Sharing of a Digital Secret Image by Diverse Media for more Security

A Dissertation Submitted in partial fulfillment of requirement for the award of Degree of

Master of Engineering

In

Wireless Communication

Submitted by

Tejbir Kaur

Roll No: 801563028

Under the Guidance of

Dr. Ajay Kakkar

Assistant Professor, ECED

Thapar University, Patiala

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

(Established under the section 3 of UGC Act, 1956)

Patiala – 147004 (Punjab

DECLARATION

I, Tejbir Kaur hereby declare that the work presented in this thesis entitled "Sharing of Digital Secret Image by Diverse Media for more Security" 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

Tejbir Kaur
Tejbir Kaur
Roll No: 801563028

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

Date: 28/8/17

Ajay kakkar
Dr. Ajay Kakkar
Assistant Professor, ECED

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.

Tejbir Kaur.

Tejbir Kaur

ME-WC

801563028

ABSTRACT

The efficient algorithms require correct protocols for authentication and key management. It is intended to modify the available cryptographic algorithm to achieve more security and this will be done by incorporating visual cryptography. The visual cryptography is an efficient method to share our data in secured manner. Conventional Visual Secret Sharing (VSS) schemes are used to hide secret images in the shares that are either encoded or printed on transparencies. Natural visual secret sharing (NVSS) in which various carrier media is used to carry secret images Natural visual secret sharing (NVSS) in which various carrier media is used to carry secret images by a share to protect the secret and the participants during the transmission phase has been proposed. The proposed $(n, n) - $ NVSS scheme shares one digital secret image over $n - 1$arbitrary selected natural images and one noise-like share. Our aim is to use visual cryptography for transmission of the secret image and to protect the network in order to keep the data confidential. The image is preprocessed, and then features extraction has been done. The PSNR values of digital and handmade image are 33.04 and 32.93 respectively. In feature extraction process thresholding, binarization and chaos process has been done. The median values of digital and handmade image come out to be 205 and 162 respectively. All the pixels have been arranged with respect to median values. Other techniques like encryption and pixel swapping have also been used. And at the end,to provide to our information more security, steganography has been used. The PSNR and elapsed time of the images has also been analyzed. The above work have its utility to transfer secret information over web, so that, intruder couldn't detect it.

TABLE OF CONTENTS

LISTS OF TABLES

LISTS OF FIGURES

LISTS OF ABBREVIATIONS

CT	Cipher Text
PT	Plain Text
TDES	Triple Data Encryption Standard
RSA	Rivest Shamir Adleman
US	Unconditionally Secure
CED	Concurrent Error Detection
VSI	Visual Security Index
HVS	Human Visual System
APE	Average Pixel Expansion
MBNS	Multiple Base Notation System Steganography
FSMM	Finite State Machine Model
SLPNN	Single-Layer Perception Neural Network
COA	Cipher Text Only Attack
KPA	Known Plaintext Attack
CPA	Chosen Plaintext Attack
DA	Dictionary Attack
BFA	Brute Force Attack
BA	Birthday Attacks
SCA	Side Channel Attacks
TA	Timing Attacks
PAA	Power Analysis Attacks

CHAPTER 1
INTRODUCTION

This chapter includes the importance of security of data of documents being transferred on a network along with the possible threats that can be arising during transmission. A brief introduction of visual cryptography, advantages of that technique, and its applications has also been discussed.

1.1 HISTORY OF CRYPTOGRAPHY:

Cryptology is a technique for youthful science [2]. In spite of the fact that is been utilized for many years for concealing the mystery messages, efficient investigation of cryptology as a science had quite recently begun around one hundred years prior[3].

The essential use of cryptography was found in 1900 BC, in the guideline board of the tomb of the privileged person in the Egypt. They used some exceptional hieroglyphic pictures there set up of more typical ones [2]. Their inspiration was not by any means to hide that message but instead to change sort of the message to such an extent that it would make it appear to be respectable. Regardless of the way that it was not a sort of secret making, but instead solidified some sort of progress of the primary, and is the most settled referred to do accordingly. Affirmation of some use of cryptography is seen in early municipal foundations [5].

Around 100 BC, Julius Caesar was well known technique which was to utilize a type of cryptography to pass on hidden messages to his commanders posted in the war. Caesar figure shown in figure 1.1 is the most specified famous figure. In a substitution method, each character of the plain was replaced by another to shape the figure. The variation utilized by Caesar was a moving by 3 figures [5]. Each character of his information was moved by 3 places, so that the character "A" was supplanted by 'D', "C" was supplanted by 'F'. The characters will wrap around toward the end, so "X" will be supplanted by 'A'. It simple to see that such figures relies on the mystery of that structure and not on the key. Once the structure is known to another person, these messages can without quite a bit of an extend be decoded [3].

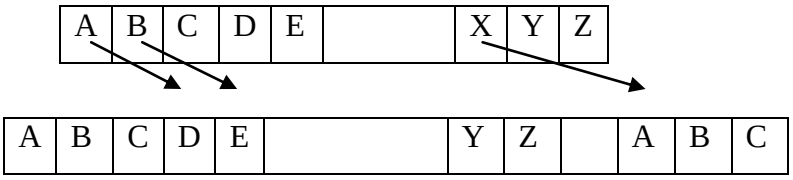


Figure 1.1 Julius Caesar's method of cryptography

In the sixteenth century a figure was composed that was the primary figure that was planned by, Vigenere utilized an encryption key. The encryption key was rehashed ordinarily all through the whole message in one of his figure, and afterward the yield figure was created by including message character with the key character modulo 26 [2]. As with the Caesar figure, Vigenere's figure shown in figure 1.2 can likewise effortlessly be broken; be that as it may, Vigenere's figure brought the general concept of bringing encryption keys, however it was wretched. By comparing this with Caesar figure, they became aware of with that the secrecy of the message relies on upon secrecy of the encryption key, instead of the secret of the framework [1].

$K =$ | C R Y P T O | C R Y P T O | C R Y P T |

$+ mod\ 26$

$M =$ H A V E A N I C E D A Y T O D A Y

$C =$ K S S U U U C L U D T U N W G C Q S

Figure 1.2 Vigenere's cipher cryptography

Also, toward the beginning of the nineteenth century when everything ended up noticeably present day and electric, Hebern was first to outline an electro-mechanical contraption and was known as the Hebern rotor machine [1]. A solitary rotor was utilized, in which the mystery key was implanted in a pivoting circle of electrical machine. The key encoded a table and each key they squeezed from the console was brought about the yield of a figure message consequently. This likewise pivoted the plate by one indent and an alternate table then would be utilized for the following plain character. Implies they changed their calculation of encryption after one line [5].

After that electro-mechanical contraption, the machine was designed by German designer Arthur Scherbius toward the finish of World War I called Engima machine, and was vigorously utilized by the German compel at the seasons of the Second World War. The Enigma machine utilized 2 or 3 or significantly more rotors. In any case, the Enigma machine's figure was broken by Poland [1].

At the Second World War, the majority of the work that was done on the cryptography was for military purposes, for the most part used to hide the mystery of military data. Nonetheless, cryptography was additionally turned out to be prominent in business needs, as organizations man was attempting to conceal their information from the unapproved clients [1].

In the 1970's, IBM clients were demanding some different type of encryption, so they formed a group called "crypto group". They had designed their own different cipher called Lucifer. Then in 1973, the Nation Bureau of Standards put out a request for proposals for a new cipher called block cipher which now become a national standard. Lucifer was eventually accepted their cipher and was called DES. In 1997, DES technique was also broken by the attack called search attack. The key was very small in DES that was the problem. Anyone can guess the key by increasing the computing power by applying different combinations of the key [1].

Figure 1.3 Engima machine

In 1997, NIST again put on a demand of proposition for another piece figure. It got around 50 entries. What's more, in 2000, it acknowledged Rijndael, and dedicated it as AES [2].

1.2 CRYPTOGRAPHY:

Cryptography is a method of hide and stores the data in such a manner that it cannot be revealed or accessed by the unauthorised user [4]. The information or data is protected by converting them into a different format which is unreadable by any unauthorized person. The text after transforming is called cipher text. [1] The message is decrypted by only those persons who are aware of the secret key used to transform cipher text into useful information. The method by which that cipher text is converted into original form is called decryption [1].

Figure 1.4 Encryption and Decryption

1.3 NEED OF CRYPTOGRAPHY:

Cryptography is actually very important in our life. There is a need of secured data communication in defense, industries, universities; etc. This technique is also helpful in security systems of banks for the electronics transfer of the money [3].

1.4 TYPES OF CRYPTOGRAPHIC ALGORITHMS:

Cryptographic algorithms are classified into several ways. For this thesis, the classification has been done on the number of keys used for encryption and decryption [1]. The two types of algorithms are:

a. Secret Key Cryptography (SKC)
b. Public Key Cryptography (PKC)

1.4.1. Secret key cryptography:

In *secret* key cryptography both encryption and decryption processes are carried out by a single key. As drawn in figure 1.2, the key is used by the sender to encrypt the plain text and then sends the cipher text to the receiver. In the receiver side, the same method is applied for the decryption [2]. Secret key cryptography is also known as *symmetric encryption*, because one key is used for both functions. Distribution of the key to both the participants is toughest task for this technique. Both the parties should be aware of the key [6].

1.4.2. Public key cryptography (PKC):

In 1976 the technique named Modern PKC technique was first time publicly described by

Professor Martin Hellman [3]. Few asymmetric encryption algorithms are; DSA, RSA and ECDSA. Many advantages, digital signature and long-term encryption are the main key features.

1.5 THE CRYPTOGRAPHIC TECHNIQUES:

Cryptography is one of the easiest and necessary techniques [8]. It is used for building of a new and secured VPN, It has two components; a)Encryption algorithm, and b) keys Encryption is provided to many applications with the identical algorithm by which data is kept secret. In this way, some basic operations on keys in the cryptography are used to provide secrecy. It may be carried out by any from these two categories symmetric cryptography and the asymmetric cryptography [2].

Symmetric cryptography is that type of cryptographic technique in which a key, which is a part of secret information is shared to sender and receiver and is used in encryption and decryption processes. The main insecure part is process in which both peers agree upon same key, until the key is agreed. Now, there is another technique called Asymmetric, or Public Key, cryptography which smartly resolves the key exchange issue occurred in previous technique by using two different keys. We can only decrypt the encrypted data using other key [3].

If someone wants to do a communication in a secured way then he/she have to encrypt the message with public key, in which the private key has not been disclosed by him/her; only the authorized recipient will be able to do decryption and the encrypted of the text and recover the original message from the text [3].

1.5.1 Symmetric ciphers:

In Symmetric ciphers a comparable key is to hide the plaintext and to interpret the message both the sender and the recipient must need to consequently agree upon this one key, which must be known to no one else, early. The cryptographic nature of a symmetric figuring may depend on the measure of the key it uses. The instances of counts are DES, Blowfish, and AES. In DES, a 64-bit key is used, in which 8 bits are held leaving 56 variable bits. It is possible to secure information with 3DES as opposed to DES. This infers the information is subjected to three dynamic encryptions [4]. The usage of various encryption cycles does not so much offer a going with augmentation in security, and may be viewed as an abuse of enlisting power for a few applications. Blowfish calculation enables implementers to choose a

key length of in the vicinity of 32 and 448 bits; monetarily usage frequently utilizes 128-piece keys [2]. DES was replaced by AES in 2002 as an encryption standard by the US government [5]. From that point forward AES has turned out to be extremely famous in light of the fact that it consolidates the speed of DES with the security level of Triple DES. AES can utilize 128, 192 and 256-piece keys; numerous open AES-based items utilize 128-piece mystery keys as a matter of course [1]. Symmetric calculations are well known in view of their speed which empowers them proficiently to encrypt substantial amounts of plaintext. There are further two subcategories of symmetric figure, stream and square figures [5].

1.5.2 Stream ciphers:

These calculations had worked upon one piece at any given moment. The information is a flood of plaintext streams into the message. Messages encrypted with a stream figure are dependably an indistinguishable size from the first plaintext. The encryption process happens by an operation in which each piece of the plaintext is XOR with an arbitrary piece to create the message as shown in figure 1.5 Random data (key) and plain text has been used to form a cipher text called Random bit generator. The quintessence of a stream figure concerns the techniques by which the mutual key is utilized to produce the flood of arbitrary bits [4].

Figure 1.5 Random bit generator

1.5.3 Block ciphers:

These ciphers encrypt information in squares of bytes, as opposed to a solitary piece at any given moment. Their block sizes differ as per the calculation, 64 bits being the commonest. Since, the plaintext is probably not going to be several of the calculation's square size, it is important to cushion the information [3]. For instance, if the square is of 64 bits length and the last piece contains 40 bits, 24 bits of cushioning must be included. The cushioning string comprises of the considerable number of zeros, ones, arbitrary bits and some different sequence. DES, AES and the Blowfish are piece figures [5].

Two main methods are used for encrypting a sequence of blocks. Either the cipher is used on all blocks without reference to what has done before and the blocks are treated independently, or the results of encrypting previous blocks affect the encryption of the current block [3].

These two are methods known as the Electronic Codebook mode and Cipher Block Chaining cipher text mode respectively.

ECB MODE: Identical blocks of cipher text were being clearly generated identical blocks of plaintext. A cracker can exploit repetition in the cipher text to release the plaintext version [5].

CBC MODE: A criticism is included, so that, the consequences of the encryption of all the past squares are not dependent over into encryption of the present but also dependent on the previous blocks. Each message content is made not just subject to the plaintext obstruct that produced it. This guarantees us that regardless of the possibility that the plaintext contains large number of squares, they each encode to an alternate figure content piece [3]. CBC takes the last piece of figure content and XORs it with the present square of plaintext. Despite the fact that CBC mode strengths indistinguishable plaintext pieces to scramble to various squares, messages that begin with similar information will encode similarly up until the principal distinction, since, the underlying plaintext pieces are indistinguishable. Different modes are accessible. However, they had not talked about here on the grounds that the entire message was utilized as a part of VPN technology only in CBC mode.

1.5.4 Asymmetric ciphers:

They most prominent favorable position of asymmetric figures is a mutual mystery key does not need to be traded over an unreliable medium, the general population Internet. A couple of keys were produced and one of them named as the Public Key and was distributed. Any gatherings wishing to discuss safely with the key's proprietor scramble the message utilizing the beneficiary's Public Key [5]. The decoding must be finished by knowing the second, Private key, which the proprietor guarantees was never discharged [2].

1.6 CRYPTOGRAPHIC ATTACKS:

The fundamental thought of an attacker is to assault on a framework to break it and to discover the concealed information from the figure content. To discover the plaintext, the one thing that is expected to known by the attacker just is to discover the decoding key, in light of the fact that the calculation is now out in the open space [2].

Therefore, they give their most extreme push to discover the mystery key [2]. Once the assailant can decide the key, the assaulted framework is considered as broken. Based on the methodology used, attacks can be classified as follows:

Cipher text Only Attacks (COA): In this sort of assault, the assailant approaches an arrangement of message. He/she doesn't approach comparing plaintext. COA is fruitful when the assailant is effective to encode a relating plaintext, it can be resolved from a given arrangement of message [6].

Known Plaintext Attack (KPA): The attacker knows the plaintext for some of the parts of that cipher text. His/her task is to decrypt the remaining part of the cipher text using this information. The task may be done by determining the key [6].

Chosen Plaintext Attack (CPA): The attacker has the some part of the text of encrypted. So, it becomes easy for him to determining the encryption key [6].

Dictionary Attack (DA): The assailant assembles builds of all the messages and comparing plaintexts that he/she has learnt over a timeframe. It would be simple for him/her to encode the mystery data utilizing the word reference [5].

Brute Force Attack (BFA): The assailant tries to locate the key by attempting all the conceivable keys. If the key is 8 bits in length, the quantity of conceivable keys is $2^8 = 256$. The aggressor knows the message and the calculation, now he/she attempts all the 256 keys one by one for decoding. In the event that the key length is huge and it will be hard to assault. An opportunity to attempt all the keys will be high [2].

Birthday Attack (BA): It is utilized against the cryptographic hash work. Assume all the students in a class have some information about their birthday celebrations, the appropriate response is from one of the conceivable dates, implies from 365/366 dates. This provides a chance to accept the principal understudy's introduction to the world date is third August. At that point, to locate the following understudy whose birth date is n date, all one have to enquire $1.25*\sqrt{365} \approx 25$ students [2].

Side Channel Attack (SCA): This assault is not against a specific kind of calculation. It is propelled to abuse the shortcoming in the physical usage of the calculation [5].

Timing Attacks (TA): A diverse technique devours different measure of time to figure on processor. By measuring those timings, it is conceivable to think about a specific calculation of the processor. If the encryption takes an excessive amount of time, it demonstrates that the mystery key is long [5].

Power Analysis Attacks (PAA): These attacks are fairly same as that of timing assaults aside from that the measure of energy utilization is utilized to acquire data about the way of the fundamental calculations [6].

1.7 BENIFITS OFCRYPTOGRAPHY:

Cryptography is a very essential tool of security. It provides the three most basic benefits which are as follows:

Confidentiality: By Encryption, one can monitor the data and correspondence from unapproved disclosure and access of data [2].

Authentication: Some of the cryptographic techniques like MAC and digital signatures can protect the information against spoofing and forgeries [2]

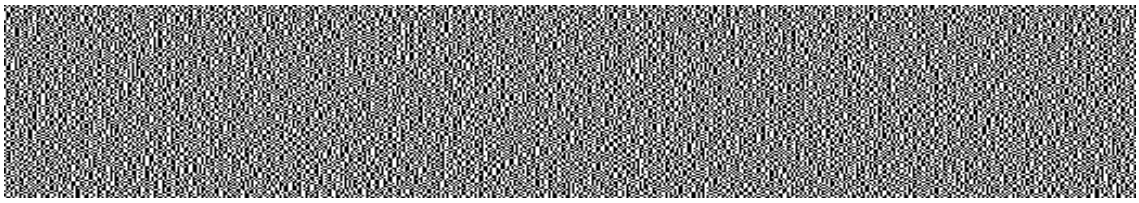
.

Data Integrity: In assuring the users about the data integrity, the cryptographic hash functions are playing vital role [2].

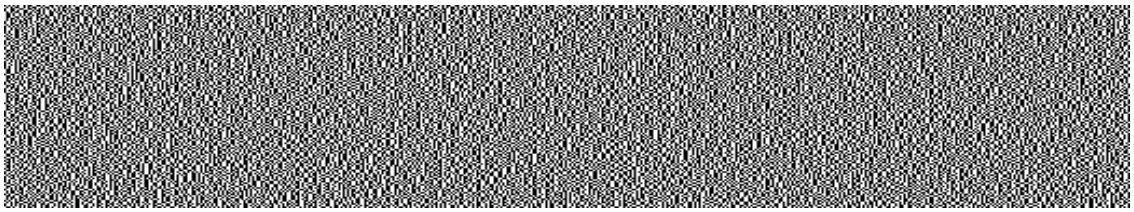
1.8 VISUAL CRYPTOGRAPHY:

It is a cryptographic strategy which permits any visual data like pictures and pictures to be encoded such that it can be decoded just by an approved client. The utilized could decode the data by the simple technique, by sight perusing. In visual mystery sharing, a picture was separated into n shares, so that, exclusive individual having every one of the offers could decode the picture, while on the off chance that they have not as much as n offers they uncovered no data about the first picture. Each offer was imprinted on a different straight forwardness, and decoding was performed by covering the offers as appeared in figure 1.6. The primary offer is of the picture named 'TEJBIR'. By applying the encryption strategies, the picture is separated into two offers, share 1 and offer 2. By stacking these two offers, the resultant picture is uncovered.

(a) Original Share



(b) Secret share 1



(c) Secret share 2

(d) Output image by combining both shares

Figure 1.6 Example of Visual cryptography

1.8.1 Algorithm for visual cryptography:

Initial step of this calculation is to make a picture which is having arbitrary pixels. Shape and size of that picture should be same as of the first picture. At that point, the second step is to make another picture of an indistinguishable size and shape from the main picture. However, pixel of the first picture is same as the relating pixel in first scrambled picture. Set a similar pixel of the second scrambled picture to the inverse shade of the first. A pixel of unique picture is not the same as a similar pixel in the main offer, now set the pixel of the second picture to indistinguishable shading from the pixel of the principal share. These two arbitrary pictures are now being joined utilizing a restrictive or (XOR) to deliver an unique picture. Each of the pixels of the images is divided into the smaller blocks. There are the same

number of black and white and blocks. If a pixel is divided into two equal parts, there are one white and one black block. And when pixel is divided into six equal parts, there are three black and three white blocks. The example images from above uses pixels that are divided into four parts.

In the figure 1.7, a pixel, which was isolated into four sections, they can have the six distinct states. On the off chance that layer 1 pixel has a given express; the pixel which is on layer 2 may have one of two states: a) altered, and b) the same to the pixel of layer 1. On the off chance that pixel of layer 2 is indistinguishable to the layer 1; the overlayed pixel will be half dark and half white. Such kind of pixel is called dark or the invalid pixel. On the off chance that the pixels of both the layers are distinctive, the overlayed adaptation will be totally dark. This is called a data pixel [6].

Also, two layers are created out of which one layer named as transparent layer (layer 1) that consists of random state, one state out of possible six states. Further, layer 2 is similar to layer 1 except that the payer 2 has exactly opposite pixel states from layer 1. When both the images are stacked one onto another, identical states are shown by gray colour and opposite's states are shown by black colour. There are different ways to apply system of pixels. Four sections are made in each pixel, where two sections are also be made in the form of rectangles or circles in any direction horizontally or vertically. Pixel systems are of various types having good resolution, better contrast or colour pixels. Pixels of layer 2 are dependent on layer 1 pixels in such a way that, if layer 1 pixels are actually random than the layer 2 pixels (empty and information pixels) also contains random pixels. The colour of layer 2 pixels cannot be known until the state of layer 1 pixels is not known. According to the Information theory, absolute secrecy is obtained, if all the requirements for randomness are fulfilled [3]. To use visual cryptography for sharing secure images, one or more random layers have to be sent by transmitter to the receiver in advance. To send a message, sender generates another layer, named layer 2 and sends it to receiver along with layer 1. The secret information is revealed by aligning the two layers, no encryption device or calculations are needed. The system is robust that doesn't break easily.

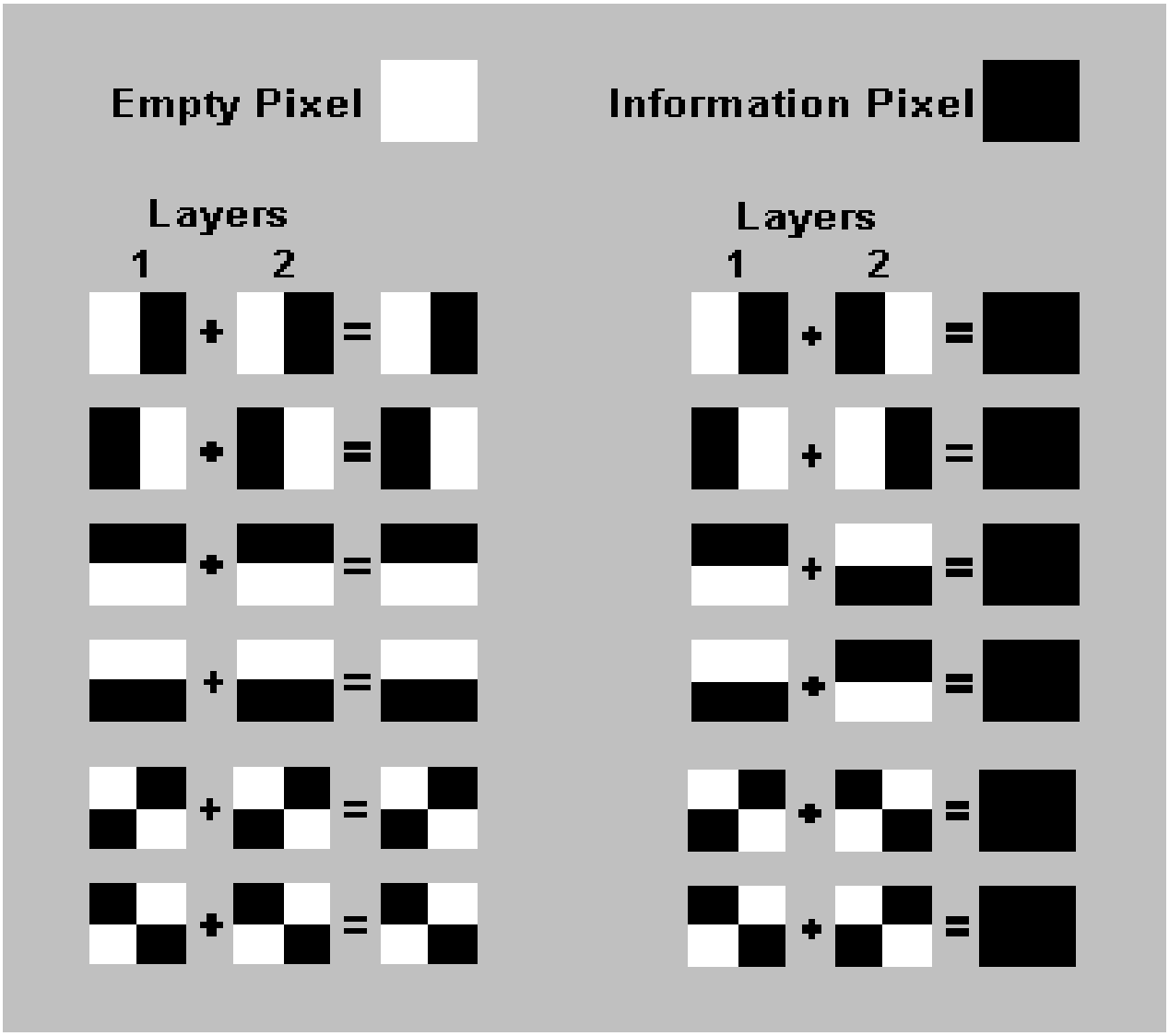


Figure1.7 Methodology of visual cryptography

1.8.2 Advantages of visual cryptography:

Visual cryptography provides great secrecy. Decryption is so easy, that there is no need of any machine and any computer to detect the data at the receiver end. Visual cryptography allows the information to travel with the secured way. It is very simple to implement. Encryption doesn't require any tough algorithm for decryption. Even the high computational power of attacker cannot predict the secret message in visual cryptography. One can send cipher text through fax, e-mail or any means of transport. Decryption algorithm is not required in Visual Cryptography. So, one can decrypt the message even without having the knowledge of cryptography.

1.8.3 Applications of visual cryptography:

There are number of applications where VC can be used. Few are explained as follows.

- Bank customer identification: It mainly deals with Image Processing and the Visual Cryptography. The signature of the candidate is processed in such a way that, they are taken as input and are divided into different number of shares depending upon the banks scheme. One share is preserved in the bank and all other shares are given to the applicant for the future use [2].
- Anti spam-bot measure: Visual cryptography is a method to encrypt a secret image into n shadow images called shares. The recovered secret image can be either darker or the lighter than the background. The secret data or secret information is hiding in the image using several encode and decode technologies [2].
- In electronic voting machines: Visual secret scheme is also used in voting system. The end to end systems often employ cryptographic system to make receipts that are allowed voters to verify that their votes were counted as cast [5].
- Coloured digital watermarks: To copyright, various colour digital watermarks have been widely used in the market [6].

1.8.4 Overheads:

Cryptography provides us a solution to secure our data but at the same time, it has number of overheads which are as follows:

Financial overheads: We need greater amount of money to keep our private data secured from the hacker [3].

Less amount of Channel bandwidth: The user has been able to utilize only the limited amount of bandwidth due to the presence of additional bits caused by keys [2].

Power Consumption: The powerful processors consume more power during the key generation process, charge sharing and the leakage current exists in this model. These factors are responsible for the loss of the data and cause node failure. [3]

Delay: The process of encryption always make some delay to convert the plain text into cipher text which. Few of the encryption algorithms also require additional padding techniques [3].

1.9 ORGANIZATION OF THESIS:

In this thesis, starting from the basics of cryptography through the advancements in the field of Visual Cryptography is discussed. The aim of this work was to design an approach that can add more data security to our system and easier to implement. There is a proposed visual cryptographic algorithm based on the natural sharing of image which drives the thesis and is discussed in chapters 3. Following is the outline of this thesis and the main contribution of each chapter:

- In Chapter 1, briefly discuss the introduction of cryptography, various attacks and encryption algorithms and visual secret sharing.
- In Chapter 2, work done by various researchers has been studied to observe the best possibilities; so as to find the gaps in studies and then to draw problem formulation. This section mentions some of the relevant papers that helped in achieving the targeted results.
- In Chapter 3, the proposed methodology of the NVSS technique has been discussed. All the processes like feature extraction, encryption has been done in this chapter.
- In Chapter 4, the results of all the operations done on the images of different formats, their thresholding values, PSNR values and final encrypted results have been discussed.
- In Chapter 5, the concluding remarks and the future scope have been discussed.

Proposed Scheme has been depicted in figure 1.8 initially, three images have been taken. First is secret image, which we have to share in secured manner, then second image is hand-printed image, it could be any image for handmade painting or any landscape image. Third image is digital image. The size of the printed image and the digital image should be same. So, to equalize the size of both images the pre-processing is done on the images. In Image Pre-processing the image is pre-processed that input image by cropping it. The process of cropping is easily performed by manual and then is stored.

After the pre-processing process of that image, the feature extraction has been done by the process known as binarization process. It is performed after the calculation of the median value of the natural share. With the binarization result the stabilization has also been done. Then, after the feature extraction we will do pixel swapping to add more security to our secret image. After encryption the data will be done by the technique called steganographic technique. Steganography is designed to be hidden from a third party. Then, the final image will be shared with the authorized user. After doing decryption the result image will be revealed.

1.10 RESEARCH METHODOLOGY:

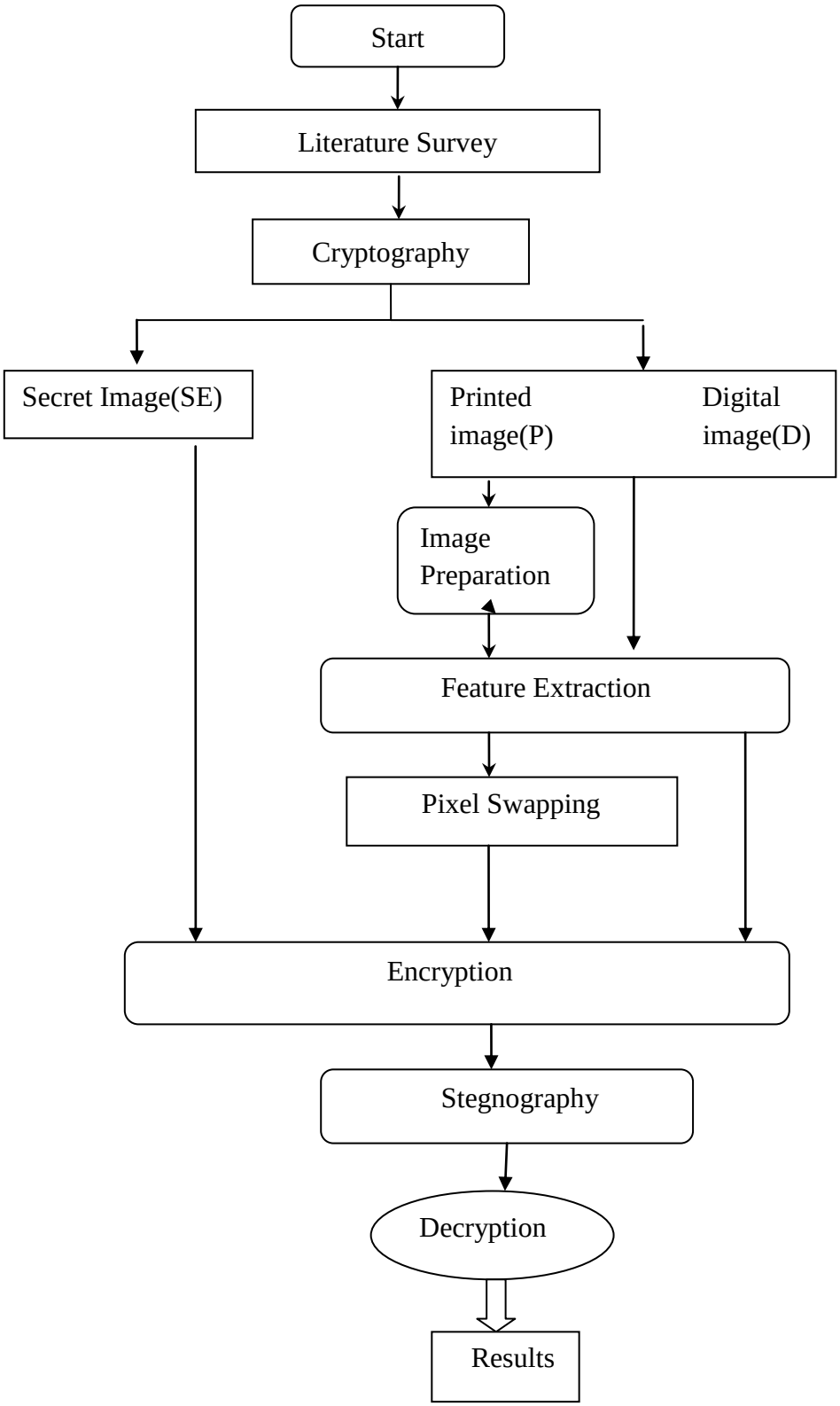


Fig. 1.8 Research methodology

CHAPTER 2
LITERATURE REVIEW

In this section, proposed work and techniques in the field of cryptography for data security carried by various research scholars has been explained. Literature survey has been divided into two parts. First part is carried out by considering the key papers in data encryption, and second part been considers the papers in visual cryptography. Various observations have been drawn the from the literature survey and objectives of thesis work have also been started and listed at the end of this chapter.

2.1 LITERATURE SURVEY:

2.1(a) DATA ENCRYPTION:

Vercauteren Frederik *et al.* [6] had taken a shot at current blame assaults against open key cryptography. They concentrated on customary plans like RSA and furthermore they exhibited the principal examination concerning the security of blending based cryptography against side-channel assault. There was an open issue in setting of pairings, if that bend parameters were mistaken.

Cheraghi Abbas *et al.* [7] had investigated the best pixel expansion from the various models of visual cryptographic schemes. In such type of a model, minimal qualified sets could easily recover hidden image and that image could be darker or lighter than the background of the image. They also presented a lower bound that depended on a coordinating of hyper chart of qualified sets, for the best pixel development of that model and the old customary model of visual cryptography plot acknowledged by the premise lattices. At last, they examined the structures in light of charts and they also displayed an upper destined for the smallest pixel extension as far as solid chromatic list.

Gonzalo R. *et al.* [8] proposed a method to construct meaningful binary images using hyper graph colorings via visual cryptography. If the shares were xeroxed into the transparencies, the hidden image would be visually decoded by superimposing all the subset of transparencies, but no hidden information would be obtained by super positioning of a forbidden subset. It constructs meaningful binary images but the visual quality was poor.

Kakkar Ajay *et al.* [9] worked on optimised way of using encryption techniques and multiple keys with less number of overheads. They have successfully achieved more secured

communication model with multiple short length keys, short length keys are easy to hack and; therefore, multiple keys were used.

Ma Kun *et al.* [10] proposed a technique named simultaneous blunder discovery (CED) scheme which was utilized to counter blame based assault against the RSA. CED plot had such a large number of favorable circumstances; for example, they had extremely solid imperviousness to the blame assaults and little measure of time overhead. They did not have the capacity to counter the exact assault; additionally it neglects to recognize a blame, if the message was zero.

Zhou Zhi *et al.* [11] worked on a halftone visual cryptography. The obtained visual quality results were better than any other available VC method. This technique was based on the new principle called blue-noise principles, the void and cluster algorithm were also utilized to encode a binary image into n halftone shares carrying useful visual information.There was a tradeoff between the halftone shares quality and the contrast of the secret to be decoded. It was better than other methods and could be broadly used in a many visual secret sharing applications.

Kang InKoo *et al*. [12] chipped away at the different techniques in the writing survey indicates better outcomes for the white and dark VC plans; in any case, they were bad to be connected specifically to hued shares because of various shading structures. This paper presented the idea of visual data pixel synchronization to accomplish a shading visual cryptography encryption strategy that produces important shading imparts to high visual quality. It was watched that there was a tradeoff between difference of encryption offers and the unscrambling share; nonetheless, one could perceive the brilliant mystery messages having even low differentiation.

Ross Arun *et al.* [13] worked on a private face image n which they were stored in two different databases such that the hidden image could be revealed only when both of the shares were available at the same time, The private image was not revealed by overlapping the individual share. It was observed that the reconstructed images were very similar to the original secret image.

Zeng Wenjun *et al.* [14] introduced new methods to perform the encryption of compressed type of digital contents that maintain a large amount of syntax compliance after their content

was secured. Experimental result indicates that the use of different edge detectors impacts the performance of the proposed VSI and that VSI-Canny demonstrates outstanding and stable performance.

Wang Xiang *et al.* [15] worked on a lossless tagged Visual Cryptography scheme. In the tagged visual cryptography (TVC), the tagged image was hidden into randomly selected shares. There was distortion in the shares by encoding. They proposed the probabilistic method which had solved the security problem of LTVC. Finally, the perfection of the proposed scheme was experimentally verified. Experimental results indicate that the use of different edge detectors impacts the performance of the proposed VSI and demonstrates stable performance.

Kang InKoo *et al*. [16] demonstrated better results for the white and dull VC arranges; regardless, they were awful to be associated particularly to tone offers in light of different shading structures. This paper displayed the possibility of visual information pixel synchronization to fulfill a shading visual cryptography encryption procedure that produces vital shading confers to high visual quality. It was watched that there was a tradeoff between contrast of encryption offers and the unscrambling share; regardless, one should observed they splendid secret messages having even low separation.

Kai-Hue Lee *et al.* [17] taken a shot at the issue of the ordinary visual mystery sharing plans which was settled by utilizing expanded visual cryptography conspire (EVCS). This approach would be advised to exhibitions than those proposed in different inquires about as far as the show quality. In non PC supported decoding conditions, the approach could be utilized for paired mystery pictures. There was a development issue of VCS for general get to structures as a scientific advancement issue with the end goal that the issue could be fathomed by improvement procedures. The exploratory outcomes show that an answer for the pixel extension issue of the EVCS for GAS's was practiced. In addition, the show nature of the recuperated picture was near that acquired utilizing traditional VC plans.

Askari Nazanin *et al.* [18] proposed a technique VC that was mainly developed for binary images. It presented new methods for halftone images. They function without any pixel expansion, with the better visual quality of recovered hidden image. While also maintained a large amount of security of that original approach which then demonstrates two main applications of VC on the halftone images, first application in the multiple VC, and the other

in the extended VC. Both the applications work without any pixel expansion and with the better amount of visual quality of recovered hidden image as compared to earlier approaches.

Xiang Tao *et al.* [19] proposed a novel VSI based on the human visual system (HVS). VSI exhibited high performance and stability on low-quality images. Experimental results indicate that the use of different edge detectors impacts the performance of the proposed scheme. The VSI evaluates two aspects of the content similarity between plain and encrypted images: the edge similarity extracted via multithreshold edge detection and the texture similarity measured by means of the co-occurrence matrix. These two components were further integrated to obtain the VSI through adaptive similarity weighting.

Nung-Ching Yang *et al.* [20] studied about the *(k, n)* visual cryptographic scheme. This technique was used for encoding the hidden image into the n shares or shadow images which was distributed among the entire n participant. When any of them wanted to reveal that secret image they superimpose their transparencies over a projector. In this way, the secret image which was hidden could be easily visually revealed by a human visualization without any complex computation.

Mitsugu *et al.* [21] they had hypothetically examined the connection between the two plans which were unequivocally secure and feebly secured plans and exhibited two new developments of WS-VSS plans for hued pictures, this security which was extremely powerless was exceptionally successful when aggressors could not utilize PC frameworks. It might require a great deal for message to mixes. It was watched that the proposed plans could be viewed as incline VSS plans for shaded mystery pictures.

Chen Yu-Chi *et al.* [22] analyzed CPVSS scheme proposed by the Hu–Tzeng [48] and proved that it was not cheating immune. They additionally analysed an improvement over the plan that helped them to beat that issue. The objective was to discover shortcomings in a cryptographic plan. In this way, cryptanalysis was very necessary. Actually they analyzed a scheme called cheating-prevention scheme in VC and have shown that it was not cheating immune.

Liu Feng *et al.* [23] proposed a step construction technique to construct VCS for general access structure by applying (2, 2)-VCS, in which a participant may receive multiple share images. This scheme was applied on a technique to simplify the access structure, which could

reduce the average pixel expansion (APE) in most of the cases compared with most of the results in the literature. So, there was an open problem to efficiently partition the access structure to reduce the APE.

Zhang Liang *et al.* [24] dealt with JPEG2000 compact pictures, it was important to broaden their concealing limit on the grounds that the accessible repetition was excessively constrained. Piece stream truncation makes it hard to shroud data. They proposed a steganography plan of high-limit with regards to the JPEG2000 standard framework, which utilizes bit-plane method twice to take care of the issue of truncation. Furthermore, inserting focuses and their power were resolved in a very much characterized quantitative way by means of repetition assessment to build concealing limit. This work was for the most part centered on managing two issues initially was bit stream truncation and other was repetition estimation.

Li Bin *et al.* [25] worked on the multiple base notation system steganography in which hidden data was converted into different symbols in a system with multiple bases called notational system. All the pixels of that host image were then modified in such a way that when the pixel values were divided by the bases and also their remainders were equal to symbols of the hidden image. Based on their observation, they proposed a steganalytic approach which was effective in not only detecting MBNS steganography but also estimating its embedding rate. They also tried to estimate the message and attacking the possible versions of the MBNS steganography.

Huang Chun-Hsiang *et al.* [26] proposed another procedure that was inconspicuous watermarking. In UVW plans, hidden data could be inserted and afterward specifically extricated utilizing the ordinary human visual framework. They likewise embraced visual cryptographic methods to monitor the security of shrouded data and, in the meantime, increment the functional estimation of visual cryptography..

DaoshunWang *et al.* [27] proposed two plans one was a probabilistic $(2, n)$ conspire which was for paired pictures and other one was deterministic (n, n) plot for all the greyscale pictures. Both of the plans utilize straightforward boolean operations and the two have no pixel extension. The principal conspire $(2, n)$ plot gives preferred difference over other and it had essentially littler regions than different strategies. Though the (n, n) conspire gives a correct reproduction.

Wu Xiaotian *et al*. [28] had abused a portion of the properties of XOR based VC. XOR based VC has two calculations which were XOR based VC for the general to get structure and versatile area increasing XOR-based VC. The XOR based VC calculation expects to execute entangled sharing utilizing GAS, while keeping up every one of the benefits. No pixel extension, consummate remaking of mystery and furthermore no code book were required. In another calculation, the main idea presented was of versatile security level, in which the security levels were recouped by the qualified sets rather than the amount of stacked offers.

Hajiabolhassan Hossein *et al.* [29] had researched the pixel extension of various models of visual cryptography plans. In such kind of model, just insignificant qualified sets were utilized to recoup the mystery picture and the recuperated mystery picture would be darker or lighter than the foundation. They presented both a lower bound, in view of an instigated coordinating of hyper chart of qualified sets for the best pixel extension of the previously mentioned showed and the conventional model of visual cryptography plot acknowledged by premise frameworks.

Wang Dao-Shun *et al.* [30] had proposed a new greyscale nRVCS with and had deal with the biggest problem which was minimum amount of pixel expansion and then proposed a greyscale RVCS by using matrices of perfect black nRVCS visual cryptography scheme. In normal encryption technique, recovering a secret image did not require any complex calculation. However, the contrast of the reconstructed image could be quite low. Also, but by this technique, they proposed an optimal GRVCS even though the basis matrices were not perfectly black. Finally, they designed an optimal-contrast GRVCS with a minimum number of shares held by each participant.

Blundo Carlo *et al.* [31] analyzed a scheme called visual cryptography in which black pixels were perfectly reconstructed, means all the sub pixels which were associated to black pixels were black. They had shown that a suitable linear programming problem was used to compute the minimum pixel expansion. Also they gave a construction for $(3, n)$thresholding scheme and a construction for $(n$ ÿ $1, n)$threshold visual scheme.

2.1(b) VISUAL CRYPTOGRAPHY:

Cimato Stelvio *et al.* [32] demonstrate how to develop VCSs where high contrast pixels were superbly reproduced. Furthermore, every member needed to store a specific number of offers,

in which each of them having an indistinguishable number of pixels from the first concealed picture. Likewise their plans had no assurance of loss of determination, and the remade picture was same as the first concealed picture. By comparing this plan to the plans of Viet and Kurosawa [10] had found that their plans require every member to store an exceptionally littler measure of data.

Hou Young-Chang *et al.* [33] worked on the colour decomposition method, past studies in black-and-white visual cryptography and on the halftone technology were the three methods proposed by them. Their methods were helpful not only in retaining the advantages of black and white visual cryptography, but also had the backward compatibility in black-and-white visual cryptography, and could be applied to gray-level and colour images easily.

Lukac Rastislav *et al.* [34] proposed a new method for sharing secrets. This method could protect an image data by analyzing B bits per pixel. In this study, decomposition/stacking technique were used to generate B bit shares. Further, decryption was successfully performed for the final result.

Shyu Shyong Jian *et al.* [35] proposed a technique based on random grid. 2-D array of pixels was used which consists of transparent and opaque pixels, distributed randomly. Random grid approach was utilized to achieve the encryption. The data set used for encryption included gray and colour images. The algorithm was designed in such a way that the information included in images was kept secret, until both the images were superimposed.

Fang Wen-Pinn *et al.* [36] proposed a technique for encryption, in which the advantages of visual sharing and cryptography were combined. The technique was lossless and fast as compared to previous techniques and it was capable of distinguishing the group from the friendly meaningful shares.

Yang Ching-Nung *et al.* [37] proposed a technique in which a secret pixel was represented by several numbers of colour sub pixels in which sub pixels were used to refer pixel expansion. A new CVCS technique was then proposed after studying addition which pixel expansion was improved as compare to previous but contrast quality was reducing in this technique.

Feng Jen-Bang *et al.* [38] proposed a technique to share more than one image, in which functions were indicated using a graph of secret pixels and share blocks. Visual patterns

generated from the graph were used to generate secrete images. Further, the images were decrypted by using the stack of images at different angles. The technique was able to achieve high efficiency for sharing more than one image.

Lou Der-Chyuan *et al.* [39] proposed a method in which the secret image could be shared along with another image by encryption. Further, to see the secret image, both the images had to be superimposed to unhide them. The proposed technique was cheaper than the technique used by Fang and Lins [55] also the efficiency came out was higher.

Tzung-Her Chen *et al.* [40] proposed a different technique based on threshold RG, VSS scheme. Although, the proposed technique was performed for the first time but the experimental results showed that the technique was good enough to give the better results than the previous techniques. Pixel expansion was avoided in this technique and also no codebook was used.

Chen Tzung-Her *et al.* [41] proposed a method to generate a better visual quality of images by reconstructing the images by redesigning the images to achieve higher level accuracy. The efficiency came out to be good enough to unhide the secret image with better quality of image, having good visual effects.

Guo Teng *et al.* [42] proposed a method which was succeeded in improving the contrast of the threshold scheme. Experimental results showed that the technique out performs better than the previous technique in terms of visual quality. Although, the exact technique was not known properly and its problem is in further study till now.

Chen Tzung-Her et al. [43] proposed a method in which secret image was not only kept hidden but capacity of sharing image was also increased with the help of a multisecret image sharing technique which was based on Boolean. Instead of $2n$ share images, n secret images were hidden by the means of $n + 1$ shared image. This technique had many benefits like easing the management overhead of meaningless share and reducing the demand of image bandwidth of transmission.

Wu Xiaotian *et al.* [44] proposed two algorithms to improve the reconstruction image quality first was RG based VSS and the second was void and cluster based pre processing. As a result both the techniques over much more enhanced visual quality. By using the RG based

VSS optimal contrast was achieved and by applying the VAC post processing method, a more even reconstructed secret image was obtained.

Lin Chang-Chou *et al.* [45] a dithering technique was used to construct the share instead of using gray sub pixels. After that to accomplish work of creating shares, the existing cryptographic schemes for binary image were applied. The major advantage of this technique was inheriting any developed cryptographic technique.

Yang Ching-Nung *et al.* [46] proposed a new scheme in which contrast of recovered image was shown by using the frequency of white pixels. This scheme was easy to implement on the bases of any VSS scheme, and it was non expansible; the size of shadow and the original image was the same. The contrast level of this technique was same as that of VSS scheme. The conventional VSS scheme could be transferred to general VSS scheme by using transfer operations.

Yang Ching-Nung *et al.* [47] used the number of extra sub pixels which were reduced to construct the ratio invariant schemes. Any arbitrary value was used to represent a pixel. The secret image was a circle; sub pixels were not a square valued i.e. the aspect ratio was changed. Then circle was changed into ellipse lead to loss of the data hidden in secret image.

Blundo Carlo *et al.* [48] considered visual cryptography plans fulfilling the model presented by Tzeng and Hu [28] another approach used for visual cryptography, designs, codes and cryptography. In such a model, the recouped mystery picture could be darker or lighter than the foundation.

Wong Fu-Hsiang *et al.* [49] attempted to build up some presence hypotheses of positive answers for the accompanying arranges nonlinear boundary value issue. A lot of work was done to examine the positive arrangements of the two-point boundary value problem for differential equations which were utilized to explain various physical, natural and concoction phenomena.

Chung Kuo-Liang *et al.* [50] presented a new finite state machine model (FSMM)-based search method to speed up the existing algorithm significantly while preserving the same image quality as in the algorithm. The observation, indicates that the sliding window for the algorithm moves from left to right one position; therefore, one output column and one input

column which were introduced at each step. Thus, a simple finite state machine could track the transitions from the current window movement to the next state.

Huang Win-Bin *et al.* [51] proposed a technique for half toning and inverse half toning which was based upon hybrid neural network was presented. A single-layer perception neural network was used to perform halftone image and by using radial-basis function neural network, its corresponding continuous tone image was reconstructed. The corresponding continuous tone images and the halftone images were produced at the same time.

Huang Yong-Huai *et al.* [52] the two highly improved algorithms which were discovered called LiH algorithms. Firstly, a vector and a lookup based IH algorithm was presented called VLIH algorithm. Using this, the image quality was improved. In the previous algorithms the LUT was built up only by utilizing gray value of pixels. VLIH and TVLIH when compares to previous LiH algorithms their experimental results demonstrate the quality advantage.

Wu Xiaotian *et al.* [53] proposed a new technique in which secret image was recovered by two methods. First, secret image was reconstructed by directly stacking the shares when computational devices were not available. Second, the hidden image was decrypted easily by applying XOR operation when some light weight computational devices were available. It was analysed that the image quality of the hidden image which was produced by stacking operation was same as that of the VSS, but the visual quality obtained was better by XOR operation.

L. Lau Daniel *et al.* [54] proposed two new techniques which were for colour halftoning. In first technique error was defused with feedback depending on output, where overlapping of coloured pixels could be used for increased colour control. The second technique was an array designed to create green noise halftone patterns using a green-noise mask which was constructed for overlapping of different coloured pixels. The process of optimal colour reproduction was not presented in this paper.

Kim Sang Ho *et al.* [55] proposed a technique called the human visual system which was an important component of many halfoning algorithms. Their halftoning texture quality provided by 4 different HVS models was compared by using the iterative direct binary search. The computational performance was improved while there was little increase in complexity of code by using the approximation to this model. After analysing many parameters of this

model, the results were ready to show that it was possible to tune it to gray level and thus got better halftone quality.

Wang Yong *et al.* [56] discovered applications in which many researches were attracted to JPEG and its detection becomes also important. There were some blind steganalysis methods, but they were either time consuming or unreliable. In this paper, a popular JPEG algorithm was detected by using very efficient steganalysis scheme. A correlation of the DCT coefficients in multidirections was described by construction of a novel kind of transition probability matrix.

Lin Chang-Chou *et al.* [57] chipped away at an (k, n) edge visual cryptography plot that was proposed to encode a mystery picture into n shadow pictures, where any k or a greater amount of them could outwardly recuperate the mystery picture. However, in the event that there were $k-1$ or not as much as k then they pick up no data about it. The unravelling procedure was same as that of an ordinary visual cryptography plot, which varies from conventional mystery sharing, did not require any convoluted cryptographic calculations and calculations. Rather, it could be decoded effectively by the human visual framework.

Liu Qingzhong *et al.* [58] proposed another plan for steganalysis of JPEG pictures, which been the most well known picture arrange, it was accepted to be generally helpful with the end goal of steganography in light of the fact that there were such a large number of free devices for delivering steganography. Firstly, Markov [8] way to deal with the between square of the discrete cosine change and to DWT was extended and afterward the components on the joint conveyances were extricated. Those elements were known as unique expanded features. After that the components were additionally removed from aligned adaptation known as EPF elements. The distinctions between both systems were figured and after that the first EPF and their distinction was converged to shape highlight vector.

Chung Kuo Liang *et al.* [59] presented novel edge based method which was for reverse half toning in which the quality of the gray image after reconstruction was improved. The LUT-based inverse half toning method was used as a pre-processing step to transform the image to a base gray image, then after that the edge of image were extracted and then classified from the base gray scale image. This study and results had demonstrated that the ELIH had a better image quality as compared to the previous LIH. Their research issues were to build up more versatile edge types.

Kim Hyoung Joong *et al.* [60] studied and proposed a scheme while keeping the distortion at the same level; new expandability could achieve more embedding capacity keeping distortion at the same level. And also more capacity was achieved by using different methods of expansion. As a result, the performance of the scheme and the results were better than the scheme developed by Tian [20].

Wang Zhongmin *et al.* [61] discovered a new method which was HVC construction basically based on error diffusion. The image that was hidden was embedded into binary valued share. Halftone shares were produced in good quality and also their error diffusion had low complexity. A reconstructed hidden image produced by stacking the shares, did not suffer from cross interference.

Chen Tzung Her *et al.* [62] mainly focused on a scheme called novel RGVSS which was clearly based on the pixel values of the logo value. The two main advantages of this technique were it did not suffer from pixel expansion problem. The second advantage was its user friendly nature. The formal analysis was demonstrated in order to illustrate its correctness.

Chiu Pei Ling *et al.* [63] worked on approach called a pixel expansion free threshold VCSs scheme which was based on an optimised technique. The evaluation of the display quality of the recovered images, they considered blackness as a performance. In order to maximize the image contrast and blackness constraints, they formulated a mathematical optimization model.

Jo Jinyong *et al.* [64] proposed a technique for incorporate the emerging SDN paradigm. This technique was called in home consumer electronic devices. Very high degree of flexibility was provided for intra home networking as well as wider connectivity for inter-home networking. The issue of the completeness of the CE devices was to be raised besides SDN-centric challenges, by generalizing AD message types for their future scope.

Hou Youthful Chang *et al.* [65] proposed a new plan in which the likelihood for either dark or white pixels of mystery picture to show up as dark pixels on the offers was the same, which approximates to $1/n$. In this way, nobody could get any concealed data from a solitary

offer, consequently security was expanded. The stacked picture would be effortlessly perceived by human eyes with no challenges, in regards to the size and the security of offers.

Zhang Lei *et al.* [66] had concentrated a visual understanding by means of a recently proposed technique which was standard based multi-highlight shared learning structure. There were a few points of interest of this technique, it incorporate the accompanying the complex data structure data of each element which was misused in realizing. It was bringing about a more dedicated arrangement owing to the worldwide mark consistency, a gathering diagram complex regularize in view of the Laplacian and Hessian regularization was developed and an effective enhancement technique was presented as a quick solver owing its speed to raised sub issues.

Chen Yu-Chi *et al.* [67] studied that there was another method than region incrimination which was called multi-secret VC, called fully incrementing visual cryptography. Visual cryptography (VC) was a variant form of secret sharing. The old methods like visual cryptography (RIVC) were reoffered as another kind of multi- secret visual scheme. RIVC characterizes s layers and takes s secrets, and after that inserts every secret into each layer. Their expressing point was to propose another idea of non-monotonic visual cryptography (NVC) for human vision framework as a primitive to develop FIVC. They also show a perfect development of basic NVC which depends on a slightly unreasonable presumption. Based on the NVC, there were couple of strategies to broaden the usefulness for complicated instances of NVC.

Lee Kai-Hui *et al.* [68] proposed a general way to deal with address issues without advanced codebook plan. This approach was mainly used for two fold mystery pictures in non-figure struck decoding conditions. This approach was to keep away from pixel extension. They composed an arrangement of segment vectors to encode mystery pixels as opposed to utilizing the customary VC-based approach. Their trial comes about demonstrate that they showed the nature of the recuperated picture was better than that of past strategies.

Guo Cheng *et al.* [69] worked shadow images with a hierarchical threshold structure was considered and studied. The hidden image was divided into several parts in this scheme and thresholding access structure was also determined with the help of sequence threshold. In this way the hidden image was reconstructed without any distortion.

Lukaca Rastislav *et al*. [70] a new scheme was proposed by which image data coded with *B* number of bits per pixel were protected and the results were analysed. B-bit shares were generated shares by combining bit-level decomposition/stacking with a $\{k, n\}-$threshold sharing strategy. As a result, the perfect amount of reconstruction was achieved. It was also noticed that it was cost effective cryptographic algorithm of image processing.

2.2 OBSERVATIONS FROM THE LITERATURE SURVEY:

From the work done by the various researches few observations have been drawn and are follows.

- A new model is needed to develop which can accept short and long data length sequence both.
- Key should be selected on the basis on the data to reduce the hacking.
- The main parts of key management system will include key generation, key establishment, key distribution and key agreement protocols. Always a strong key is required to protect the system from various attacks.
- A perfect method of image hiding is needed with less number of shares and less complexity and to achieve more security.

2.3 GAPS AND PROBLEM FORMULATION:

For secured communication, it is necessary to use appropriate cryptographic algorithms to provide the required security services. The efficient algorithms require correct protocols for authentication and key management. It is intended to design the available cryptographic algorithm to achieve more security and this will be done by incorporating visual cryptography. Figure1.8 in the previous chapter depicts the proposed flowchart. The proposed approach will be implemented using MATLAB R2013a. The above work have its utility to transfer secret information over web, so that, intruder couldn't detect it.

2.4 OBJECTIVES:

From the previous section, objectives have been drawn and are as follows:

- To study the various Data encryption and visual cryptography techniques.
- To use visual cryptography for transmission of the secret image.
- To use thresholding and binarization techniques to hide the data in the image.
- To use steganography and encryption techniques for more security of digital image.

CHAPTER 3

PROPOSED METHODOLOGY

3.1 IMAGE PREPARATION PROCESS:

The image preparation processes are used for pre processing printed images. As we know, printed image can be any handmade image. It can be acquired by any popular electronics device such as scanner or digital camera. To reduce the difference between the encryption and decryption processes, the resolution and image size should be similar. The hand printed image is drawn on a simple A4 size sheet and to make it digital, we can capture it using popular smart phone like iphone7 or with digital camera. The acquired image as shown in figure 3.1 has been cropped and resized according to our requirements. To equalize the size of the image we can crop the image by a regular manner.

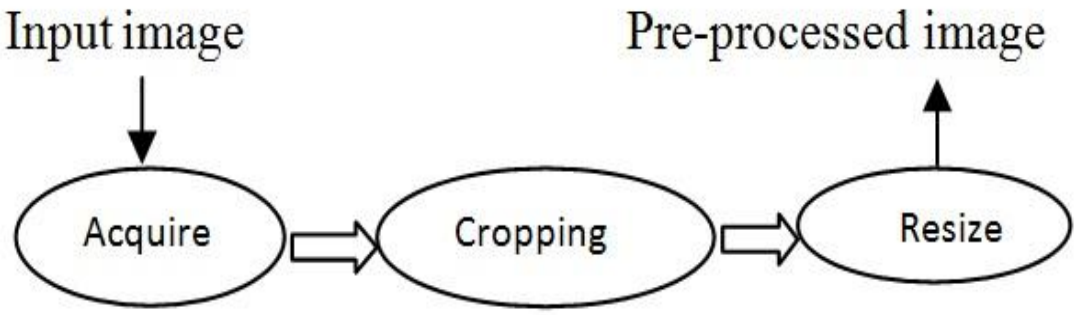


Figure 3.1 Flow diagram of Image Preparation Process

For visual cryptography the proposed algorithm for image preparation process has been shown in figure 3.1. The proposed algorithm for digital image sharing is listed below:

3.2 PROPOSED ALGORITHM FOR DIGITAL IMAGE SHARING

1) Take one digital image (data) of size 512×512.

2) Take a secret image of same format and of same size.

3) Now, take a handmade image or one can use any painting which has been drawn by hand.

4) A picture of handmade image has been taken by any popular Smartphone e.g. I phone 7.

5) For pre-processing of handmade image, cropping of that image has been done. Then, resize it into 512×512 pixels, so it will be equal to digital image.

6) Now, apply process of feature extraction on both digital and handmade images.

7) Further, pixel swapping has been done.

8) Use encryption technique to encrypt all three images into a single image.

9) Now, hide that image with the help of steganography technique.

10) Generated the final image.

11) Decrypt the share using same algorithm in decryption process

(a) (b)

Figure 3.2 Cropping of image

The image shown in figure 3.2 are the images showing the method of pre processing. The image has been cropped to equalize its dimensions with the digital image.

3.3 FEATURE EXTRACTION PROCESS:

In feature extraction process is a process that extracts feature images from the natural shares. The module which is the core module of the feature extraction process is applicable to printed and digital images simultaneously. The feature extraction process consists of three steps. Algorithm for pixel swapping is given by us:

1) Divide N into $b \times b$ pixels.
2) For each block repeat 3-10th step.
3) For all $X1 \leq X \leq X\,b$, $Y1 \leq Y \leq Y\,b$. Calculate the Hxy .
4) Calculate M.
5) Randomly select QS pixels where $fxy = 1$ and $Hxy = M$.
6) Calculate Qc.
7) Randomly select Qc pixels where $fxy = 1$.
8) Randomly select Qc pixels where $fxy = 0$.
9) Output F.

3.3.1 Thresholding:

In the least difficult thresholding strategies, every pixel in a picture is supplanted with a dark pixel if the picture force is not as much as some settled steady T and supplanted by a white pixel if the picture power is more than that consistent. In the image shown in figure 3.3 these outcomes oblivious segment are winding up noticeably thoroughly dark, and the water zone and light part ending up totally white as shown in figure 3.3.

Figure 3.3 Thresholding of image

3.3.2 How thresholding works:

The image which is used as an input image in the thresholding operation is typically a greyscale image or coloured image. In the method the output is a binary image representing the segmentation. Black pixels correspond to background and white pixels correspond to all the lower pixel values. The colour of the pixel in the image is decided by the by a single parameter called the *intensity threshold*. In a single pass, all the pixels in the image are compared with this threshold value. If the intensity of the pixel is higher than the threshold, the pixel is set to white in the output. If it is less than the threshold, it is set to black pixel. We can obtain the intensity threshold by various methods. We can take a mean of all the pixel value from all the pixels and take it as the threshold value and set all the pixels to black and white according to that value. Thresholding is used as pre-processing to extract an interesting subset of image structures which then be passed along to another operator in an image processing chain.

Binarization is done after the thresholding. The stabilization process is basically used in odd pixel images to balance the black and white pixels on the image.

3.3.3 Chaos: In characteristic picture, pixels having the equivalent esteems may bunch together. These grouped pixels may have similar component esteem; henceforth it will prompt the element picture and to the produced that picture uncovering a few surfaces of the normal picture in the consequent encryption handle. The procedure used to take out the surface that may show up on the separated element pictures and the produced offers are called chaos.

The quality of the digital and natural image is determined by considering image quality parameters such as, PSNR and MSE and is shown in table 4.2.

For a $M \times N$ gray scale image, the PSNR value is calculated as the following:

$$PSNR = 10log10\ (255/MSE) \text{ ----------} \quad (1)$$

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

Where $x\ (i, j)$ and $x'\ (i, j)$ are the pixel values of the digital and natural image, respectively and MSE is the mean square error which is given in equation 2.

3.4 PIXEL SWAPPING: Pixel value swapping is the second method of encryption applied on image. It can add more to the security of image. Pixels of any image can be swapped by different ways. Either we can interchange their positions with respect to each other or others algorithms can be used. Original image is taken as shown in figure 3.4; convert it into the grey scale image. Get another image by adding noise to the first image as shown in figure 3.5.

Figure 3.4 Original image

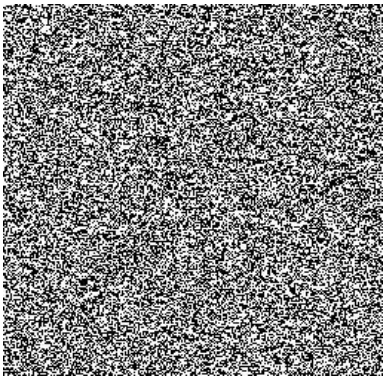


Figure 3.5 Image after pixel swapping

The pixel swapped image is prepared by subtracting the image containing noise from the grey scale image. The resultant image is pixel swapped. We can easily decrypt the image by applying opposite algorithm.

A. Algorithm for Feature Extraction Process

1) Take an image for feature extraction.
2) Find the threshold value of that image.
3) Set the pixel value greater than threshold to 1, and remaining to 0.
4) Now equalize the white and the black pixels of the image, which is called stabilization.
5) For feature extraction of other images repeat all the steps.

200	204	167	240
230	200	250	179
210	169	111	120
225	208	119	233

(a)

0	0	0	1
1	0	1	0
1	0	0	1
1	1	0	1

(b)

1	0	0	1
1	0	1	0
1	0	0	1
1	0	0	1

(c)

Figure 3.6 Example of stabilization technique

In stabilization all pixels are converted into 1 and 0 according to the thresholding value of the pixels as shown in figure 3.6(b). The values are then stabilized according to the neighbor pixels as shown in figure 3.6(c). The uneven pixel value is changed as shown in figure 3.6(c) according to the majority pixels and the image is stabilized

3.5 ENCRYPTION: To secure picture substance, most existing encryption calculations are intended to change a unique picture into a surface like or clamor like picture which is, be that as it may, a conspicuous visual sign showing the nearness of an encoded picture and in this manner brings about an altogether expansive number of assaults. It utilizes a limited arrangement of directions which are just known to sender or beneficiary to change over unique picture into encoded picture. These calculations for the most part required an arrangement of characters called key. By utilizing the key, we can encode and unscramble the mystery picture. All the three images are encrypted here. The digital image, the natural one and secret image is also encrypted. The key is needed to encrypt the images; same key is used by the receiver to decrypt the images.

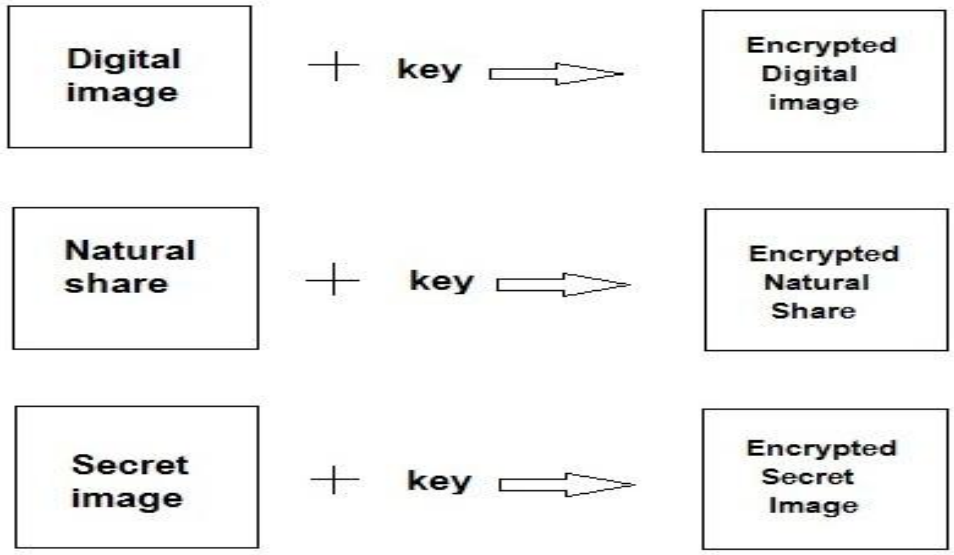


Figure 3.7 Encryption method

From the results shown in figure 3.7, we got three images. One is the encrypted digital share, encrypted natural share and the secret encrypted share. By applying adding algorithm all the three images are added together to form one share. That secret share is then stegnographed.

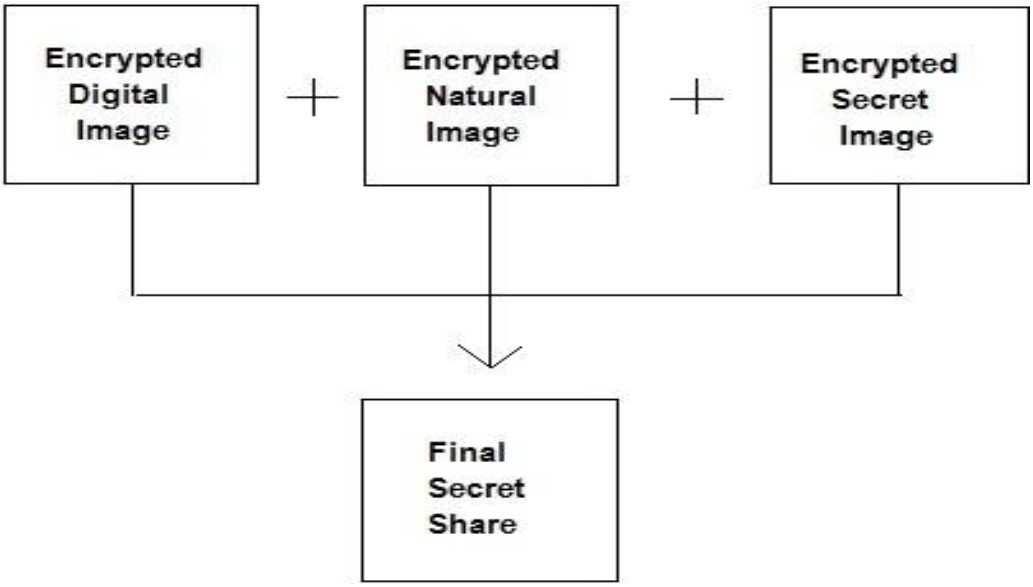


Figure 3.8 Adding of shares

Steganography is method to hide the data or image within image. Steganography is just a type of encryption technique that can be used with the cryptography as a more secured method.We can apply steganography method to images, a video file or any type of audio file.

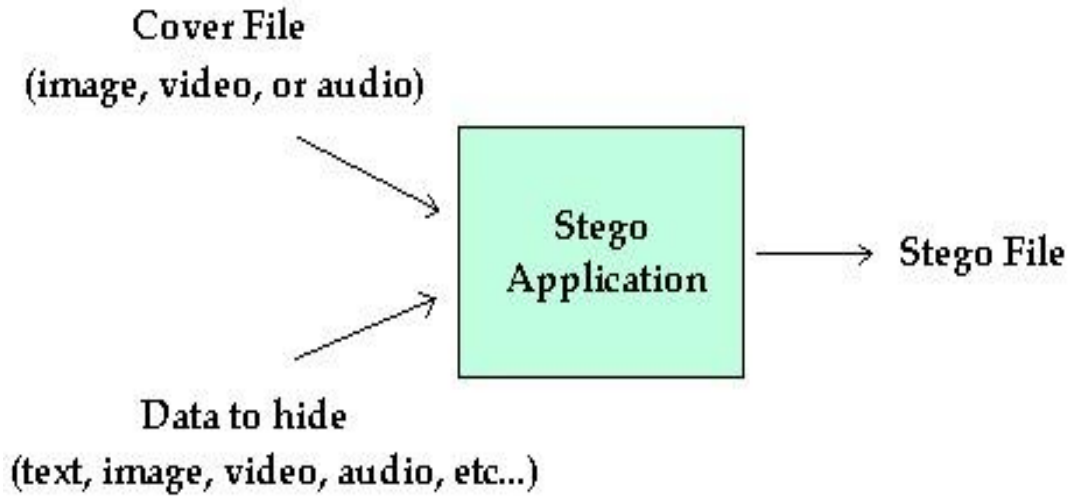


Figure 3.9 Image stegnography

After embedding cover file into hidden image the stegno image is produced as shown in fig 3.9. It protects images or hidden files from pirating copyrighting as well as aiding in unauthorized viewing. The first one is the cover image. The data may be in the form of text, audio or any image. In this case data is in the form of secret image.

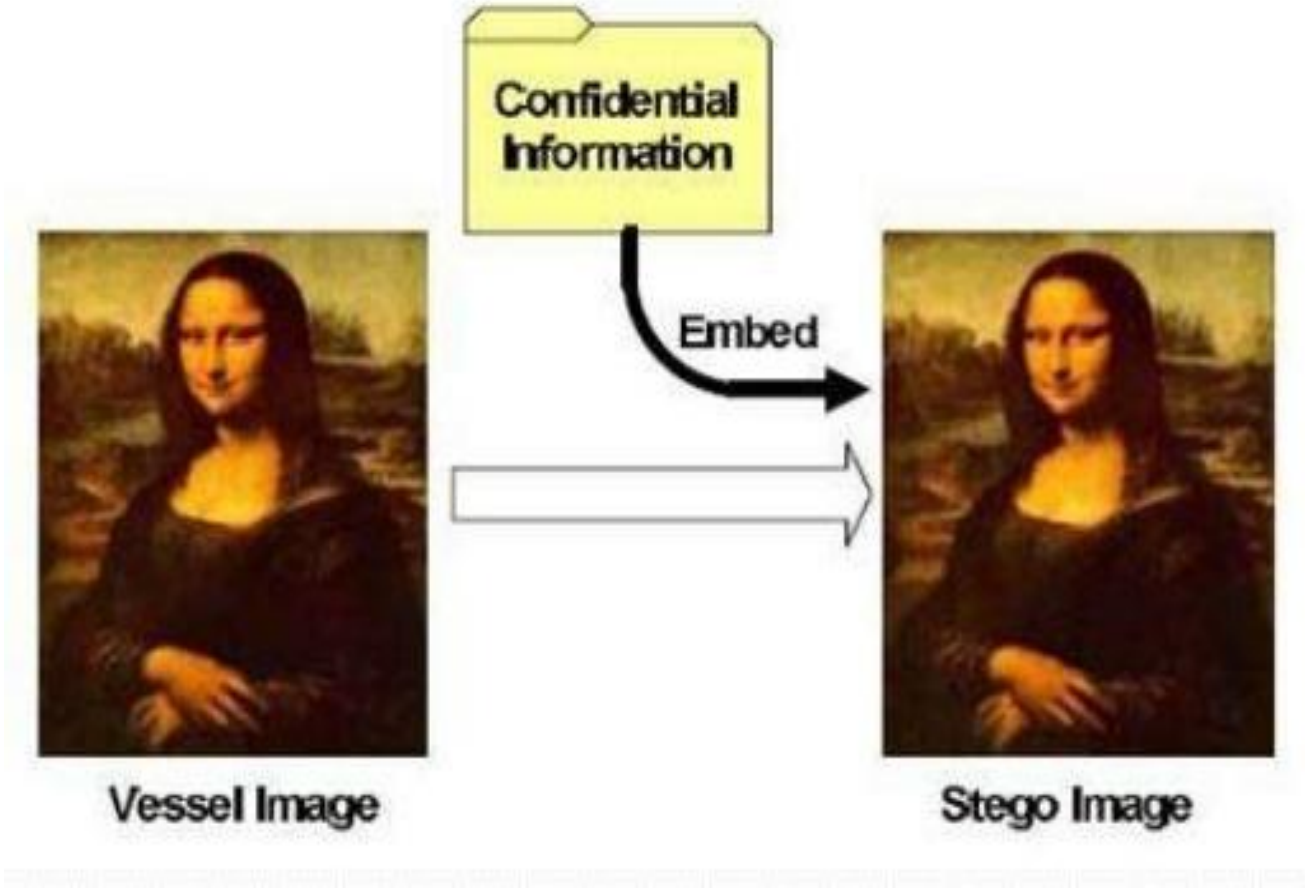


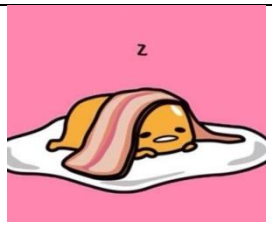
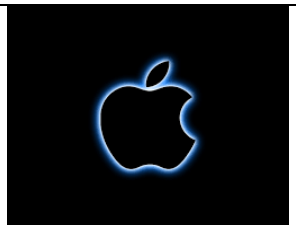
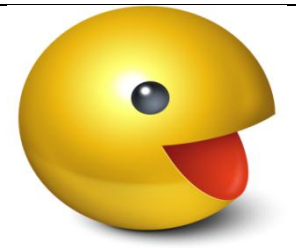
Figure 3.10 Stegnography

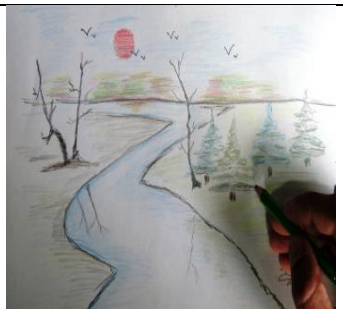
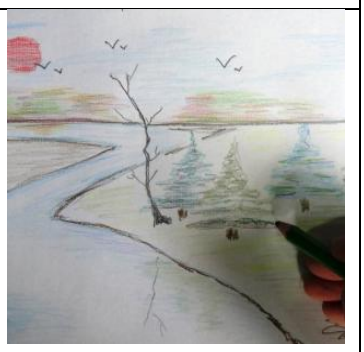
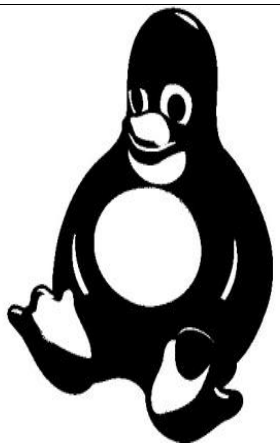
The input is a hidden image which we want to hide. And the other image is cover image in which the secret image is to be hidden. Secret image is embedded into cover image as shown in figure 3.10. There is no perceptual difference between the original and the stenographic image.

CHAPTER 4

RESULTS AND DISCUSSIONS

As explained in flow chart the printed image is pre-processed by the method of image preparation. In this method, the image captured by smart phone is cropped to size (512*512), so that, it becomes equal to the size of digital image. Feature extraction is done on both digital and cropped image. In feature extraction process there are three steps.1) Binarization, 2) Stabilization, and 3) Chaos. To get the binarized image, the threshold value is to be set of these images. The threshold value of image is average intensity value of pixels. So, pixel values which are above threshold are set to be 1, and remaining 0. The threshold for digital image of jpg format is 205. And threshold value for cropped image of same format is 162. All the other threshold values are mentioned in the table 4.1:

	Image Format		
	JPG	***PNG***	***BMP***
Secret image	 (a)	 (b)	 (c)
Digital image	 (d)	 (e)	 (f)

Original Handmade image	 (g)	 (h)	 (i)
After pre-processing	 (j)	 (k)	 (l)
Binarized digital image	 (m)	 (n)	 (o)

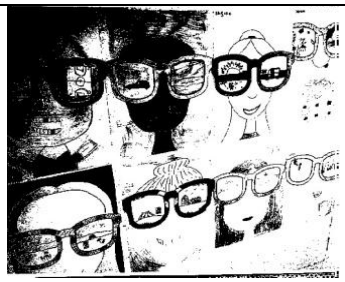
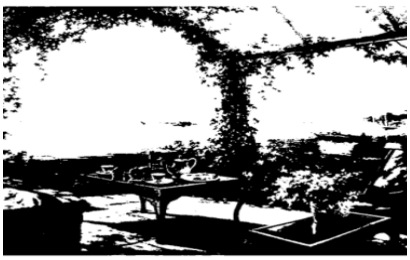
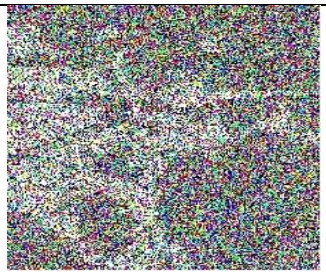
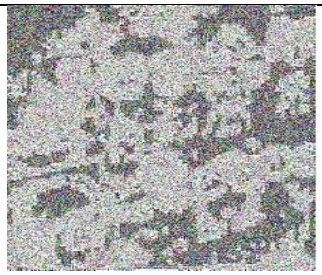
Binarized handmade image	 (p)	 (q)	 (r)
Pixel swapped image	 (s)	 (t)	 (u)

Table 4.1: (a) (b) and (c) are secret images of different formats ;(d) (e) and (f) are the digital images;(g) (h) and (i) are the natural handmade images;(j), (k) and (l) are the images produced after preprocessing;(m) ,(n) and (o) are the binarized images;(p) ,(q) and (r) are the binarized handmade images;(s), (t) and (u) are pixel swapped images.

The comparison between the PSNR's of the both digital and natural image is given in the table 4.2:

	Jpg	Png	Bmp
Digital Image	33.04	28.2	33.00
Natural Image	32.93	27.79	33.07

Table 4.2 PSNR of the digital image and the natural image of the different formats.

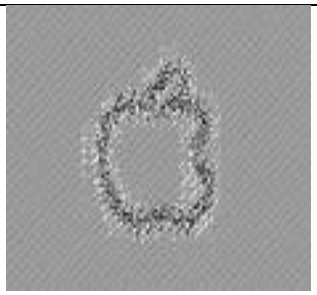
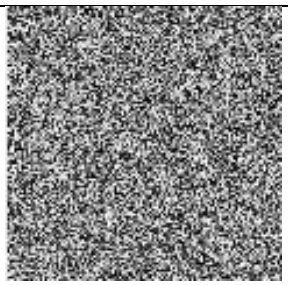
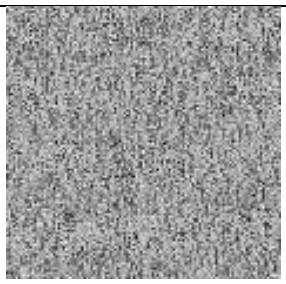
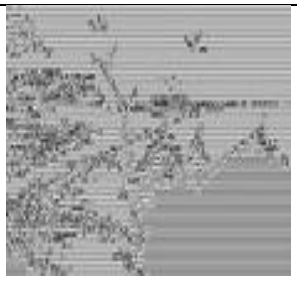
To get the binarized image, the threshold value is to be set of these images. The threshold value of image is average intensity value of pixels. So, pixel values which are above threshold are set to be 1, and remaining 0. The threshold for digital image of jpg format is 205. And threshold value for cropped image of same format is 162. All the other threshold values are mentioned in the table 4.3:

S. NO.	IMAGE FORMAT	THRESHOLD VALUE OF DIGITAL IMAGE	THRESHOLD VALUE OF HANDMADE IMAGE
1	JPG	205	162
2	PNG	145	166
3	BMP	194	167

Table 4.3 Median values of all images of different formats

4.1 ENCRYPTION:

After pixel swapping, the encryption has been done on all the images. Pixel swapping is done only on feature extracted image but encryption has been done on digital image, natural image and secret image too. Results of encrypted images of different formats are given in table 4.4.

	jpeg format	png format	bmp format
Encrypted Digital image:	 (1)	 (2)	 (3)
Encrypted natural image:	 (4)	 (5)	 (6)

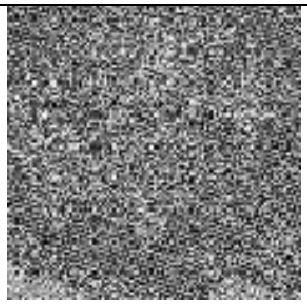
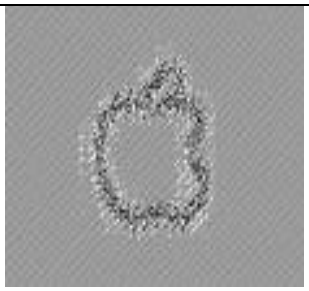
Encrypted Secret image:	 (7)	 (8)	 (9)

Table 4.4 (1) (2) and (3) are the encrypted digital images ; (4) (5) and (6) are the encrypted natural image; (7) (8) and (9) are the encrypted secret image of jpeg ,png and bmp format respectively.

The elapsed time of the encryption process has been calculated and given in the table below:

	Elapsed time		
	Jpeg	Png	Bmp
Digital Image	23.39	0.62	9.03
Natural Image	15.35	11.18	14.85
Secret Image	12.84	16.22	1.44

Table 4.5 Elapsed time of the encryption of digital image, natural image and secret image of jpeg, png and bmp format respectively.

The histogram for the secret image of jpeg format is created. The histogram for the original jpeg secret image and the encrypted secret image has also been created and shown in figure 4.2 and 4.2 respectively.

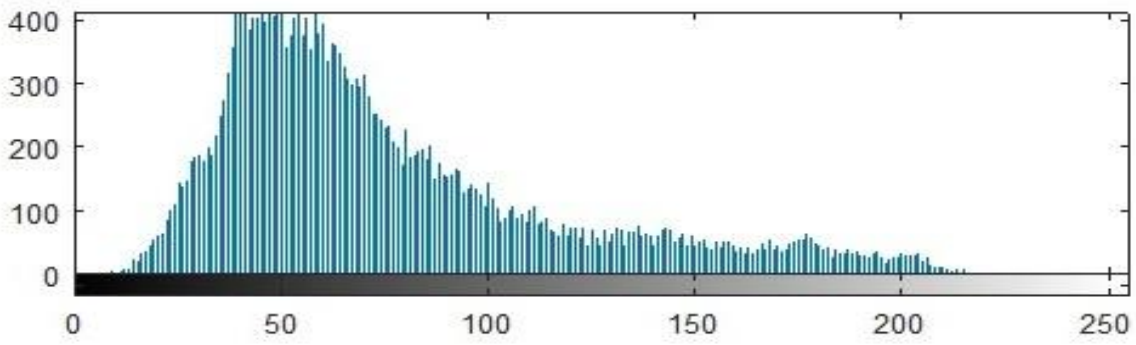


Figure 4.1 Histogram of secret image

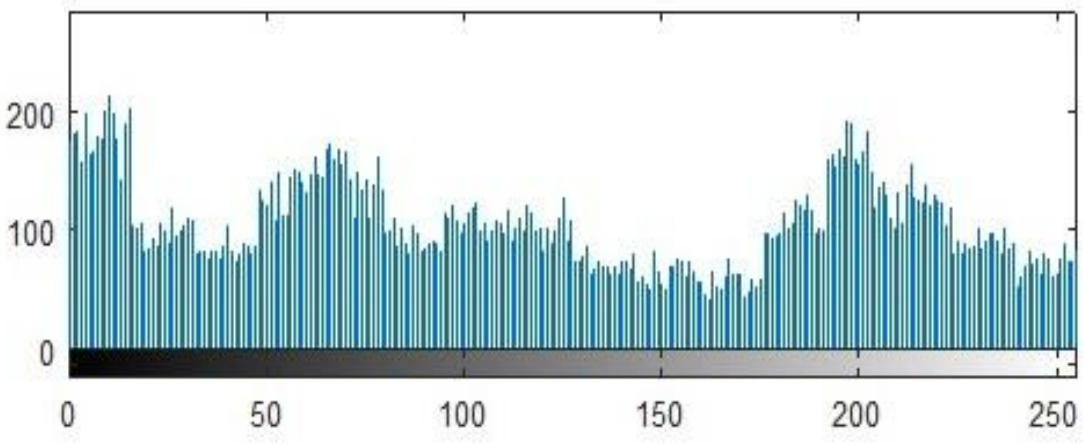


Figure.4.2 Histogram of secret image after encryption

Histograms are used to do comparison between two images. If the histogram of two images is same, it means they have same intensity values or image characteristics. And if the histogram of two images is different, it means they have different characteristics. Hence, it is difficult to obtain any information related to secret image from encrypted share. The histogram of the original secret image and the encrypted secret image has been studied. The histograms of both images are different. It proves that the encrypted image is totally different from original image. So, it is secure to transmit without any risk of attack by unauthorized person.

After the encryption of all the shares, the adding of images has been done. All the three images are added together to form one final share.

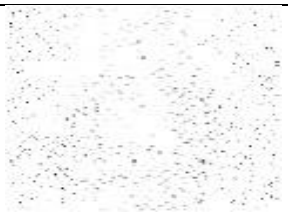
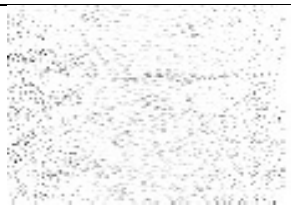
	Jpeg	Png	bmp
Secret Shares	 (1)	 (2)	 (3)

Table 4.6 Secret images after encryption

4.2 HIDING THE IMAGE:

	Jpeg format	**Png format**	**Bmp format**
Cover image	 (A)	 (B)	 (C)
Cover image after watermarking	 (D)	 (E)	 (F)

Table 4.7 Hidding of image by watermarking technique

The images shown in table 4.6 are the secret images which are obtained after the encryption process. (1) is the jpeg secret image and (2), (3) are the bmp and png format respectively. Secret images of different formats are successfully hidden in the cover images. Now, we can share or transmit these cover images to the receiver end without any risk of attack. The secret image is decrypted by applying the opposite algorithm as the encryption is done.

CHAPTER 5

CONCLUDING REMARKS AND FUTURE SCOPE

Literature survey has been successfully done on cryptography and VC for image encryption. A few of the observations have also been drawn from which the problem formulation and gaps are identified. Some of the expects are key management system, forward and backward secrecy and computation complexity The work has been done using the "MATLAB R2015a" software to simulate the modified encryption algorithm in order to obtain the optimized results.The VSS scheme shares a digital image by using diverse image media. The diverse image media means the media that include $n-1$ randomly chosen images. Regardless of the number of participant's increases, this technique only one noise share for sharing the secret image. Comparing with the existing secret sharing schemes, transmission risk is reduced by using proposed scheme and the highest level of user friendliness is been, both for shares and for participants. Four major contributions have been analyzed from this study, images were sent in a heterogeneous medium for the first time. Secondly, hand-printed images for image sharing schemes have been successfully introduced. Third, a useful concept was used for unaltered images. Fourth, a method to store the image into another image using stegnographic technique has been developed. The perfectly reconstructed recovered image will be formed after decryption process will be done. By comparing the pixel values of hidden image and the recovered image it can be analyzed that there will no pixel expansion in the recovered image. There will be no change between hidden image and recovered image. Steganography and encryption techniques also have been used for secured transmission. As a future work, we can use optimized encryption technique and evaluate them and compare them with the existing techniques.

REFERENCES

[1] Alfred J.Menezes,Paul C.van Oorschot and Scott A.Vanstone (1996).Handbook of Applied Cryptography, *CRC*, Edition 5.

[2] Bruce Schneier (1996). Applied Cryptography, John Wiley and Sons, Edition 2.

[3] William Stallings (2011). Cryptography and Network Security, Principles and Practice, *Pearson*

[4] *Prentice Hall Pearson Education*, Edition 5.

[5] Data Encryption Standard (1999), *Federal Information Processing Standard Publication, FIPS*, 46(3).

[6] Randall k.Nichols Panos C. Lekkas, Wireless, (2002), Security Models, Threats and Solutions, *McGraw-Hill Companies, first edition*, DOI: 10.1036/0071399437.

[7] Vercauteren Frederik (2006). A Fault Attack on Pairing-Based Cryptography, *IEEE Transaction on Computers*, 55(9), 1075-1080.

[8] Cheddad Abbas, Condell Joan, Curran Kevin and Mc Kevitt Paul (2010). Digital image steganography: Survey and analysis of current methods, *School of Computing and Intelligent System*, 909(3), 727-752.

[9] R. Arce Gonzalo (2006). Halftone Visual Cryptography, *IEEE Transaction on Image Processing*, 15(8), 2441-2453.

[10] Kakkar Ajay, Singh M. L. and Bansal P. K. (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.

[11] Ma Kun, Liang Han and Wu Kaijie (2012).Homomorphic Property-Based Concurrent Error Detection of RSA: A Countermeasure to Fault Attack, *IEEE Transactions on Computers*, 61(7), 1040-1049.

[12] Zhou Zhi, Arce Gonzalo R. and Di Crescenzo Giovanni (2006). Halftone Visual Cryptography, *IEEE Transaction on Image Processing*, 15(8), 2441-2453.

[13] Kang InKoo (2011). Color Extended Visual Cryptography Using Error Diffusion, *IEEE Transaction on Image Processing*, 20(1), 132-145.

[14] Ross Arun and Othman Asem (2011).Visual Cryptography for Biometric Privacy, *IEEE Transaction on Information Forensic and Security*, 6(1), 70-81.

[15] Zeng Wenjun (2002). A Format-Compliant Configurable Encryption Framework for Access Control of Video, *IEEE Transactions on Circuits and Systems for Video Technology*, 12(6), 545-557.

[16] Wang Xiang, Pei Qingqi and Li Hui (2014). A Lossless Tagged Visual Cryptography Scheme, *IEEE Signal Processing Letters*, 21(7), 853-856.

[17] Inkoo Kang InKoo (2011). Color Extended Visual Cryptography Using Error Diffusion, *IEEE Transaction on Image Processing*, 20(1), 132-145.

[18] Lee Kai-Hui and Chiu Pei-Ling (2014).Digital Image Sharing by Diverse Image Media, *IEEE Transaction on Information Forensic and Security*, 9(1), 88-98.

[19] Askari Nazanin, M. Heys Howard and R. Moloney Cecilia (2014). Novel Visual Cryptography Schemes without Pixel Expansion for Halftone Images, *Canadian Journal of Electrical and Computers Engineering*, 37(3), 168-177.

[20] Xiang Ta o, Guo Shangwei and Li Xiaoguo (2016). Perceptual Visual Security Index Based on Edge and Texture Similarities, *IEEE Transaction on Information Forensic and Security*, 11(5), 951-963.

[21] Yang Ching-Nung (2014).Property Analysis of XOR-Based Visual Cryptography, *IEEE Transactions on Circuits and Systems for Video Technology*, 24(2), 189-197.

[22] Iwamoto Mitsugu (2012).A Weak Security Notion for Visual Secret Sharing Schemes, *IEEE Transaction on Information Forensic and Security*, 7(2), 372-382.

[23] Chen Yu-Chi (2017). Fully Incrementing Visual Cryptography from a Succinct Non-Monotonic Structure, *IEEE Transactions on Information Forensics and Security*, 12(5), 1082-1091.

[24] Liu Feng, Wu Chuankun(2010). Step Construction of Visual Cryptography Schemes, *IEEE Transactions on Information Forensics and Security*, 5(1), 27-38.

[25] Zhang Liang and Wang Haili (2009). A High-Capacity Steganography Scheme for JPEG2000 Baseline System, *IEEE transactions on Image Processing*, 18(8), 1797-1803.

[26] Li Bin (2008).Steganalysis of Multiple-Base Notational System Steganography, *IEEE Signal Processing Letters*, 15, 493-496.

[27] Huang Chun-Hsiang, Chuang Shang-Chih, Huang Yen-Lin, and Wu Ja-Ling(2009). Unseen Visible Watermarking: A Novel Methodology for Auxiliary Information Delivery via Visual Contents, *IEEE Transaction on Information Forensic and Security*, 4(2), 193-206.

[28] Wang Daoshun (2007). Two secret sharing schemes based on Boolean operations, *Pattern Recognition*, 40(10), 2776-2785.

[29] Wua Xiaotian and WeiSun(2013). Improving the visual quality of random grid-based visual secret sharing, *Signal Processing*, 93(5), 977–995.

[30] Hajiabolhassa Hossein and Cheraghi Abbas (2010). Bounds for visual cryptography schemes, *Discrete Applied Mathematics*, 158(6), 659-665.

[31] Wang Dao-Shun (2013). Optimal Contrast Grayscale Visual Cryptography Schemes with Reversing, *IEEE Transactions on Information Forensics Security*, 8(12), 2059- 2072.

[32] Blundo Carlo, Cimatob Stelvio and De Santis Alfredo (2006). Visual cryptography schemes with optimal pixel expansion, *Theoretical Computer Science*, 369(1), 169-182.

[33] Cimato Stelvio (2005). Ideal contrast visual cryptography schemes with reversing, *Information Process Letters*, 93(4), 199-206.

[34] Hou Young-Chang and Quan Zen-Yu (2011).Progressive Visual Cryptography with Unexpanded Shares, *IEEE Transaction on Circuits and Systems for Video Technology*, 21(11), 1760-1764.

[35] Lukac Rastislav and N. Plataniotis Konstantinos (2005). Multi-dimensional Image Processing, *Special Issue on Multi-dimensional Image Processing*, 11(5), 355-474.

[36] Shyong Jian Shyu and Ming Chiang Chen (2011). Optimum Pixel Expansions for Threshold Visual Secret Sharing Schemes, *IEEE Transactions on Information Forensics and Security*, 6(3), 960-969.

[37] Fang Wen-Pinn (2008).Friendly progressive visual secret sharing, *Pattern Recognition*, 41(4), 1410-1414.

[38] Yang Ching-Nung (2008). Coloured visual cryptography scheme based on additive colour mixing, *Pattern Recognition*, 41(10), 3114-3129.

[39] Jen-Bang (2008). Visual secret sharing for multiple secrets, *Pattern Recognition*, vol. 41(12), 3575-3581.

[40] Lou Der-Chyuan, Chen Hong-Hao, Wu Hsien-Chu (2011). A novel authenticatable colour visual secret sharing scheme using non-expanded meaningful shares, *Pattern Recognition*, 32(3), 118-134.

[41] Chen Tzung-Her and Tsao Kai-Hsiang, Threshold visual secret sharing by random grids, *Journal of Systems and Software*, 84(7), 1197-1208.

[42] Chena Tzung-Her, Lee Yao-Sheng, Huang Wei-Lun (2013). Quality-adaptive visual secret Sharing by random grids, *Journal of Systems and Software*, 86(5), 1267–1274.

[43] Guo Teng, Liu Feng and Wua ChuanKun (2013). Threshold visual secret sharing by random grids with improved contrast, *Journal of Systems and Software*, 86(8), 2094-2109.

[44] Chen Tzung-Her, Wu Chang-Sian (2011). Efficient multi-secret image sharing based on Boolean operations, *Journal of Systems and Software*, 91(1), 90-97.

[45] Wua Xiaotian,Sun Wei (2013). Random grid-based visual secret sharing with abilities of OR and XOR decryptions, *Journal of Systems and Software*, 24(1), 48–62.

[46] Lin Chang-Chou and Tsai Wen-Hsiang (2003). Visual cryptography for gray-level images by Dithering Techniques, *Pattern Recognition Letters*, 24(1), 349–358.

[47] Yang Ching-Nung (2004). New visual secret sharing schemes using probabilistic method, *Pattern Recognition Letters*, 25(4), 481-494.

[48] Yang Ching-Nung and Tse-Shih Chen (2005). Aspect ratio invariant visual secret sharing scheme with minimum pixel expansion, *Pattern Recognition Letters*, 26(2), 193-206.

[49] Blundo Carlo (1998).Visual cryptography scheme with perfect reconstruction of black pixels, *Computers & Graphics*, 22(4), 449-455.

[50] Wong Fu-Hsiang, Wang Sheng-Ping,Yu Shiueh-Ling and Lian Wei-Cheng (1990) Existence of Positive Solutions for an .n C 2/-order nonlinear BVP, *Computers & Graphics*, 84(6), 228-251.

[51] Chung Kuo-Liang, Chen Ping-Zen, Pan Ying-Lin (2009). Speed up of the edge-based Inverse halftoning algorithm using a finite state machine model approach, *Computers and Mathematics with Applications*, 58(3), 484-497, 2009.

[52] Huang Win-Bin, Alvin W.Y. Su and Kuo Yau-Hwang(2008). Neural network based method for image halftoning and inverse halftoning, *Pattern Recognition Letters*, 34(4), 2491-2501.

[53] Huang Yong-Huai, Chung Kuo-Liang, Dai Bi-Ru(2011). Improved inverse halftoning using vector and texture-lookup table-base learning approach, *IEEE Transaction on Information Forensic and Security*, 38(12), 15573-15581.

[54] Wu Xiaotian and Sun Wei (2014). Extended Capabilities for XOR-Based Visual Cryptography, *IEEE Transaction on Information Forensic and Security*, 9(10), 1592-1605.

[55] Daniel L. Lau, Gonzalo and Neal C. Gallagher (2000). DigitalColor Halftoning with Generalized Error Diffusion and Multichannel Green-Noise Masks, *IEEE Transaction on Image Processing*, 9(5), 923-935.

[56] Kim Sang Ho (2002). Impact of HVS Models on Model-Based Halftoning, *IEEE Transaction on Image Processing*, 11(3), 258-269.

[57] Wang Yong, Liu Jiufen, Zhang Weiming and Lian Shiguo (2011). Reliable JPEG steganalysis Based on multi- directional correlations, *IEEE Transaction on Image Processing*, 25(8), 577-587.

[58] Lin Chang-Chou, Tsai Wen-Hsiang(2011),Visual cryptography for gray-level images by Dithering techniques, *Department of Computer and Information Science,* 24(3), 349- 358, 2011.

[59] Liu Qingzhong,Andrew H. Sung, Qiao Mengyu, Chen Zhongxue ,Bernardete Ribeiro, An improved approach to steganalysis of JPEG images, *Information Sciences*, 180(2), 1643-1655.

[60] Chung Kuo-Liang and Wu Shih–Tung (2005). Inverse Halftoning Algorithm Using Edge-Based Lookup Table Approach, *IEEE Transaction on Image Processing*, 14(10), 1583-158.

[61] Joong Kim Hyoung, Sachnev Vasiliy, Yun Qing Shi (2008). Novel Difference Expansion Transform for Reversible Data Embedding, *IEEE Transaction on Information Forensic and Security*, 3(3), 456-465.

[62] Wang Zhongmin, Gonzalo R. Arce, Di Crescenzo Giovanni(2009). Halftone Visual Cryptography via Error Diffusion, *IEEE Transaction on Information Forensic and Security*, 4(3), 383-396.

[63] Chen Tzung-Her and Tsao Kai-Hsiang (2011).User-Friendly Random-Grid-Based Visual Secret Sharing, *IEEE Transactions on Circuits and Systems for Video Technology*, 21(11), 1693-1703.

[64] Chiu Pei-Ling and Lee Kai-Hui (2011). A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes, *IEEE Transaction on Information Forensic and Security*, 6(3), 996-100

[65] Jo Jinyong and Kim JongWon(2014).Software-defined Home Networking Device for Multihome Visual Sharing, *IEEE Transactions on Consumer Electronics*, 60(3), 534-539.

[66] Hou Young-Chang and Quan Zen-Yu (2015). A privilege-based visual secret sharing model, *Journal of Visual Communication and Image Representation archive Volume*, 33(1), 358-367.

[67] Zhang Lei (2016). Visual Understanding via Multi-Feature Shared Learning with Global Consistency, *IEEE Transactions on Multimedia*, 18(2), 247-259.

[68] Chen Yu-Chi, Horng Gwoboa and Tsai Du-Shiau (2012). Comment on Cheating Prevention in Visual Cryptography, *IEEE Transactions on Image Processing*, 21(7), 3319-3326.

[69] Lee Kai-Hui and Chiu Pei-Ling (2012). An Extended Visual Cryptography Algorithm for General Access Structures, *IEEE Transactions on Information Forensics and Security*, 7(1), 219-229.

[70] Guo Cheng and Chang Chin-Chen and Qin Chuan (2012). A multi-threshold secret image Sharing scheme based on MSP, *Department of Computer Science*, 33(12), 1594-1600.

[71] Rastislav Lukac (2005). Bit-level based secret sharing for image encryption, *Pattern Recognition*, 38(5), 767-772.

LIST OF PUBLICATIONS

- Kaur Tejbir and Kakkar Ajay (2017).Digital Image Sharing by Diverse Image Media, *International Journal of Computer Application 171(3), 26-29.*
- Kaur Harpreet, Kaur Lovepreet and Kaur Tejbir (2017). Triple security of data using encryption keys and image steganography, *International Journal of Computer Application ,171(7),19-22.*