to SED. But it should be noticed that the embedding capacity is more in case of SED method. More number of bits are embedded using the SED. Although the MSE is less and PSNR values are high in case of FED, but the stego images obtained in case of SED are also imperceptible for human eyes to view any major distortion in them, in addition capacity is also high in case of SED.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE OF RESEARCH

There are always two main requirements of image encryption, first it should be sent securely to the receiver and secondly it should be reached in minimum or optimum time. The presented work is focused on optimizing the encryption algorithm in order to achieve the above two factors. Literature survey has been successfully done on image encryption. A few of the observations has also been drawn from which the problem formulation and gaps are identified. Simulation results have been achieved using MATLAB R2013a. The data has been successfully embedded into the cover image and thus stego image has been obtained. Also LSB substitution scheme is used for embedding any secret data into gray images with different pixel sizes and formats. This is by uniform replacing of three LSB's of cover image by the secret data which has to be embedded. Comparison among the various images with different formats and pixel size is also done. PSNR and MSE values are also calculated. For enhanced protection of the data triple security algorithm is also proposed using encryption keys and image steganography which provides more safety to secret data. The impact of embedding data in smooth pixels and the edge pixels are also studied and thus an edge detection algorithm using k-mean clustering is proposed. Finally comparison among fuzzy edge detection and proposed edge detection algorithm is done which shows that the proposed SED provides more embedding capacity along with an acceptable picture quality. So, as a future work the image quality and the embedding capacity can be further improved and embedding and analysis can be also performed for audio or video files.

REFERENCES

[1] Menezes Alfred J, Oorschot Paul C van and Vanstone Scott A. *Handbook of Applied Cryptography*. CRC Press, 1996.

[2] Schneier Bruce. *Applied Cryptography.* John Wiley and Sons, 1996.

[3] Frank Y Shih. *Digital Watermarking and Steganography: Fundamentals and Techniques.* Second Edition Hardcover, 2017.

[4] Stallings William. *Cryptography and Network Security, Principles and Practice.* Pearson Prentice Hall, Pearson Education, 2011.

[5] Maniccam SS and Bourbakis NG (2001). Lossless image compression and encryption using SCAN, *Pattern Recognition*, 34, 1229-1245.

[6] Chang CC and Yu TX (2002). Cryptanalysis of an encryption scheme for binary images, *Pattern Recognition Letters*, 23, 1847-1852.

[7] Wu DC and Tsai WH (2003). A steganographic method for images by pixel-value differencing, *Pattern Recognition Letters*, 24, 1613-1626.

[8] Chang CC and HW Tseng (2004). A steganographic method for digital images using side match, *Pattern Recognition Letters*, 25, 1431-1437.

[9] Munoz-Rodriguez JA and Rodriguez-Vera R (2005). Image encryption based on a grating generated by a reflection intensity map, *Journal of Modern Optics*, 52(10), 1385-1395.

[10] Shin CM and Kim SJ (2005). Image encryption using modified exclusive-OR rules and phase-wrapping technique, *Optics Communications*, 254, 67-75.

[11] Lukac R and Plataniotis KN (2005). Bit-level based secret sharing for image encryption, *Pattern Recognition*, 38, 767-772.

[12] Wang RZ and Chen YS (2006). High-Payload image steganography using two-way block matching, *IEEE Signal Processing Letters*, 13(3), 161-164.

[13] Mao Y and Wu M (2006). Joint Signal Processing and Cryptographic Approach to Multimedia Encryption, *IEEE Transactions on Image Processing*, 15(7), 2061-2075.

[14] Wang CM *et al.* (2008). A high quality steganographic method with pixel-value differencing and modulus function, *The Journal of Systems and Software*, 81, 150-158.

[15] Kekre HB, Athawale A and Halarnkar PN (2008). Increased Capacity of Information Hiding in LSB's Method for Text and Image, *International Journal of Computer, Electrical, Automation, Control and Information Engineering*. 2(5), 1497-1500.

[16] Joshi M, Chandrashakher and Singh K (2008). Color image encryption and decryption for twin images in fractional Fourier domain, *Optics Communications*, 281, 5713-5720.

[17] Zhang Z, Zhu C, and Zhao Y (2008). Two-Description Image Coding with Steganography, *IEEE Signal Processing Letters*, 15, 887-890.

[18] Liu Z, Ahmad MA and Liu S (2009). Image encryption scheme based on the commutation and anti-commutation rules, *Optics Communications*, 279, 285-290.

[19] Singh M, Kumar A and Singh K (2009). Encryption by using matrix-added or matrix-multiplied input images placed in the input plane of a double random phase encoding geometry, *Optics and Lasers in Engineering*, 47, 1293-1300.

[20] Liu Z *et al.* (2009). Triple image encryption scheme in fractional Fourier transform domains, *Optics Communications*, 282, 518-522.

[21] Yang H *et al.* (2010). A fast image encryption and authentication scheme based on chaotic maps, *Communication Nonlinear Science Numerical Simulation*, 15, 3507-3517.

[22] Luo W, Huang F and Huang J (2010). Edge Adaptive Image Steganography Based on LSB Matching Revisited, *IEEE Transactions on Information Forensics and Security*, 5(2), 201-214.

[23] Lin GS, Chang YT and Lie WN (2010). A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on simulated annealing algorithm, *IEEE Transactions on Multimedia*, 12(5), 345-357.

[24] Guo JM and Le TN (2010). Secret Communication using JPEG Double Compression, *IEEE Signal Processing letters*, 17(10), 879-882.

[25] Zhang J and Zhang D (2010). Detection of LSB Matching Steganography in Decompressed Images, *IEEE Signal Processing Letters*, 17(2), 141-144.

[26] Wang X and He G (2011). Cryptanalysis on a novel image encryption method based on total shuffling scheme, *Optics Communications*, 284, 5804-5807.

[27] Wua CC, Kao SJ and Hwang MS (2011). A high quality image sharing with steganography and adaptive authentication scheme, *The Journal of Systems and Software*, 84, 2196- 2207.

[28] Liao X, Wen QY and Zhang J (2011). A steganographic method for digital images with four pixel differencing and modified LSB substitution, *Journal of Visual Communication and Image Representation*, 22, 1-8.

[29] Chung Hou *et al.* (2011). An Optimal Data Hiding Scheme with tree-based parity check, *IEEE Transactions on Image Processing*, 20(3), 1-7.

[30] Roy S *et al.* (2011). A secure keyless image steganography approach for lossless RGB images, *International Conference on Communication, Computing & Security* [2nd, India: 2011], pp. 573-575.

[31] Satir E and Isik H (2012). A compression-based text steganography method, The *Journal of Systems and Software*, 85, 2385-2394.

[32] Kakkar A, Singh ML and Bansal PK (2012). Mathematical Analysis and Simulation of Multiple Keys and S-Boxes in a Multi-node network for Secure Transmission, *International Journal of Computer Mathematics*, 89(16), 2123-2142.

[33] Ma K, Liang H and Wu K (2012). Homomorphic Property-Based Concurrent Error Detection of RSA: Countermeasure to Fault Attack, *IEEE Transactions on Computers*, 61(7), 1042-1049.

[34] Bhati S *et al.* (2012). A New Approach towards Encryption Schemes: Byte – Rotation Encryption Algorithm, *Proceedings of the World Congress on Engineering and Computer Science* [2nd, San Francisco, USA: 2012].

[35] Pareek NK, Patidar V and Sud KK (2013). Diffusion–substitution based gray image encryption scheme, *Digital Signal Processing*, 23, 894-901.

[36] Pakshwar R, Trivedi VK and Richhariya V (2013). A Survey on Different Image Encryption and Decryption Techniques, *International Journal of Computer Science and Information Technologies*, 4 (1), 113-116.

[37] Juneja M and Sandhu PS (2013). An Analysis of LSB Image Steganography Techniques in Spatial Domain, *International Journal of Computer Science and Electronics Engineering*, 1(3), 454-459.

[38] Yang C *et al.* (2013). Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography, *IEEE Transactions on Information Forensics and Security*, 8(1), 216-228.

[39] Chakraborty S, Jalal AS and Bhatnagar C (2013). Secret image sharing using grayscale payload decomposition and irreversible image steganography, *Journal of Information Security and Applications*, 18, 180-192.

[40] Tang M, Hu J and Song W (2014). A high capacity image steganography using multi-layer embedding, *Optik*, 125, 3972-3976.

[41] Sarreshtedari S and Akhaee MA (2014). One-third probability embedding: a new ±1 histogram compensating image least significant bit steganography scheme, *IET Image Process*, 89(2), 78-89.

[42] Kekre HB, Sarode T and Halarnkar P (2014). A Hybrid Approach for Information Hiding and Encryption using Multiple LSB's Algorithms, *International Journal of Application or Innovation in Engineering and Management*, 3(6), 42-51.

[43] Kanan HR and Nazeri B (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, *Expert Systems with Applications*, 41, 6123-6130.

[44] Subhedar MS and Mankar VH (2014). Current status and key issues in image steganography: A survey, *Computer Science Review*, 95-113.

[45] Agrawal V, Agrawal S and Deshmukh R (2014). Analysis and Review of Encryption and Decryption for Secure Communication, *International Journal of Scientific Engineering and Research*, 2(2), 2347-3878.

[46] Cheon JH and Kim J (2015). A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption, *IEEE Transactions on Information Forensics and Security*, 10(5), 1052-1063.

[47] Zhang Y and Zhang LY (2015). Exploiting random convolution and random subsampling for image encryption and compression, *Electronics letters*, 51(20), 1572-1574.

[48] Ahani S and Ghaemmaghami S (2015). Color image steganography method based on sparse representation, *IET Image Process*, 9, 496-505.

[49] Sun Y *et al.* (2015). Image compression and encryption scheme using fractal dictionary and Julia set, *IET Image Process*, 9(3), 173-183.

[50] Feng B, Lu W, and Sun W (2015). Secure Binary Image Steganography based on minimizing the Distortion on the Texture, *IEEE Transactions on Information Forensics and Security*, 10(2), 243-255.

[51] Maheswari SU and Hemanth DJ (2015). Frequency domain QR code based image steganography using Fresnelet transform, *International Journal of Electronics and Communication*, 69, 539-544.

[52] Farhat F and Ghaemmaghami S (2015). Towards blind detection of low-rate spatial embedding in image steganalysis, *IET Image Processing*, 9(1), 31-42.

[53] Guo L *et al.* (2015). Using Statistical Image Model for JPEG Steganography: Uniform Embedding Revisited, *IEEE Transactions on Information Forensics and Security*, 10(12), 2669-2680.

[54] Li B *et al.* (2015). A Strategy of Clustering Modification Directions in Spatial Image Steganography, *IEEE Transactions on Information Forensics and Security*, 10(9), 1905-1917.

[55] Wu J *et al.* (2016). Multiple-image encryption based on computational ghost imaging, O*ptics Communications*, 359, 38-43.

[56] Shihua ZS *et al.* (2016). Encryption method based on a new secret key algorithm for color images, *International Journal of Electronics and Communication*, 70, 1-7.

[57] Jain M and Lenka SK (2016). A Review of Digital Image Steganography using LSB and LSB Array, *International Journal of Applied Engineering Research,* 11(3), 1820-1824.

[58] Sedighi V, Cogranne R and Fridrich J (2016). Content-Adaptive Steganography by Minimizing Statistical Detect ability, *IEEE Transactions on Information Forensics and Security*, 11(2), 1-14.

[59] Sajedi H (2016). Steganalysis based on steganography pattern discovery, *Journal of Information Security and Applications*, 30, 3-14.

[60] Dadgostar H, Afsari F (2016). Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB, *Journal of Information Security and Applications*, 30, 94-104.

[61] Mahato S, Yadav DK and Khan DA (2017). A minesweeper game-based steganography scheme, *Journal of Information Security and Applications,* 32, 1-14.

[62] Malik A, Sikka G and Verma HK (2017). A high capacity text steganography scheme based on LZW compression and color coding, *Engineering Science and Technology, an International Journal*, 20, 72-79.

LIST OF PUBLICATIONS

- Kaur H and Kakkar A (2017). Image steganography using edge detection and clustering of pixels, *International Journal of Computer Application*, 172(2), 41-45.

- Kaur L, Kaur H and Kaur T (2017). Triple security of data using encryption keys and image steganography, *International Journal of Computer Application*, 171(7), 19-22.

- Kaur H and Kakkar A (2017). Comparison on different image formats using LSB Steganography, *IEEE International Conference on Signal Processing, Computing and Control* [4th: Solan, Himachal Pradesh, India] (accepted, Conference will be held on 21-23 September, J.P. University, Solan).

.

Harpreet_13-07-2017

ORIGINALITY REPORT

%15	%7	%13	%4
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Dadgostar, H., and F. Afsari. "Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB", Journal of Information Security and Applications, 2016. Publication	%1
2	www.mathworks.com Internet Source	%1
3	felicitysmoak.info.tm Internet Source	%1
4	www.isaet.org Internet Source	%1
5	academic.odysci.com Internet Source	<%1
6	Mahato, Susmita, Dilip Kumar Yadav, and Danish Ali Khan. "A minesweeper game-based steganography scheme", Journal of Information Security and Applications, 2017. Publication	<%1