

Thesis No. CSER-M-18-02

# **An Approach to Ensure the Secrecy of Scene Images**

By

**Arindom Mondal**

A Thesis submitted in partial fulfillment of the requirements for the degree of  
Master of Science in Computer Science and Engineering



Khulna University of Engineering and Technology  
Khulna 9203, Bangladesh  
July 2018

## Declaration

---

This is to certify that the thesis work entitled “**An Approach to Ensure the Secrecy of Scene Images**” has been carried out by Arindom Mondal in the Department of Computer Science and Engineering, Khulna University of Engineering & Technology, Khulna 9203, Bangladesh. The above thesis work or any part of this work has not been submitted anywhere for the award of any degree or diploma.

*RAA*  
10-07-18

---

Signature of Supervisor

**Dr. Kazi Md. Rokibul Alam**  
Professor,  
Dept. of Computer Science and Engineering,  
Khulna University of Engineering & Technology.

*Arindom*  
10.7.18

---


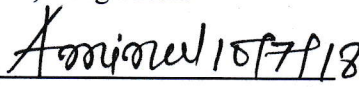
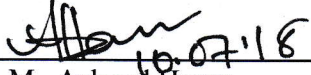
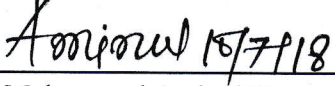

Signature of Candidate

**Arindom Mondal**  
Roll: 1507503  
Dept. of Computer Science and Engineering,  
Khulna University of Engineering & Technology.

## Approval

This is to certify that the thesis work submitted by Arindom Mondal entitled “An Approach to Ensure the Secrecy of Scene Images” has been approved by the board of examiners for the partial fulfillment of the requirements for the degree of Master of Science in Engineering in the Department of Computer Science and Engineering, Khulna University of Engineering & Technology, Khulna, Bangladesh in July 2018.

### BOARD OF EXAMINERS

1.  10.07.18  
Dr. Kazi Md. Rokibul Alam  
Professor  
Dept. of Computer Science and Engineering  
Khulna University of Engineering & Technology  
Khulna, Bangladesh.  
Chairman  
(Supervisor)
2.  10/7/18  
Head  
Dept. of Computer Science and Engineering  
Khulna University of Engineering & Technology  
Khulna, Bangladesh.  
Member
3.  10.07.18  
Dr. K. M. Azharul Hasan  
Professor  
Dept. of Computer Science and Engineering  
Khulna University of Engineering & Technology  
Khulna, Bangladesh.  
Member
4.  10/7/18  
Dr. Muhammad Aminul Haque Akhand  
Professor  
Dept. of Computer Science and Engineering  
Khulna University of Engineering & Technology  
Khulna, Bangladesh.  
Member
5.  10/7/18  
Dr. Rameswar Debnath  
Professor  
Computer Science and Engineering Discipline  
Khulna University  
Khulna, Bangladesh.  
Member  
(External)

## Acknowledgements

---

At first, I would like to thank Almighty for showering all his blessings on me whenever I needed. Then it is my immense pleasure to express my indebtedness and deep sense of gratitude to my supervisor Dr. Kazi Md. Rokibul Alam, Professor, Department of Computer Science and Engineering (CSE), Khulna University of Engineering & Technology (KUET) for his continuous encouragement, constant guidance and keen supervision throughout of this study. I am especially grateful to him for giving me his valuable time whenever I need and always providing continuous support in my effort.

I am extremely grateful to all the faculty members of the Department of CSE, KUET to have their privilege of intensive, in depth interaction and suggestions for the successful completion of my master degree. Finally I am grateful to my parents, family member's, colleagues and friends for their patience, support and encouragement during this period.

July 2018

Author

## Abstract

---

This thesis proposes a multi-stage encryption technique to enhance the level of secrecy of image to facilitate its secure transmission through the public network. A vast number of researches have been done on image secrecy. The existing image encryption techniques like visual cryptography (VC), steganography, and watermarking etc. while are applied individually; usually they cannot provide unbreakable secrecy. Through combining several separate techniques, a hybrid multi-stage encryption technique is proposed in this thesis, which provides nearly unbreakable image secrecy, while the encryption/decryption time remains almost the same of the exiting techniques. The technique consecutively exploits VC, steganography and one time pad (OTP). At first it encrypts the input image using VC, i.e., splits the pixels of the input image into multiple shares to make it unpredictable. Then after the pixel to binary conversion within each share, the exploitation of steganography detects the least significant bits (LSBs) from each chunk within each share. At last, OTP encryption technique is applied on LSBs along with randomly generated OTP secret key to generate the ultimate cipher image. Besides, prior to sending the OTP key to the receiver, first it is converted from binary to integer and then an asymmetric cryptosystem is applied to encrypt it and thereby the key is delivered securely. Finally, the outcome, the time requirement of encryption and decryption, the security and statistical analyses of the proposed technique are evaluated and compared with existing techniques.

# Contents

---

<b>Title</b>	<b>Page</b>
Title Page	<b>i</b>
Declaration	<b>ii</b>
Approval	<b>iii</b>
Acknowledgement	<b>iv</b>
Abstract	<b>v</b>
Contents	<b>vi</b>
List of Tables	<b>viii</b>
List of Figures	<b>ix</b>
Nomenclature	<b>x</b>
<b>Chapter I    Introduction</b>	<b>1</b>
1.1 Motivation	1
1.2 Overview of the Field	2
1.3 Objectives of the Thesis	3
1.4 Thesis Organization	4
<b>Chapter II    Literature Review</b>	<b>5</b>
2.1 Visual Cryptography Based Technique	5
2.2 Steganography Based Technique	6
2.2.1 Discrete Cosine Transform (DCT) Based Technique	7
2.2.2 List Significant Bit (LSB) Based Technique	8
2.3 Watermarking Based Technique	9
2.4 Hybrid Techniques	12
2.4.1 Visual Cryptography Followed by Steganography	13
2.4.2 Steganography Followed by Visual Cryptography	14
2.5 Our Contributions	15
<b>Chapter III    Cryptographic Tools and Proposed Technique</b>	<b>16</b>
3.1 Visual Cryptography	16
3.2 Extended Visual Cryptography (EVC)	20
3.3 Steganography	21
3.3.1 List Significant Bits (LSB) Technique	23
3.3.2 LSB Implementation for Monochrome Image	24

3.3.3 LSB Implementation for Color Image	24
3.4 One Time Pad (OTP)	25
3.5 Paillier Cryptosystem	26
3.6 Proposed Technique	27
3.6.1 Random OTP Secret Key Generation	28
3.6.2 Image Encryption Technique	29
3.6.3 Image Decryption Technique	30
<b>Chapter IV Experimental Studies</b>	<b>32</b>
4.1 Experimental Setup	32
4.2 Output of Encryption Step	32
4.2.1 Output After Applying VC	32
4.2.2 Output After Transforming into Binary Image	33
4.2.3 Output After Applying Steganography with OTP	34
4.3 Sending OTP Secret Key to the Receiver	36
4.4 Output of Decryption Steps	37
4.4.1 Output After Applying Steganography with OTP	37
4.4.2 Output After Transforming Binary Image into Pixels	37
4.4.3 Final Output	39
4.5 Experimental Results and Performance Comparisons	40
4.6 Security and Statistical Analysis	42
4.6.1 Histogram Analysis	42
4.6.2 Salt & Pepper Noise Attack	44
4.6.3 Chosen-Plaintext Attack (CPA)	46
4.7 Results and Discussion	47
<b>Chapter V Conclusions</b>	<b>48</b>
5.1 Summary of the Work	48
5.2 Future Perspectives	48
<b>References</b>	<b>49</b>
<b>Publication in Progress</b>	<b>53</b>

## List of Tables

---

<b>Table No.</b>	<b>Caption of the Tables</b>	<b>Page</b>
3.1	VC Technique for Encoding the Pixels into Two Shares	18
4.1	Generated Final Ciphertext (a portion)	35
4.2	Generated Plaintext of a Share Image (a portion)	37



## List of Figures

---

Figure No.	Caption of the Figure	Page
2.1	Structure of a 32-Bit Pixel	8
2.2	Digital Watermarking - Embedding Process	11
2.3	Digital Watermarking - Extracting Process	11
2.4	Block Diagram of DCT Based VC and Steganography	12
3.1	Working Procedure of Visual Cryptography	17
3.2	Expansion and Encryption of Source Pixel	19
3.3	Encryption and Decryption for Color Image	20
3.4	Basic Steganographic System	22
3.5	Encryption and Decryption Process of Steganography Technique	22
3.6	Flow Chart of Random OTP Secret Key Generation Process.	28
3.7	Flow Chart of Image Encryption Technique.	29
3.8	Flow Chart of Image Decryption Technique.	30
4.1	Output Image after Applying VC Technique.	34
4.2	Pixel Appearance of Final Ciphertext of Share Images.	36
4.3	Retrieved Share Images and Input Images	38
4.4	Sample of all Experimental Images	39
4.5	Time Requirement of Encryption Process for Various Images by the Proposed Technique	40
4.6	Time Requirement of Decryption Process for Various Images by the Proposed Technique.	40
4.7	Time Requirement of Encryption and Decryption Operations by the Proposed Technique	41
4.8	Comparison in Case of Encryption Time Requirement Among Various Techniques.	42
4.9	Comparison in Case of Decryption Time Requirement Among Various Techniques	42
4.10	Histogram Plot for the Image of Fig. 5.1 (a): (a) Input Image, (b) Encrypted Image, and (c) Retrieved Image.	43
4.11	Histogram Plot for the Image of Fig. 5.1 (d): (a) Lena Image, (b) Input Lena Image, and (c) Encrypted Lena Image.	44
4.12	(a) KUET Image. Salt and Pepper Noise Attacked of KUET Images: (b) 10%, (c) 30% and (d) 50%.	45
4.13	(a) Lena Image. Salt and Pepper Noise Attacked of Lena Images: (b) 10%, (c) 30% and (d) 50%.	45
4.14	(a) Baboon Image. Salt and Pepper Noise Attacked of Baboon Images: (b) 10%, (c) 30% and (d) 50%.	46

## Nomenclature

---

VC	Visual Cryptography
EVC	Extended Visual Cryptography
HVS	Human Visual System
OTP	One Time Pad
DCT	Discrete Cosine Transform
CPA	Chosen Plaintext Attack
RGB	Red, Green, Blue
RGBA	Red, Green, Blue, Alpha
HSV	Hue, Saturation, Value
PVD	Pixel Value Differencing
SNR	Signal to Noise Ratio
DIIVC	Digital Invisible Ink Using Visual Cryptography
SAE	Stacked Auto Encoder

# CHAPTER I

## Introduction

### 1.1 Motivation

Nowadays due to diversified and extensive users of computer networks and internet, the number of intrusions is increasing. Therefore, while image, message etc. are transmitted over computer networks, secure communication is essential. Note that an image consists of several pixels which are highly correlated, whereas a message consists of text, characters and/or binary and/or integer and/or hexadecimal values [1]. Thus, an image is distinct from a message and hence their encryption techniques are also somehow different. In addition, very often hugely it is required to share the image over the network. Thereby like message encryption, image encryption is another significant branch of cryptography. RSA, ElGamal, AES, DES etc. are examples of some well-known message encryption techniques. To encrypt an image, techniques like visual cryptography (VC) [1], steganography [2], watermarking [3], deep learning-based ones [23, 24], chaotic system and symmetric/asymmetric cryptosystem-based ones [16, 17] etc. have been developed. However, while image is retrieved through decryption, many of them are not extremely efficient. The increased secrecy of image over public network is necessary, for instance, transmitting bank cheque image, hand-written signature, biometric authentication etc.

Intuitively, VC, watermarking, steganography etc. techniques are exclusively associated with image encryption and their advantage is: to conduct their encryption and decryption processes usually they do not need to rely on any specific key/keys. For example, while encryption, VC splits an image into  $n$  shares and decrypts it by superimposing the shares [12]. The limitation of VC is: its original formation is restricted to binary images. Also, the alignment of two shares is not so easy to perform unless some special alignment marks are provided [5]. Steganography hides an image within another cover image to protect its contents [2]. Hence, the handling of the cover image along with the input image makes the encryption and decryption process bulky [10]. Watermarking technique combines cover image with a watermark, which is hard to be detected or removed. By the way, the owner of the image can prove its copyright by extracting the watermark from the watermarked image. However, note

that the watermarking technique is not free from attacks. The attacks associated with this technique are: compression, blurring, noise, distortion, sharpening, scaling, cropping etc. [11]. Thus, these techniques are substantially weaker than cryptography-based message encryption techniques. Thereby while they are applied separately or jointly, they possess various limitations.

To protect images, various encryption techniques based on traditional cryptosystems has been developed. But most of the images by using these techniques become distorted after being encryption with a lot of limitations. For which, the growth of networked multimedia systems has created a great need for securing these images where it ensures the authentication of image content and ownership with no distortion.

## **1.2 Overview of the Field**

In the advent of booming communication technology, the needs for information sharing and data transfer have increased exponentially. The threat of an intruder accessing secret information has been an ever-existing concern for data communication in public domain. Secure image transmission whether the image having some information or text, is also the focusing area for security. While using these secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal images that they want. To deal with the security problems of secret images, various image secret sharing techniques have been already proposed. To encrypt an image, techniques like visual cryptography (VC) [1], steganography [2], watermarking [3] etc. have been developed. However, while image is retrieved through decryption, they are not extremely efficient in various domain. The increased secrecy of image over public network is necessary, for instance, transmitting bank cheque image, face detection, iris identify, hand-written signature verification, finger print security, biometric authentication etc. For a perfect image security technique, there are five vital features [40] that should be considered. The first one is the capacity payload which refers to the amount of secret information that a stego-cover can carry before the distortions become noticeable. The second feature is the undetectability which means that the existence of the secret information should be undetectable whenever the stego-object is detected and analyzed. Other features that should be considered are: invisibility, security and robustness [11,40].

VC is one of the most important cryptographic field within the security profession that splits an image into two or more separate random images called shares and decrypts it by superimposing of the all shares [1], then original image appears. Because of its simplicity, anyone can physically manipulate the elements of the system and visually see the decryption process in action without any knowledge of cryptography i.e. without performing any cryptographic computations [12]. The main drawbacks of traditional VC are: its original formation is restricted to binary images, pixel expansion and low resolutions [38].

Steganography embeds an image within another cover image in such a way that the intruder cannot identify the existence of the input image from the embedded image [2]. The technique proposed in [7] directly hides the image by replacing the LSBs of each pixel of the cover image. It embeds the same number of bits of the input image that makes a minor change of the cover image. The main drawbacks of these steganographic techniques are: the use of cover image makes the image encryption and decryption process so bulky [10] and increase the processing time and storage capacity. VC involves changing data into an unreadable cipher where steganography embeds message into a cover media and hides its existence.

Watermarking is the most common technique for protecting digital image where it hides an image into another cover image [3,11]. It combines the cover image with a watermark, which is hard to be detected or removed. By the way, the owner of the image can prove its copyright by extracting the watermark from the watermarked image. However, note that watermarking technique is not attack free. The attacks associated with many techniques are: compression, blurring, noise, distortion, sharpening, scaling, cropping etc. [11].

Intuitively, VC, watermarking, steganography etc. techniques are substantially weaker than cryptography-based message encryption techniques and hence while these techniques are applied separately or jointly they possess various limitations. Although these techniques are already combined to achieve higher levels of security, still there is a demand of highly secure technique to transfer image over any communication media to minimizing the threat of intrusion.

### **1.3 Objectives of the Thesis**

This thesis enlarges the level of secrecy of image by combining several existing techniques i.e. VC, steganography and one time pad (OTP) consecutively. Thereby, it unifies ‘the benefits of cryptosystems not relying on any specific key/keys’ along with ‘the strength of the

cryptosystem relying on a specific key'. Here for the sake of encryption and decryption purposes, VC and steganography do not need to rely on any specific key/keys whereas OTP technique needs to rely on a specific key. In addition, OTP technique possesses "perfect secrecy" and cannot be cracked. Here at first VC splits pixels of the input image into  $2^n$  shares, where  $n \geq 1$ . Note that with the increasing  $n$ , the level of secrecy increases. Now pixels of each share are transformed into their corresponding binary values. Then instead of using a cover image, it only detects LSBs from each chunk of binary values of each share exploiting steganography. Lastly, it applies OTP encryption technique on LSBs using random OTP secret key to generate the final cipher image. Besides before sending the OTP key to the receiver, it is transformed into integer value to encrypt it using Paillier cryptosystem for the decryption purpose. Thus, the successive exploitation of several techniques increases the level of secrecy of the input image significantly while maintaining its quality.

The overview of the proposed technique is summarized as follows. To enhance the level of secrecy of image encryption, it:

- adopts a hybrid technique through combining the advantages of cryptosystems not relying on any specific key/keys with the strength of the cryptosystem relying on a specific key.
- develops a multi-stage encryption technique that combines VC, Steganography along with OTP techniques altogether. Thereby while decryption; it decrypts the image at distinct levels reversely.

#### 1.4 Thesis Organization

The rest of the thesis is organized as follows.

- **Chapter II** discuss the various existing image security techniques.
- **Chapter III** describes required cryptographic tools to develop the proposed technique. Also describes the proposed technique in detail, i.e. random OTP secret key generation and steps of encryption, decryption process.
- **Chapter IV** describes the experimental studies. Where output of encryption and decryption step, statistical analysis, results and performance are discussed.
- **Chapter V** concludes this thesis together with the outline of probable future directions of research opened by this work.

# CHAPTER II

## Literature Review

To ensure the secrecy of image, researchers have exploited numerous techniques like chaotic system and symmetric/asymmetric cryptosystem based ones, VC, steganography, watermarking, VC followed by steganography, steganography followed by VC, machine learning based ones etc. This chapter categorically reviews these existing techniques of ensuring image secrecy.

### 2.1 Visual Cryptography (VC) Based Technique

The technique of VC introduced in [1] is for monochrome image. For encryption it divides an image consists of random white and black pixels into  $n$  shares and then for decryption, the superimposing of all shares is required. It is a unique technique in the sense that the encrypted image can be decrypted directly by the human visual system (HVS). For each pixel of each share, two blocks are generated in the corresponding location. It is assumed that in each share any white pixel is transparent, and any black pixel is opaque which are stored as binary 0 and 1 values, respectively [12]. The major drawbacks of VC based techniques are pixel-expansion, low resolution, alignment problems etc. [5].

Another secret sharing technique presented in [37], which reconstructs a message with two colors by arranging the colored or transparent sub-pixels. Both approaches assign a color to a sub-pixel at a certain position, which means that displaying  $m$  colors uses  $m-1$  sub-pixels. The resulting pixels contain one colored sub-pixel and the rest of the sub-pixels are black [4].

Random Grids extends the solution to the secret sharing problem by executing a collection of 2-D transparent and opaque pixels arranged randomly which reveals the secret to the HVS when being superimposed [38]. Unlike other VC techniques, random grid does not need the basis matrices to encode the shares. Pixel expansion is disallowed which is therefore a great advantage of using Random Grids. Also, the sizes of secret image and the shares are identical to each other.

A different data concealment of identity method proposed in [10] separating an image into blocks, where each block was repartitioned into overlapping sub-blocks. Each sub-block

relates to a level number according to its pattern, indicating power on visibility by assumed change of the central pixel in the sub-block. Data will be concealed by changing the central pixel in a sub-block. A technique presented in [28] which enable multicolor with relatively less subpixels (24 colors with  $m = 4$ ). However, each sheet must contain color random images, which means applying this approach to the extended VC is impossible.

Binary visual cryptography technique is applied to gray level images, that a gray level image is converted into halftone images [10]. The method that uses the density of the net dots to simulate the gray level is called “Halftone” and transforms an image with gray level into a binary image before processing.

The technique presented in [29] for images with  $c$  colors. The principle of this technique is to transform one pixel of image to  $b$  sub-pixels and each sub pixel is divided into  $c$  color regions. In each sub-pixel, there is exactly one-color region colored and all other color regions are black. The color of one pixel depends on the interrelations between the stacked sub-pixels. A major disadvantage of this technique is that the number of colors and the number of sub-pixels determine the resolution of the revealed secret image. If the number of colors is large, coloring the sub-pixels will become a very difficult task.

## **2.2 Steganography Based Technique**

Steganography [7] hides the input image inside another image known as cover image so that it reduces the suspicion of the intruder. LSB is one of the most common techniques used in steganography. In this technique, the LSBs from the pixel of the input image are replaced with the message information so that it cannot be observed by the human visual system. The reason is that the amplitude of the change is very small [9].

However, in the proposed technique, instead of using the cover image, random secret key is exploited to encrypt LSBs of each chunk of each share applying OTP encryption technique which increases the security of the image as well as makes the encryption and decryption process faster than that of using the cover image. Here the number of LSBs of each chunk of each share must be equal to the number of bits of OTP key.

Steganography embeds an image within another cover image in such a way that the intruder cannot identify the existence of the input image from the embedded image [2]. Among many variations of steganographic techniques already proposed, the technique proposed in [7]



directly hides the image by replacing the LSBs of each pixel of the cover image. It embeds the same number of bits of the input image that makes a minor change of the cover image. The main drawbacks of steganographic techniques are: the use of cover image makes the image encryption and decryption process bulky and increase the processing time and storage capacity.

The steganographic technique is proposed by in [17], where the number of 1's and number of 0's in the red component of the first pixel is computed first. Then, the absolute difference between this two is calculated and is divided by 2. Hence, the resultant numbers of bits are embedded in other two channels like as green and blue.

It is a significant sub division of information hiding that presented in [38]. In the frequency domain group, the frequency coefficients of the images are derived and is used to embed the messages with them [38]. These hiding methods overcome the robustness and imperceptibility problem found in the spatial domain.

Color images are represented in distinct color spaces such as RGB (Red Green Blue), HSV (Hue, Saturation, Value), YUV, YIQ, YCbCr (Luminance/Chrominance) etc [19]. YCbCr is one of the best representations for steganography because the eye is sensitive to minor changes in luminance but not in chrominance, so the chrominance part can be altered without visually impairing the overall image quality much. Y is luminance component and Cb, Cr are the blue and red chrominance components respectively. The values in one color space can be easily converted into another color space using conversion formula [31].

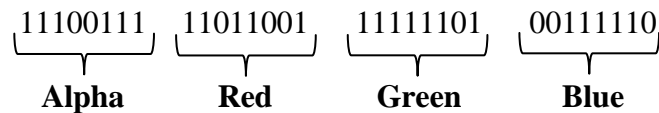
### **2.2.1 Discrete Cosine Transform (DCT) Based Technique**

Transform domain technique embeds the secret information in a cover image done by altering the DCT (Discrete Cosine Transform) coefficients [9]. It splits the image into parts of differing importance and transforms an image from the spatial domain to the frequency domain with high, middle and low frequency components. It hides secret information in the significant areas in the cover image that makes them robust against compression, cropping and other image processing attacks [9].

DCT represents the entire image as coefficients of different frequencies of cosines and calculated by taking 8x8 blocks of the image, which are then transformed individually. By applying DCT [38], JPEG transforms the information of color domain into frequency domain, then the image is divided into blocks with 8X8 pixels, which is transformed into frequency

domain. Each block of an image is represented by 64 components, which are called DCT coefficients [9]. The global and vital information of an image block is represented in lower DCT coefficients, while the detailed information is represented in upper coefficients. The compression of an image is achieved by omitting the upper coefficients.

DCT transforms image from spatial domain to frequency domain [9] and converts secret object into binary form that hides the bits chosen in middle and high frequency coefficients. DCT decomposes signal into low, middle and high frequency coefficients. The secret image is hidden in high and middle frequency regions but not in lower region because human visual system is more sensible to modifications that may occur in lower frequency band. Like other multimedia components, image is sensed by human. Pixel is the smallest unit constructing a digital image. Each pixel of a 32-bit digital color image is divided into four parts, namely Red, Green, Blue and Alpha; each with 8 bits. Alpha part represents degree of transparency. A 32-bit sample pixel is represented in the following Fig. 2.1.



**Figure 2.1:** Structure of a 32-Bit Pixel

Human visual system acts as an OR function where two transparent objects stacked together, produce transparent object. But changing any of them to non-transparent, final objects will be seen non-transparent.

The technique proposed in [3] divides a cover image into two blocks and each block is transformed with a two-dimensional discrete cosine transform (DCT) to classify as smooth block or edge block. Then biometric features are embedded in the low frequency coefficients of the 8×8 DCT blocks while the edge blocks are eliminated. However, the elimination of the edge blocks degrades the quality of the input image. Also, attacks like random cropping or shuffling can destroy the coded watermark [11].

### 2.2.2 List Significant Bit (LSB) Based Technique

An LSB steganography technique proposed in [35] for producing pseudorandom number and this number is further used as key for pixel location for storing secret data in cover image. For increasing capacity and imperceptibility based on probabilistic XOR secret sharing is

presented in [36]. An innovative approach proposed in [30] based on LSB using secret key. The secret key encrypts the hidden information and then it is stored into different position of LSB of the image.

A new adaptive LSB steganographic method [18] based on pixel-value differencing (PVD) by using the difference between two consecutive pixel values that identifies how many message bits will be embedded. In comparison with PVD [19], it provides more capacity and better quality that's why it's very easy for an attacker to identify the region where the message bits are embedded.

### **2.3 Watermarking Based Technique**

The watermarking technique hides an image into another cover image. The technique proposed in [3] that divides a cover image into two blocks and each block is transformed with a two-dimensional discrete cosine transform (DCT) to classify as smooth block or edge block. Then biometric features are embedded in the low frequency coefficients of the  $8 \times 8$  DCT blocks while the edge blocks are eliminated. However, the elimination of the edge blocks degrades the quality of the input image. Also, attacks like random cropping or shuffling can destroy the coded watermark [11]. The watermarking technique proposed in [21] is a multiple staged one. To endow the watermarked document, it produces a watermark specification by creating a template specification that illustrates the way to combine the watermark into the targeted document.

Watermarking [11] is most common technique for protecting digital data which is a method to assert an intellectual copyright in the electronic world. Digital watermarking is the process of embedding information into a digital signal. The signal may be audio, pictures or video. The embedded information is known as a watermark that can be extracted or detected. A watermark may be a digital signal or pattern which is inserted into a digital data. Since this signal or pattern is present in each unaltered copy of the original data, the digital watermark may also serve as a digital signature for the copies. Watermarking has become one of the widely used techniques to protect the copyright, prove authenticity, and avoid forgery of images.

Watermarking technique in [22] presents a blind image watermarking technique that embeds watermark messages at different wavelet blocks is presented base on the training of BPNN in wavelet domain. Reference [23] presents an adaptive image watermarking algorithm

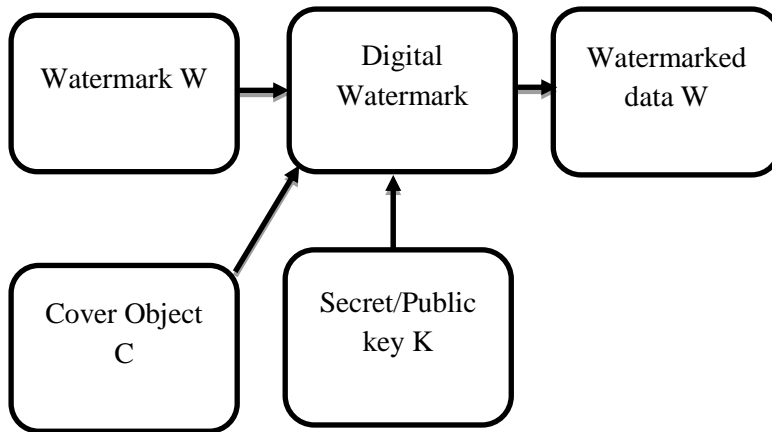
which is based on synthetic human visual system (HVS) characteristic and associative memory function of neural network.

Digital watermarking techniques are basically classified into three categories. Private watermarking which requires the prior knowledge of the original data and secret keys at the receiver. The watermark information and secret keys must be available at the receiver in Semi private or semi blind watermarking. Public or blind watermarking where the receiver must only know the secret keys [24]. The robustness of private watermarking techniques is high to endure signal processing attacks. However, they are not feasible in real applications, such as DVD copy protection where the original information may not be available for watermark detection. On the other hand, semi-blind and blind watermarking techniques are more feasible in that situation [25].

Agrawal and Kiernan [32] present a robust watermarking technique for relational databases. According to an embedding key, some bits of some attributes of some tuples are modified to embed watermark bits. In [33] further extend this technique to embed multiple bits information instead of one-bit information as in [32] technique into a relational database so that potential illegal distributors can be tracked. Also, this technique is claimed to be more robust since false negative and false positive detection rates are bounded.

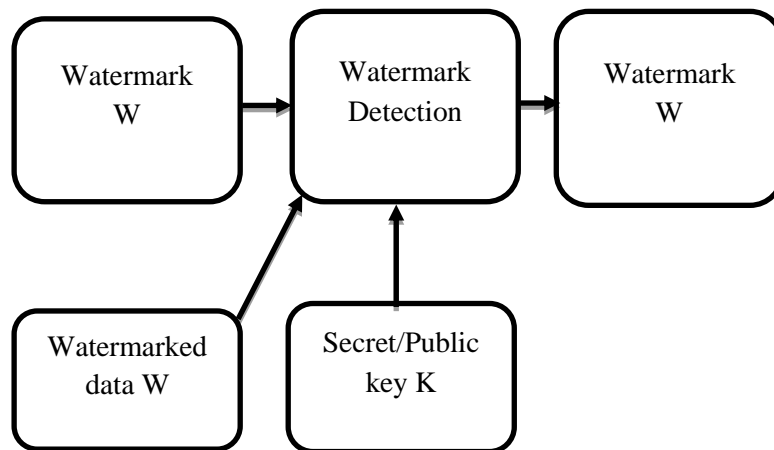
Watermarking is defined as a technique which embeds data into digital contents such as text, still images, video and audio data without degrading the overall quality of the digital media [16]. A watermark is the information to be hidden and indicates that the hidden information is transparent, while the term cover media indicates the media used for carrying the watermark. The watermarked data is the media which contains the watermark. In digital watermarking technology, the phrase embedding, and extraction means the procedures used for inserting the watermark into the cover media and extracting the embedded watermark from the watermarked data respectively. Detection is an important process that is used for detecting whether the given media containing a watermark.

Watermarking system is made up of a watermark embedding system and a watermark recovery system [23]. The system also has a key which could be either a public or a secret key. The key is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and recovery processes of watermarking are shown in Fig. 2.2 and Fig. 2.3.



**Figure 2.2:** Digital Watermarking - Embedding Process

For the embedding process, the inputs are the watermark, cover object and the secret or the public key. The watermark used can be text, numbers or an image. The resulting final data received is the watermarked data  $W$ .



**Figure 2.3:** Digital Watermarking - Extracting process

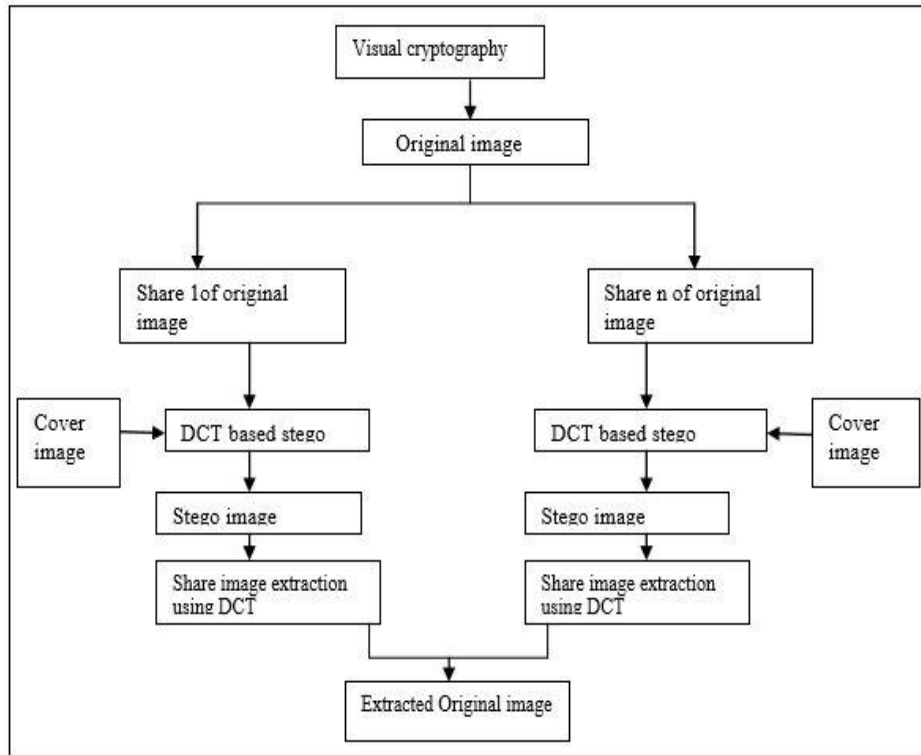
The inputs during the decoding process are the watermark or the original data, the watermarked data and the secret or the public key. The output is the recovered watermark  $W$ . Watermarked images are affected by various attacks such as cropping, salt and pepper noise and rotation. These attacks destroy the inserted watermark, so that the copyright problem may arise [22]. The effect of these attacks can be reduced by properly inserting the watermark with effective techniques.

## 2.4 Hybrid Technique

To ensure the secrecy of an image, the technique proposed in [4] combines steganography and VC that splits the image into two shares where each share is stored in different databases. Later, while retrieving the image, the superimposing of both shares is required. Here for storing the shares in two different databases, the storage cost is increased.

Both steganography and VC have problems, whenever they are used independently it gives only single layer of security which can be easily broken by intruders. If it combines features of both steganography and VC then it provides 2 layers of security. The Fig. 2.4 block diagram shows the actual working of the method [20] that combinations VC and steganography.

A spiral based LSB technique for hiding message in images is proposed in [26]. It uses LSB substitution technique to embed the watermark and order of insertion of watermark based on spiral substitution algorithm. In [27] 3rd and 4th LSB substitution technique is proposed elaborately. Here in used 3rd and 4th LSB bit position of cover image pixel to embed two watermark bits. For which the technique may increase the storage capacity to accommodate the watermark bits, but results decrease in perceptual quality of watermarked image.



**Figure 2.4:** Block Diagram of DCT Based VC and Steganography

Exploiting face image, another multi-stage face recognition technique proposed in [48] adopts a local structure which is based on a multi-phase collaborative representation technique. It studies the local structure connection-ship of overlapping patches. Besides currently due to extensive popularity of devices like digital cameras, intelligent mobile devices, techniques proposed in [51, 52] deals with social/community-contributed image retrieval/understanding focusing on the transformation of images and by analyzing the content. The technique proposed in [51] is based on the deep learning framework known as weakly-supervised deep metric learning. The technique proposed in [52] proposes a weakly supervised deep matrix factorization algorithm that can deal with the incomplete, noisy or subjective tags while eliminating the redundant or noisy visual features.

To maintain the privacy of the image while transmitting it over the internet, the technique proposed in [49] performs image compression as well as encryption sequentially. To do so, it employs deep learning-based algorithms. At first, it uses Stacked Auto Encoder (SAE) to compress the image. Then to encrypt this compressed one, it uses chaotic logistic map. To encrypt a batch of images where each image is encrypted with an autonomous sequence, another deep learning-based technique is proposed in [50] that also employs a SAE to generate two chaotic matrices. The first matrix is used to generate a total shuffling matrix that shuffles the pixel positions on the input image. Then the second matrix is used to generate the series of autonomous sequences that establishes confusion between the shuffled image and the cipher image. However, the shortcoming of this technique is, it cannot handle input images with many sizes.

#### **2.4.1 Visual Cryptography Followed by Steganography**

To ensure the image secrecy, the hybrid technique proposed in [6] is known as VC followed by steganography. It splits the input image into multiple shares using VC and converts pixels of each share into binary values. Similarly, pixels of the cover image that is used for transmitting the input image is also converted into binary values. Then LSBs of each chunk of each share are computed from that binary values of cover image and replaced one by one bit with the binary values of the input image [6]. Here, steganography hides share images generated by VC into the LSBs of the pixel values in the cover image.

VC is done by k-n secret sharing, where image is divided into multiple shares. Pixel is the smallest unit constructing a digital image in which each pixel of a 32-bit digital color image is divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits [20]. Alpha part

represents degree of transparency. This type of VC technique is insecure as the reconstruction is done by simple OR operation. After this process shares are covered by image called stego image that is used to cover the shares and original image is extracted by using (Discrete Cosine Transform) DCT method. DCT transforms image from spatial domain to frequency domain [9]. We convert secret object into binary form and hides the bits chosen in middle and high frequency coefficients. DCT decomposes signal into low, middle and high frequency coefficients [9]. The secret image is hidden in high and middle frequency regions but not in lower region because human visual system is more sensible to modifications that may occur in lower frequency band [20].

Visual secret sharing method using secret key steganography proposed in [34]. Here at sender, secret message of predefined font is encrypted using secret key. An encrypted secret message is further encoded in shares to get two layered security. Moreover, these encoded shares are modified as per cover message while keeping cover message unchanged. At receiver, both shares are required for first layer of decoding. This decoding reveal cover share only whereas due to low signal to noise ratio (SNR) of secret message, it is not visible and hidden within superimposed share [34]. Further, by applying proposed digital invisible ink using VC (DIIVC) algorithm, encrypted secret message is revealed. Notably, DIIVC algorithm requires appropriate threshold value to provide undistorted encrypted secret message. Finally, secret message is revealed by second layer of decoding using authentic secret key.

#### **2.4.2 Steganography Followed by Visual Cryptography**

The hybrid technique proposed in [7] is known as steganography followed by VC where the input image is embedded inside a cover image using steganography and then the embedded image is divided into different shares using VC. At first both the input image and the cover image are converted into pixel and then to binary data. After computing the LSBs of each chunk of the cover image and replacing one by one bit with the binary value of input image, this binary image is split into multiple shares.

A novel hybrid technique proposed in [21] based on steganography and cryptography to embed data in color images. This technique shows its larger capacity for hiding data than other technique without loss of imperceptibility integer wavelet transform and genetic algorithm. The technique is very efficient, especially when applied to those images whose pixels are scattered homogeneously and for small data.



## 2.5 Our Contributions

Discussed upstairs these techniques are substantially weaker than cryptography-based message encryption techniques. Thereby while they are applied separately or jointly, they possess various limitations. Different from the above techniques, to encrypt the image more securely, the hybrid technique proposed in this thesis unifies ‘the benefits of cryptosystems not relying on any specific key/keys’ along with ‘the strength of the cryptosystem relying on a specific key’. For this purpose, it consecutively combines VC, steganography and OTP altogether. Here at first VC splits pixels of the input image into  $2^n$  shares, where  $n \geq 1$ . Note that while the value of  $n$  increases, the level of secrecy also increases. Now pixels of each share are transformed into their corresponding binary values. Then instead of using a cover image, it only detects LSBs from each chunk of binary values of each share exploiting steganography. Lastly, it applies OTP encryption technique that possesses ‘perfect secrecy’ and cannot be cracked on LSBs using random OTP secret key to generate the final cipher image. Besides before sending the OTP key to the receiver, it is transformed into integer value to encrypt it using paillier cryptosystem for the decryption purpose. Thus, the successive exploitation of several techniques increases the level of secrecy of the input image significantly while maintaining its quality.

## CHAPTER III

### Cryptographic Tools and Proposed Technique

The proposed technique exploits several cryptographic tools. These are: VC, steganography, OTP and Paillier cryptosystem. Where the image encryption technique consists of several stages like random OTP secret key generation, image encryption and image decryption. This chapter describes the preliminary knowledge of required cryptographic tools and proposes technique.

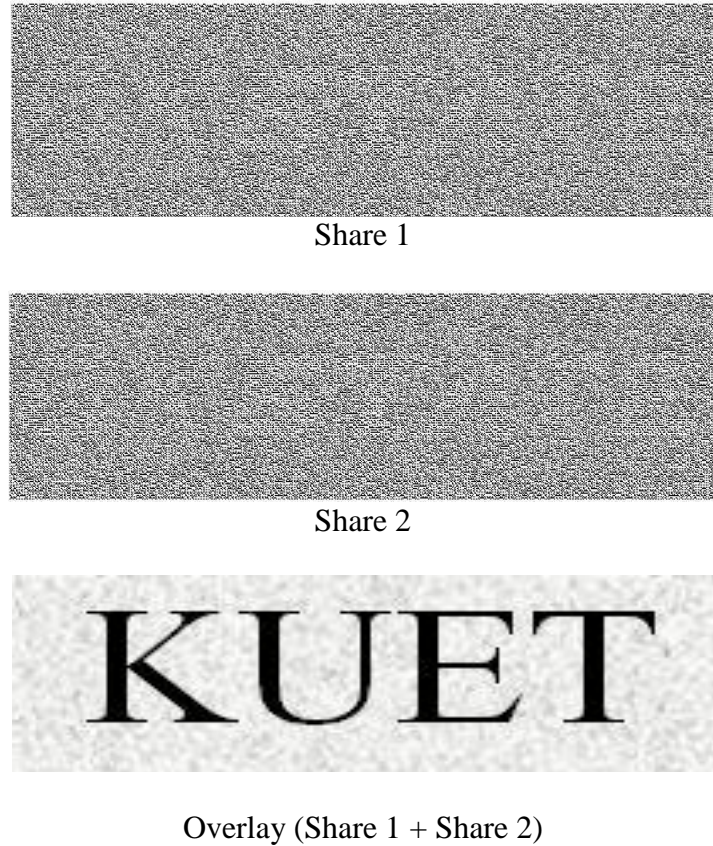
#### 3.1 Visual Cryptography (VC)

The technique VC is introduced by Naor and Shamir in [1] for monochrome images. It demonstrated a visual secret sharing technique, where an image broken up into  $n$  shares so that only someone with all  $n$  shares could decrypt the image, while any  $n - 1$  shares revealed no information about the original image. Each share is printed on a separate transparency, and decryption are performed by overlaying the shares. When all  $n$  shares are overlaid, the original image would appear.

It is a cryptographic technique which allows visual information i.e. image, text etc. to be encrypted in such a way that decryption can be performed by the human visual system, without any complex cryptographic algorithms [1]. The secret image splits into two or many shares [4], each of which individually cannot provide any information about the secret image. The secret image can be only retrieved when the desired numbers of shares are superimposed with one another. During decryption, all the shares are needed to be stacked that reveals the secret image. Therefore, it does not require any complex calculation as like other traditional cryptography techniques.

Basically, VC operates on binary inputs hence natural images must be converted into halftone images using density of dots to simulate grey level. Here, binary data can be displayed as transparent when printed on transparent screen. In VC, each pixel of the image is divided into smaller blocks and always has the same number of black and white (transparent) blocks [1]. For example, if a pixel is divided into two parts (2 subpixels), there will be one

white and one black blocks. Similarly, if the same pixel is divided into four equal parts (4 subpixels), there will be two white and two black blocks. The share images in the Fig. 3.1 presented the working procedure of VC.



**Figure 3.1:** Working Procedure of VC















From Fig. 3.1 we can observe that the original image is broken up into two parts which are its shares i.e. share-1 and share-2. Separately these shares look like random noise but when combining all the shares that reveals the original image.

The basic model of VC is introduced in [1] where an input image is divided into  $2^n$  shares where  $n$  is already mentioned. Later, only someone with all shares can decrypt the image while someone with any  $2^n-1$  share(s) can reveal no information about the input image.

For monochrome image, an image is a collection of binary data 0 and 1 displayed as black and white pixels. Where, VC splits each pixel into white and black sub-pixels which is shown in Table 3.1. If the pixel is white, then any one row among the top two rows is chosen to generate share 1 and share 2. If the pixel is black, then any one row among of the bottom two rows is chosen to generate share 1 (S1) and share 2 (S2).

At the time of superimposing each pixel of share 1 and share 2, the retrieval of the pixel is shown in the last column of Table 3.1.

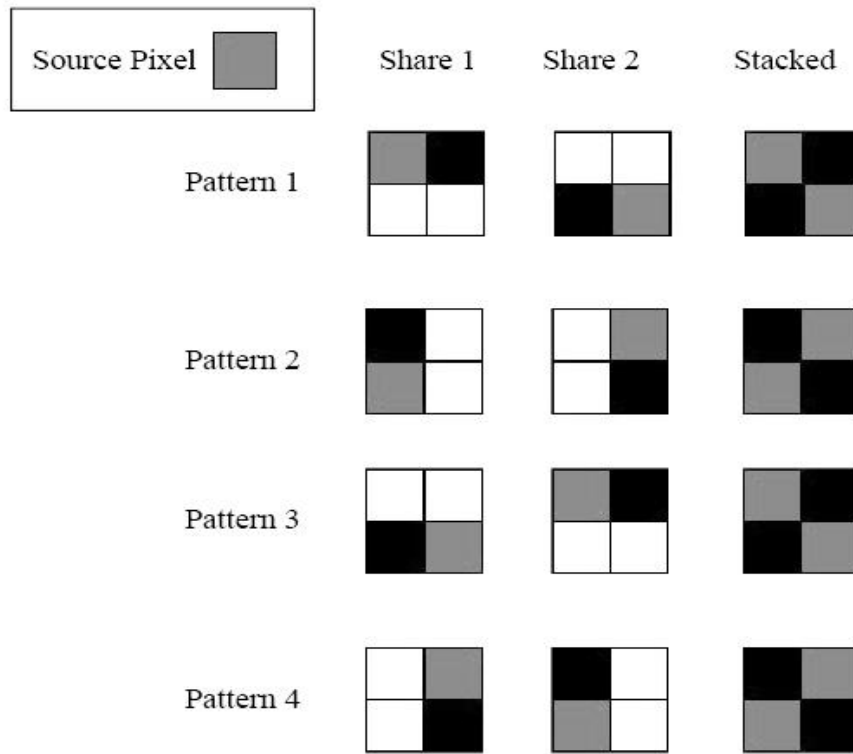
**Table 3.1:** VC Technique for Encoding the Pixels into Two Shares [1].

Pixel		S1	S2	S1 + S2
	$p = 0.5$			
	$p = 0.5$			
	$p = 0.5$			
	$p = 0.5$			

For color image as described in [12], there are mainly three inputs in the system i.e. RGB as well as RGBA color model. VC splits the input image into  $n$  shares and each RGB share is converted into 24-bit color image. The main parameters of VC include image contrast and the number of sub pixels of the retrieved image. The contrast of color image is comparatively different between the original and the retrieved image. A source image of  $m \times n$  pixels needs two pieces of host images of the same size where  $m$  and  $n$  represent the number of rows and columns respectively. Mainly three processes build the overall system i.e. pixel extraction, encryption and decryption.

In the pixel extraction phase the same positioned pixel from the RGB images are extracted and considered for the encryption process. For the inputs of the RGBA values, the technique reads from the pixel  $(0, 0)$  to the pixel  $(m, n)$ . For example, when a pixel is scanned, a green and a brown pixel are obtained from the hosts, and a blue pixel is obtained from the source

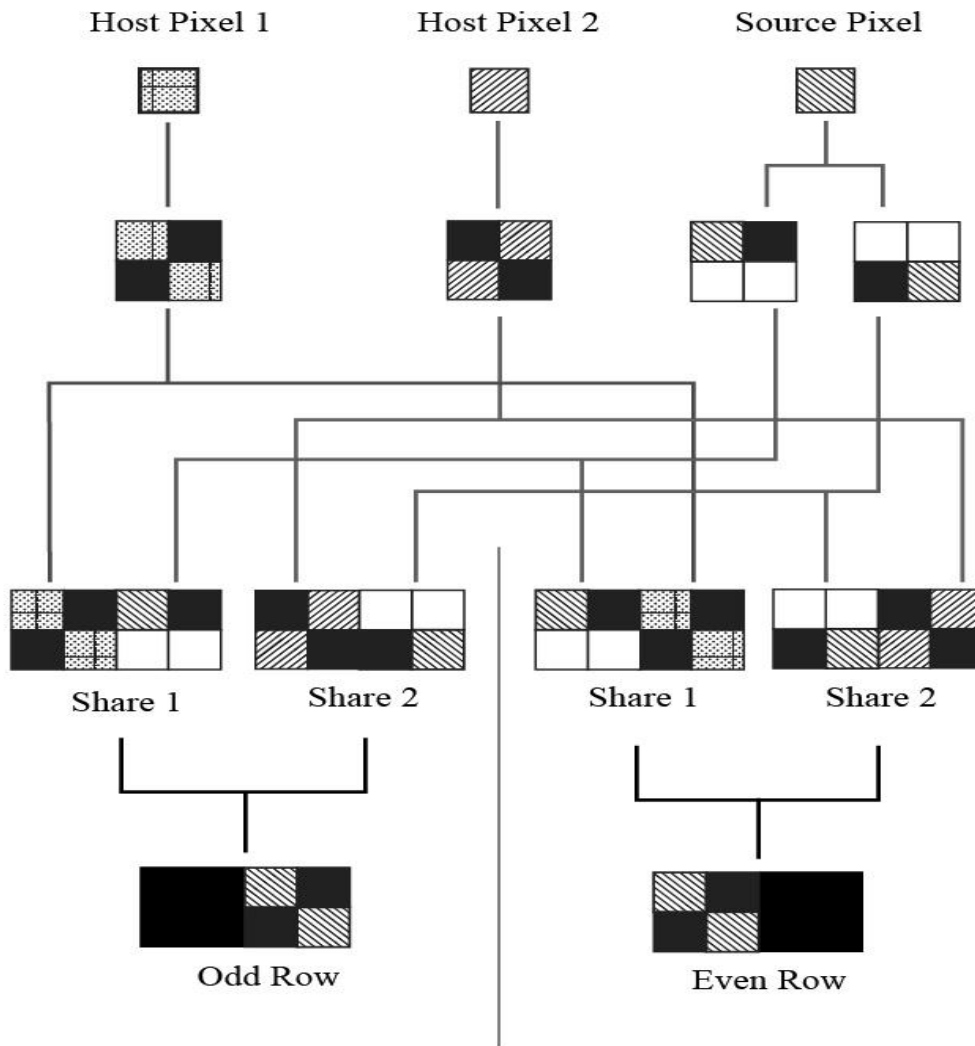
image. Now the problem is to encrypt the blue pixel with these share pixels so that the superimposed pattern reveals a bluish pattern.



**Figure 3.2:** Expansion and Encryption of Source Pixel [12]

In the encryption process, two share images of size  $4m \times 2n$  are created. At first, the host pixels are expanded according to Table 3.1. Now the expanded pixel patterns are selected randomly. But whichever it takes, after the superimposing, the block turns to black. It happens because the opposite diagonal positions are colored black.

Next, the source pixel is expanded. It is done according to Fig. 3.2. In this process, four pixels are used to represent one pixel. Among the four pixels, one is the source color, one is black and the rest two is transparent. The patterns are selected carefully so that the superimposing gives two black pixels and two color pixels. After the expansion process, three pieces of  $2 \times 2$  blocks of pixels are obtained. These blocks are used to create the pixel patterns for the shares. The overall process is shown in Fig. 3.3.



**Figure 3.3:** Encryption and Decryption for Color Image [12]

Say  $H_1$  and  $H_2$  are the host patterns and  $S_1$  and  $S_2$  are the source pixel patterns selected for the procedure. The final pixel patterns for the shares are generated by placing  $H_1$  and  $S_1$  together and  $H_2$  and  $S_2$  together. For the odd rows,  $S_1$  and  $S_2$  are placed at the right of  $H_1$  and  $H_2$  respectively. For the even rows, it does the opposite. Two different actions for different rows are done for the perfect hiding of the source pixel. Now whatever the row is, the stacked pattern which is of the size  $4 \times 2$ , consists of 2 color pixels and 6 black pixels.

### 3.2 Extended Visual Cryptography (EVC)

Extended Visual Cryptography (EVC) [37] is a type of cryptography which encodes several images in the way that when the images on transparencies are stacked together, the hidden

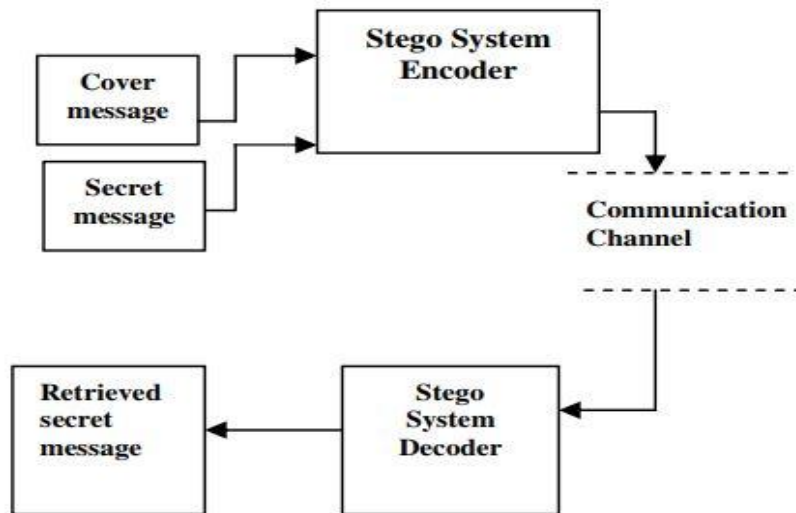
message appears without a trace of original images. EVC reconstructs the image by stacking some meaningful images together that successfully works for natural images not only binary images (i.e. text images) [37]. It is a cryptographic technique which encodes several images in the way that when the images on transparencies are stacked together, the hidden message appears without a trace of original images. Decryption is performed directly by the human visual system with no special cryptographic calculations.

The technique of EVC in [37] for natural images is used to produce meaningful binary shares which takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. Generally, VC suffers from the deterioration of the image quality.

### **3.3 Steganography**

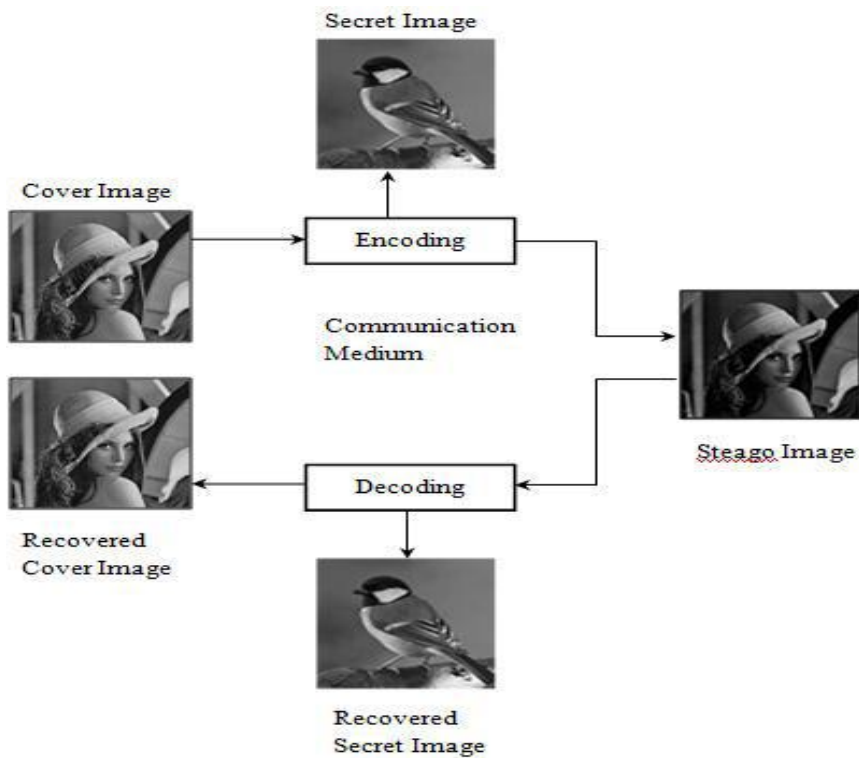
Steganography [2] is the science of invisible communication that is an art of hiding information or data inside another data. The main objective of steganography is to protect the contents of secret information where secret information is communicated through unknown carrier data. The embedding of secret information is done in such a way that very existence of the secret information is invisible to any viewers where carrier's data could be many forms such as images, audio, video, text or any other data. A good steganography technique aims at three aspects: capacity (maximum information that can be hidden inside the cover image), visual quality of stego-image must remain unchanged (imperceptibility) and robustness [2].

Digital steganography has many applications in our daily life. When sensitive data is transmitted from one place to another they must be protected from modifying, copying and claiming their ownership [4]. There must be a way to provide integrity, availability, confidentiality services to the information exchanged where will all these services provide steganography [5]. Basic steganographic technique shown in Fig. 3.4 where the object which is used to hide secret information is called cover object. Stego message is referred as a message that is obtained by embedding secret message into cover message where the hidden information may be either plain text, or images etc.



**Figure 3.4:** Basic Steganographic System

In steganography [6], the image media are most popular as a carrier data because of the existence of substantial number of redundant bits in it. The hidden information may be text, cipher text or any other digital form that represented as a bit stream can be embedded using steganography technique. The basic encryption and decryption process of steganography technique shown in Fig. 3.5.



**Figure 3.5:** Encryption and Decryption Process of Steganography Technique.



Steganography is most commonly implemented in image files. However, embedding data into image changes its color frequencies in a predictable way. To overcome this predictability, we propose the concept of multiple cryptography where the data will be encrypted into a cipher and the cipher will be hidden into a multimedia image file in encrypted format. Hiding messages in images in such a manner that the alterations made to the image are perceptually indiscernible. However, the question whether the result in images that are statistically indistinguishable from untampered images has not been adequately explored. In this thesis we look at some specific image-based steganography techniques which only altered its bit position or LSB based steganography.

However, in our proposed technique in this thesis instead of using the cover image, random secret key is exploited to encrypt LSBs of each chunk of each share applying OTP encryption technique which increases the security of the image as well as makes the encryption and decryption process faster than that of using the cover image. Here the number of LSBs of each chunk of each share must be equal to the number of bits of OTP key.

### **3.3.1 Least Significant Bit (LSB) Technique**

LSB is the most common technical embedding technique for hiding data inside the cover file. The amount of data to be hidden inside the image depends upon the size of the image and the number of LSB to be used. LSB insertion works simply just by swapping LSB of every pixel in cover image with the data to be hidden. Altering the LSBs results in a color slightly changed from the original one which is unable to be detected by human eye. The reason being human eye is not sensitive enough to recognize the difference in color between pixels which differs by just 1 unit. Advantages of LSB techniques providing strong encrypting key to secure data and encryptions of the message, so that who extracts it must also decrypt it before it makes sense.

The technique proposed in [6] to ensure the secrecy of images that combines VC and steganography. At first it splits the input image into multiple shares using VC and converts pixels of each share into binary values. Similarly, pixels of the cover image that is used for transmitting the input image is also converted into binary values. Then LSBs of each chunk of each share are computed from that binary values of cover image and replaced one by one bit with the binary values of the input image. Here, steganography hides share images generated by VC into the LSBs of the pixel values in the cover image.

The technique proposed in [30], that hides the data inside images using dissimilarity of LSB embedding system. Then embedding data is hidden in the LSB of each byte in the image. By using stego analysis techniques, data hidden inside an image using normal LSB technique is applied. But not only it hides the user's data or secret data within an image, but it also compresses & encrypts the user's data [30].

### 3.3.2 LSB Implementation for Monochrome Image

LSB is the lowest bit in a sequence of binary number. Say, if bits of binary number are 10101001, the LSB is far right 1. The LSB based steganography is used to insert the secret data into the LSB of the pixel values in a cover image [30]. For example, to insert a bit of secret information say **01010001** in an 8th bit of some or all the bytes of a cover image is as follows:

*Pixel of Cover image:*  
(10101111 11101001 10101000)  
(10100111 01011000 11101001)  
(11011000 10000111 01011001)

*After change, the LSB:*  
(1010111**0** 1110100**1** 1010100**0**)  
(1010011**1** 0101100**0** 1110100**0**)  
(1101100**0** 1000011**1** 0101100**1**)

Here, secret bits **01010001** are embedded into first eight bytes of the cover image and only three bits are changed. This minimal change is not noticed by the human visual system, hence the LSB insertion is very easy to implement and most popular method in steganography technique.

### 3.3.3 LSB implementation for Color Image

LSB insertion is most common and simple technique to embed information in a color image file. The LSB of some or all the bytes inside an image is changed to contain a bit of the secret message. When using a 24-bit image, a bit of the red, green and blue color components can be used to store 3-bits of secret message in each pixel by LSB insertion as in 24bit image [10]. Color variations of each pixel are derived from three primary colors as red, green and

blue where each color represented by 8-bits. Thus, a  $1024 \times 768$ -pixel image can hide 2,359,296-bits (294,912-bytes) of secret data. For example, a grid for 3 pixels of a 24-bit color image, using 9- bytes of memory can be as follows:

(00101101 00101010 11011101)  
(01101001 11000101 01010101)  
(11010010 11011010 10100101)

When the number 150, which binary representation is **10010110**, is inserted into the LSBs of this part of the image, following grid results:

(00101101 00101010 110111**00**)  
(01101001 110001**00** 01010101)  
(11010011 11011010 10100101)

The bits in bold are the only bits that are changed in the 8-bytes that are used to hide the number 150. On an average, only a few of the bits in an image modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary color adding up to 16 million (16,777,216) color combination, changing the LSB of a pixel results in slight changes in the intensity of the colors which are too small to be recognized by the human eye. So, the message is effectively hidden. One of the disadvantage of the LSB insertion is that it requires a large cover image to create a usable amount of hiding space.

### 3.4 One Time Pad (OTP)

Due to the boundless development of Internet and communication technologies, the extensive use of images in numerous areas such as military, engineering, medical, science, art, entertainment, advertising, education has become unavoidable. With the increasing use of digital techniques for transmitting and storing images, the fundamental issue of protecting the confidentiality, integrity as well as the authenticity of images has become a major concern. Though the rapid improvement of attacking skills the safety systems having respective drawbacks and limitations and the dilemma between security performance. By considering these, a well-known realization of perfect secrecy with truly random key generation technique is the one-time pad (OTP) [8] for use in automatic encryption and decryption of messages.

In cryptography, OTP is an encryption technique that cannot be cracked in which each character of the plaintext is combined with a character from a random key stream [8]. The random key generation system of OTP has at least the same length as the actual message (i.e. the plaintext) and consists of truly random numbers [7]. Each letter of the plaintext is added to one element from the OTP using modulo-addition. This results in a ciphertext that has no relation with the plaintext when the key is unknown. At the receiving end, the same OTP is used to retrieve the original plaintext. For this to work, the following rules are mandatory:

- ❖ The OTP should consist of truly random characters.
- ❖ The OTP (i.e. the key) should have the same length as the plaintext.

Only if the above rules are strictly obeyed, the OTP is safe. The OTP encryption is an XOR (exclusive-OR) operation between the original message bit and the key bit.

OTP [8] encryption technique is applicable for binary data, and it possesses perfect secrecy. Here the same secret key is shared separately by the sender and the receiver for encryption and decryption purposes respectively. Also, already told that, the length of the key is as same as the length of the message to be encrypted. In this technique, a plaintext is paired with the secret key where usually XOR operation is applied. Thus, each bit of the plaintext is encrypted by combining it with the corresponding bit from the pad. The data encrypted with the key based on the randomness have the advantage that theoretically there is no way to “break the code” by analyzing a succession of data.

### **3.5 Paillier Cryptosystem**

Homomorphic encryption technique provides a way to outsource computations to the cloud while shielding the confidentiality of the data. Dealing with the huge and growing data sets that are being managed today, reputable encryption performance is a major step for practicality of homomorphic encryption technique. Paillier [13] technique is the most well-known, and maybe the most effective partially homomorphic encryption technique. It is so fastest probabilistic homomorphic technique than RSA in decryption.

The distinguishing technique used in public key cryptography using asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys: a public key and a private key. The private key is kept secret, whilst the public key may be widely distributed. Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key. The

keys are related mathematically, but the private key cannot be feasibly (i.e., in actual or projected practice) derived from the public key.

Paillier [13] is a public key cryptosystem which is described below.

1. Key Generation:

- a) Two large primes  $p$  and  $q$  are chosen randomly and independently of each other such that  $\gcd((p, q), (p-1)(q-1)) = 1$ .
- b) Now  $n = p \cdot q$  and  $\lambda = \text{lcm}(p-1; q-1)$  is computed.
- c) A random integer is selected  $g$  where  $g$ 's order is a non-zero multiple of  $n$  (since  $g = (1+n)$ ). Ensuring that  $n$  divides the order of  $g$  by checking the existence of the following modular multiplicative inverse:  $u = L(g^\lambda \bmod n^2)^{-1} \bmod n$ , where function  $L$  is defined as (Lagrange function)  $L(u) = u^{-1} / n$  for  $u \equiv 1 \pmod n$ .
- d) Now the public key is  $(n, g)$
- e) The private key is  $(p, q, \lambda)$ .

2. Encryption:

- a) Plaintext or message is  $m$  where  $0 < m < n$ .
- b) Finding a random  $r$ . where  $0 < r < n$
- c) Then the ciphertext is  $c = g^m \cdot r^n \bmod n^2$ .

3. Decryption:

- a) The ciphertext  $c < n^2$ .
- b) Retrieval of plaintext  $m = L(c^\lambda \bmod n^2) / L(g^\lambda \bmod n^2) \bmod n$ .  
Or in same expression  $m = L(c^\lambda \bmod n^2) \cdot \mu \bmod n$

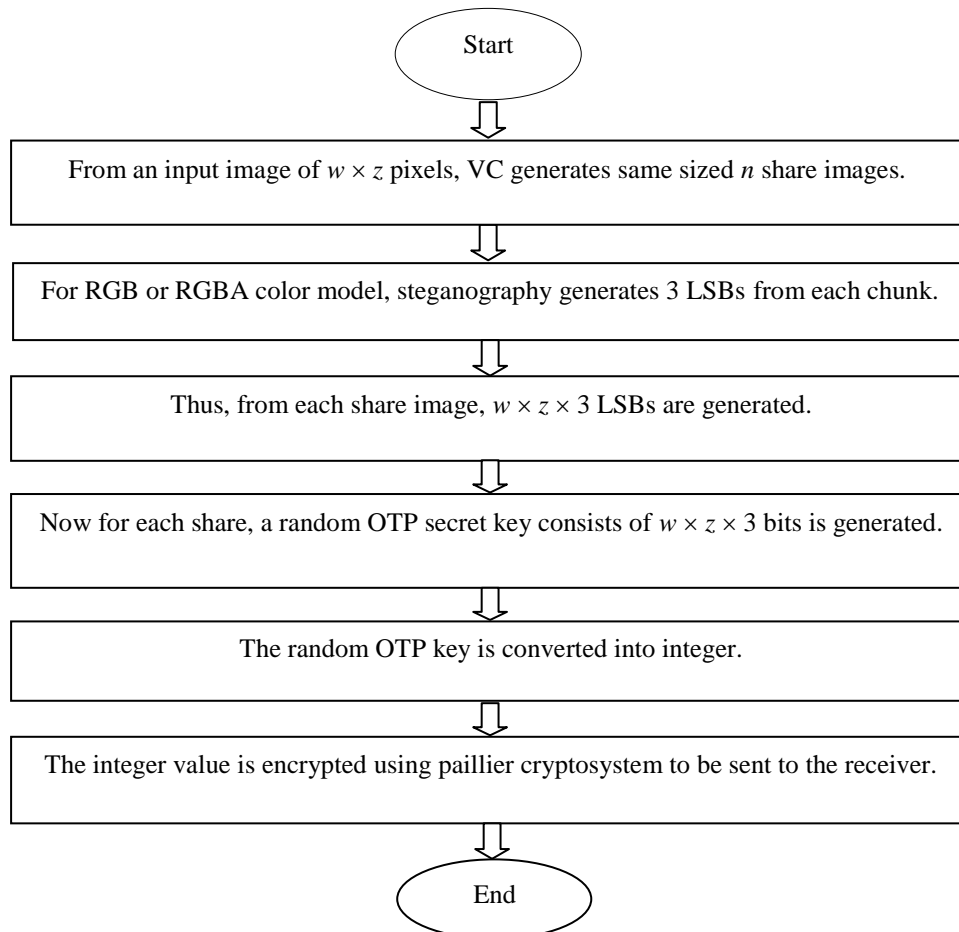
Looking at the form of the equation, one will see that the decryption will be done by first removing the random part  $r^n$ , then retrieving the exponent  $m \bmod n^2$ .

### 3.6 Proposed Technique

The proposed image encryption technique consists of several stages. These are: random OTP secret key generation, image encryption and image decryption, as described below.

### 3.6.1 Random OTP Secret Key Generation

To generate the OTP key to be used for encryption and decryption purpose, a random secret key is generated where in binary the length of the key is equal to the number of LSBs within each chunk of each share.



**Figure 3.6:** Flow Chart of Random OTP Secret Key Generation Process.

Here already mentioned that at first the exploitation of VC generates  $n$  share images from an input image of  $w \times z$  sized pixels where each share also consists of the same number of pixels. Here  $w$  and  $z$  both are positive integers where the image consists of  $w$  rows and  $z$  columns. Now for RGB or RGBA color model steganography is applied which generates  $(24 / 8) = 3$  LSBs from each chunk. Thereby from each share image, there exists  $w \times z \times 3$  LSBs. Therefore, the number of bits of OTP key will also be equal to  $w \times z \times 3$  bits.

Before sending the key to the receiver, it is transformed from binary to integer value and then encrypted using the public key of Paillier cryptosystem. The receiver decrypts it using

its secret decryption key of Paillier cryptosystem, transforms it from integer to binary to be used for image decryption. Fig. 3.6 shows the key generation process.

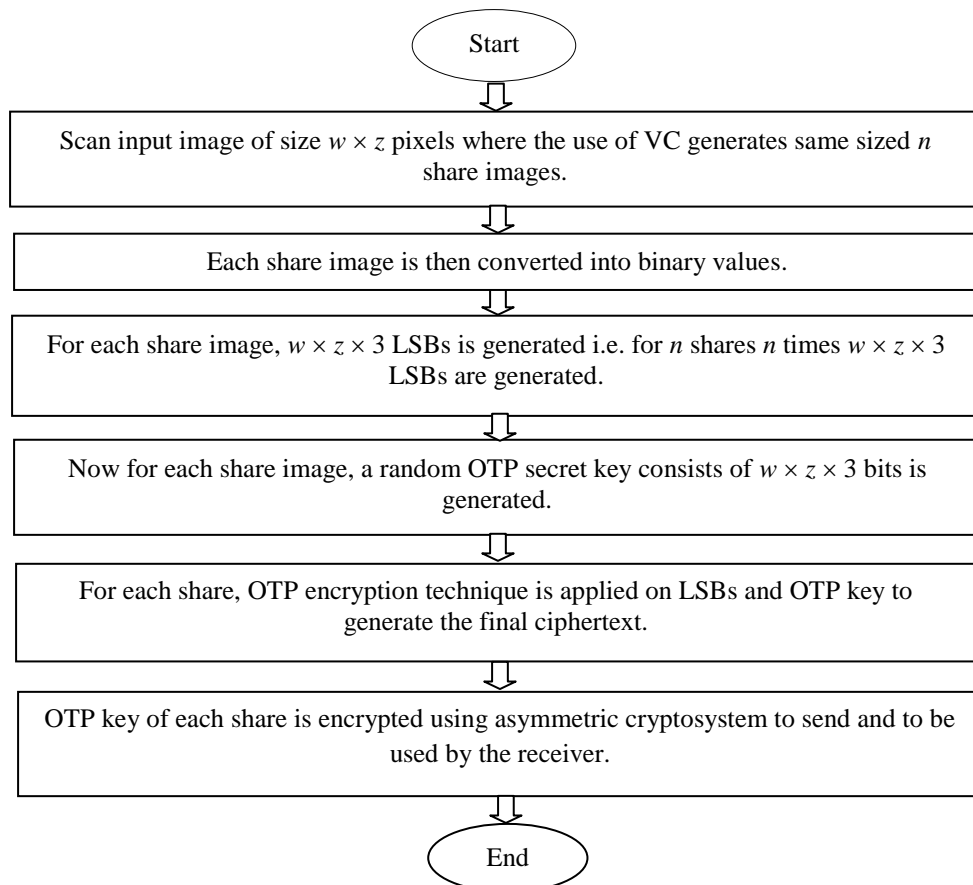
### 3.6.2 Image Encryption Technique

This section describes the technique to encrypt the image. Fig. 3.7 depicts the process.

*Step 1:* In the proposed technique at first the sender scans the input image of  $w \times z$  pixels. Now VC technique is applied on the input image that generates  $2^n$  share images consisting of  $w \times z$  pixels where  $n$  is greater than or equal to one.

*Step 2:* Converting pixels of each share image into binary values.

*Step 3:* Using steganography, the LSBs from each chunk of each share are computed. Here for RGB or RGBA color model, each chunk generates 3 LSBs. Thus, for each share totally there are  $w \times z \times 3$  LSBs.



**Figure 3.7:** Flow Chart of Image Encryption Technique.

*Step 4:* Now for each share, a random binary OTP secret key of  $w \times z \times 3$  bits are generated. Thus, for  $n$  shares,  $n$  times  $w \times z \times 3$  bits are generated separately.

*Step 5:* For each share, the final ciphertext is generated by applying OTP technique over LSBs along with OTP secret key. For example, for the first share image first  $w \times z \times 3$  bits and similarly for the  $n$ -th share image  $n$ -th  $w \times z \times 3$  bits are used as the OTP keys.

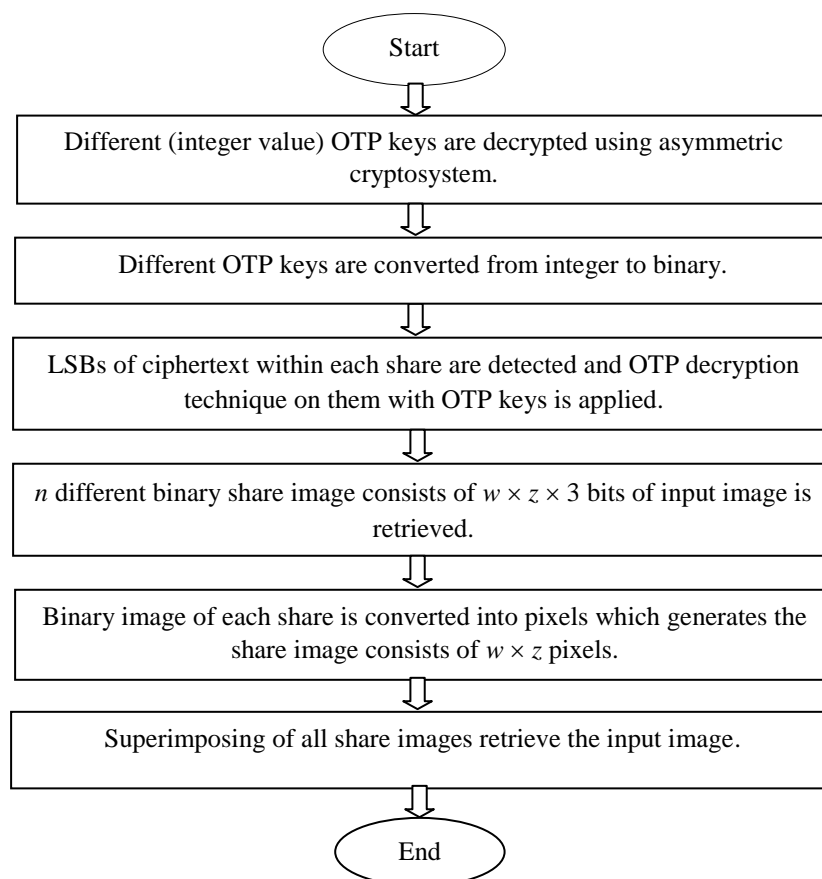
*Step 6:* At last the OTP keys are also encrypted by using asymmetric cryptosystem to send them to be used by the receiver.

### 3.6.3 Image Decryption Technique

This section describes the decryption process of the image. Fig. 3.8 depicts the process.

*Step 1:* At first the receiver decrypts  $n$  different OTP keys using its secret key of asymmetric cryptosystem.

*Step 2:* Each different OTP key is converted from integer to its corresponding binary value. Thus, it generates  $n$  different OTP keys of  $w \times z \times 3$  bits.



**Figure 3.8:** Flow Chart of Image Decryption Technique.



*Step 3:* The receiver detects the LSBs of ciphertext of each share image, and then applies OTP decryption technique (XOR operation) on them along with OTP secret key.

*Step 4:* This operation retrieves  $n$  different binary share images each consists of  $w \times z \times 3$  bits of the input image.

*Step 5:* The binary image of each share image is converted into pixels which generate the share image of size  $w \times z$  pixels.

*Step 6:* Finally, the superimposing of all share images retrieves the original input image.

# CHAPTER IV

## Experimental Studies

Our experiments performed on diverse sizes of images with a numerous formats of color images explicitly, 'jpg', 'bmp', 'png', 'gif', 'tif' etc. Where the observation and analyzing results from various aspects such as histogram analysis, salt and pepper noise attacks, chosen-plaintext attack (CPA) etc. are considered. This chapter briefly describes these experimental studies step by step with executional time and comparisons with various techniques.

### 4.1 Experimental Setup

A prototype system of the proposed technique has been developed under the environment on Intel(R) Core™ i5-6200U 2.40 GHz x64-based processor with 8 GB of RAM running on Windows 10 operating system. The prototype has been developed in programming language MATLAB 16.0 [14]. Color images of various formats namely, 'jpg', 'bmp', 'png', 'gif', 'tif' etc. of same dimensions i.e.,  $200 \times 200$  pixels have been considered for the experiment. Here some images have been collected from our own sources that are shown in first column of Fig. 4.1 (a), Fig. 4.1 (b) and Fig. 4.1 (c) and some are benchmark images obtained from [41] that are shown in first column of Fig. 4.1 (d), Fig. 4.1 (e) and Fig. 4.1 (f) are used to depict the output of the proposed image encryption and decryption techniques.

### 4.2 Output of Encryption Step

This section presents the output of the encryption step where consecutively VC, steganography and OTP are applied.

#### 4.2.1 Output after Applying VC

*Step 1:* Scan the input images of Fig. 4.1 (a), (b), (c), (d), (e) and (f) where the sizes of the images are different but as already said that their dimensions of pixels are same. Here the format of the first image is .jpeg while the second one is .png and the rest of the images are .jpeg.

Step 2: After applying VC, two share images are generated i.e. *share1* and *share2* which are presented in the third and fourth columns of Fig. 4.1.

#### 4.2.2 Output after transforming into binary image

The pixels of the share images presented in the third and fourth columns of Fig. 4.1 are now converted into binary images. Here the output of a portion of share 1 image of Fig. 4.1 (a) is as follows:

```
01110101011110000111011101110111011100101111001101111010011110010111100100
111010110010101011111001010010111111010100010100010100000111010111011010010
100010100101001011001
```

#	input image	share 1	share 2
(a)			
(b)			
(c)			
(d)			



**Figure 4.1:** Output Image after Applying VC Technique.

#### 4.2.3 Output after Applying Steganography with OTP

*Step 1:* Applying steganography, LSBs from each chunk of binary image of each share are detected where the numbers of LSBs within each share are  $150 \times 188 \times 3 = 84600$ . Here LSBs within a portion of the binary image of share 1 of Fig. 4.1 (a) are shown as bold:

```
01110101011110000111011101110111011100101111001101111010011110010111100100
111010110010101011111100101001011111110101000101000101000001111010111011010010
100010100101001011001
```

*Step 2:* A random OTP secret key is generated where the number of bits is 84600. A portion of the key is as follows:

```
110100010101010101100101010101110101001101010010010100101101110000101110010
111010
```

*Step 3:* On LSBs OTP encryption operation (i.e. XOR operation) is applied using OTP key. A portion of the generated ciphertext is shown in Table 4.1.

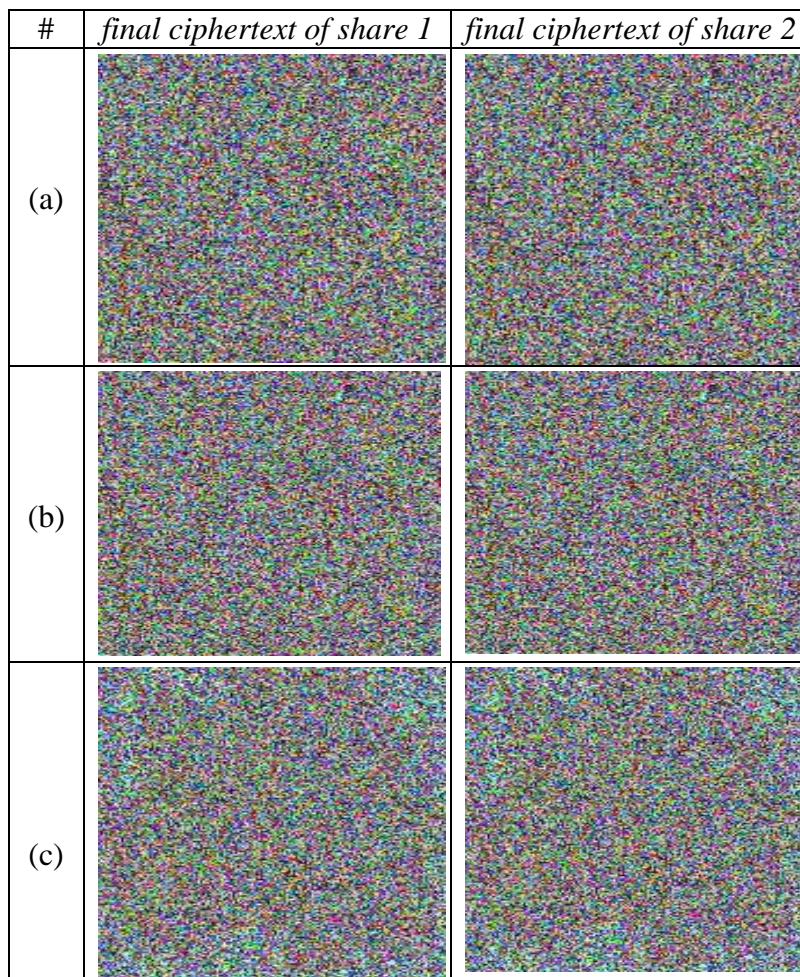
**Table 4.1:** Generated Final Ciphertext (A Portion)

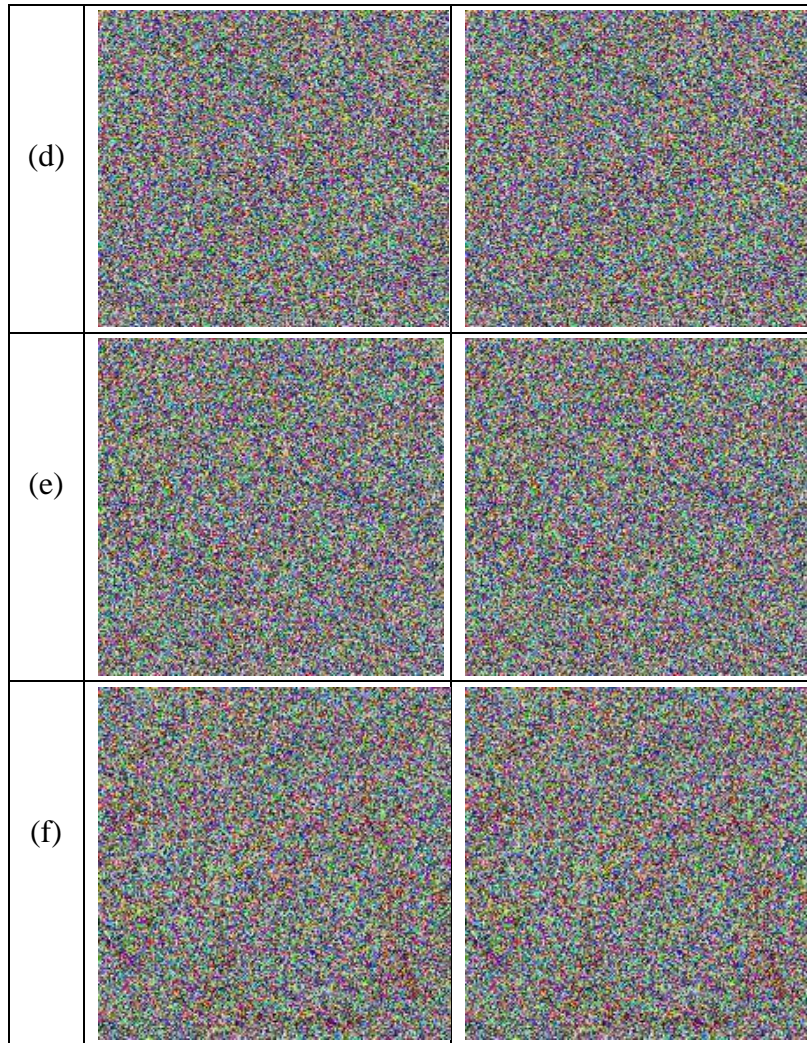
LSBs	0111010101111100001110111101110111101111001				
Key $\oplus$	1	1	0	1	0
Ciphertext	0	1	1	0	1

Now a portion of the final ciphertext is shown below where the changed bits are shown using red color:

0111010001111001011101110111011100111100101111001101111010011110010111100100  
111010110

Also, the pixel appearance of this binary image is shown in Fig. 4.2.





**Figure 4.2:** Pixel Appearance of Final Ciphertext of Share Images.

### 4.3 Sending OTP Secret Key to the Receiver

*Step 1:* The sender transforms OTP secret key (consists of 84600 bits) from binary to integer.

*Step 2:* The sender encrypts the OTP key using the public encryption key of Paillier cryptosystem and sends it to the receiver.

*Step 3:* The receiver decrypts the integer value of OTP key using the secret decryption key of Paillier cryptosystem and transforms it into binary value to decrypt the image.

However, the OTP key encryption process is required to only transmit it securely, not the main part of image encryption and decryption; therefore, these results are not presented herein.

## 4.4 Output of Decryption Step

### 4.4.1 Output after Applying Steganography with OTP

*Step 1:* The receiver identifies LSBs from each chunk of each share of the final ciphertext. For example, a portion of share 1 of Fig. 4.2 (a) is as follows:

011101000111100101110111011101100111100101111001101111010011110010111100100  
111010110

*Step 2:* On LSBs OTP decryption operation (i.e. XOR operation) is applied using the same random OTP secret key. A portion of the generated plaintext of share 1 of Fig. 4.2(a) is shown in Table 4.2.

**Table 4.2:** Generated Plaintext of a Share Image (a Portion)








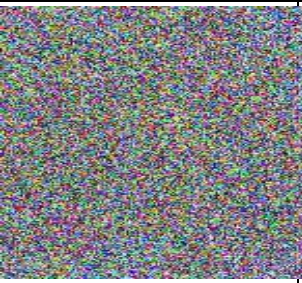




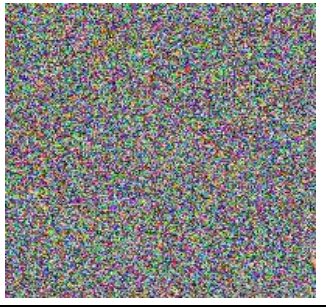
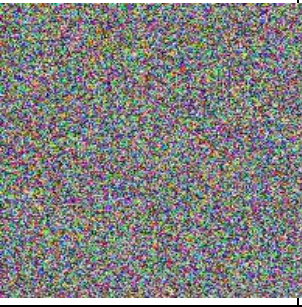

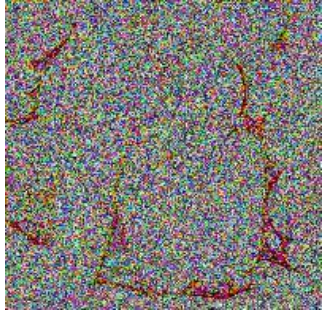
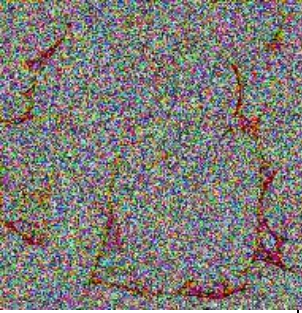

<b>LSBs</b>	0111010001111001011101110111011001111001				
Key $\oplus$	1	1	0	1	0
Plaintext	1	0	1	1	1

Now a portion of the final plaintext of share 1 is shown below where the changed bits are shown using red color:

01110101011110000111011101110111011100101111001101111010011110010111100100  
111010110

### 4.4.2 Output after Transforming Binary Image into Pixels

The binary image of each share is converted into pixels that are shown in first and second columns of Fig. 4.3. Thus, share images are generated. Finally, the superimposing of share images retrieves the input image which is shown in the third column of Fig. 4.3

Retrieved			#
<i>share 1</i>	<i>share 2</i>	<i>output image</i>	
			(a)
			(b)
			(c)
			(d)
			(e)
			(f)

**Figure. 4.3:** Retrieved Share Images and Input Images.



### 4.4.3 Final Output

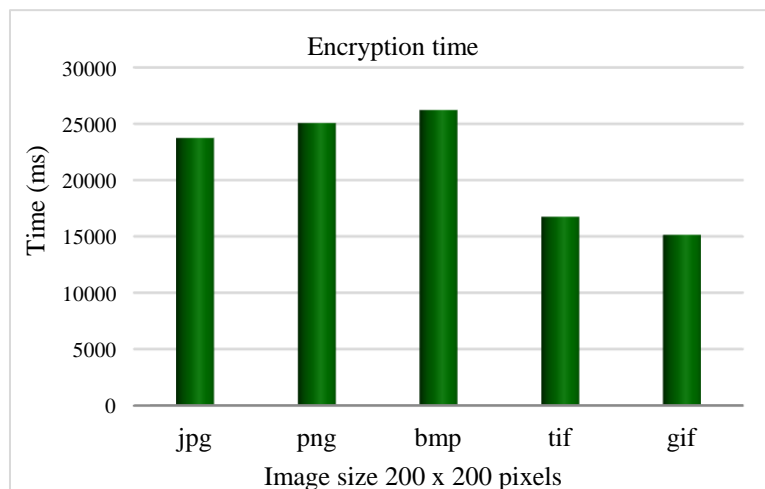
Herein represent all the shares and cipher text of those shares of each image for our experimental analysis in Fig. 4.4.

Input Image	Share 1	Share 2	ciphertext of share 1	ciphertext of share 2	Retrieved image

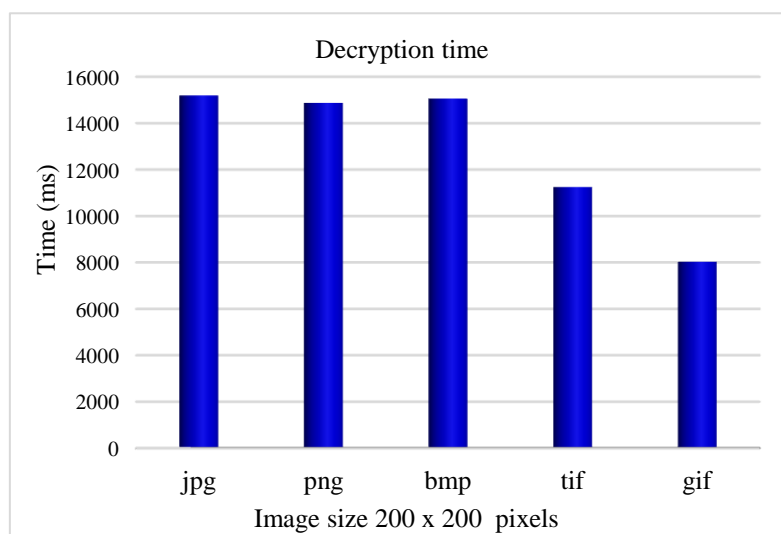
Figure. 4.4: Sample of all Experimental Images.

#### 4.5 Experimental Results and Performance Comparisons

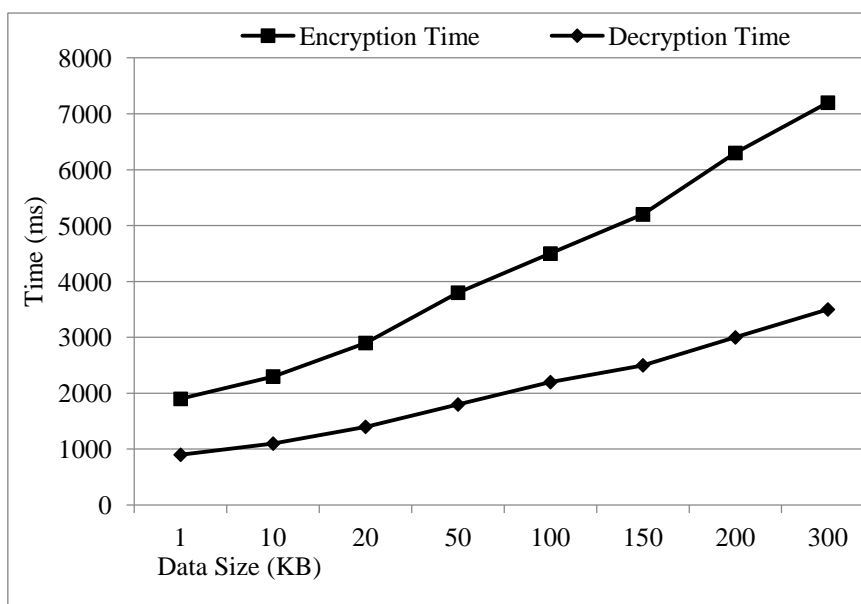
For the proposed technique, the time requirement of encryption, decryption and combined of encryption-decryption processes has been presented in Fig. 4.5, Fig. 4.6 and Fig. 4.7 respectively. Here, the encryption/decryption time has been shown under different input image sizes. As expected, with the increasing image size, encryption/decryption time also increases. However, comparatively encryption process requires more time than decryption. The reason is, in encryption stage the generation of shares of the image takes larger time than that of superimposing of shares in decryption stage.



**Figure 4.5:** Time Requirement of Encryption Process for Various Images by the Proposed Technique.



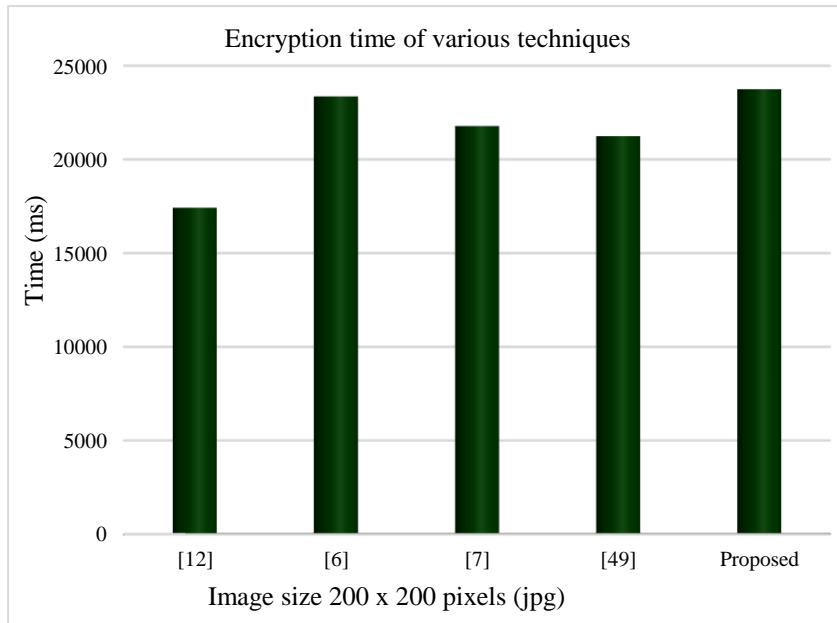
**Figure 4.6:** Time Requirement of Decryption Process for Various Images by the Proposed Technique.



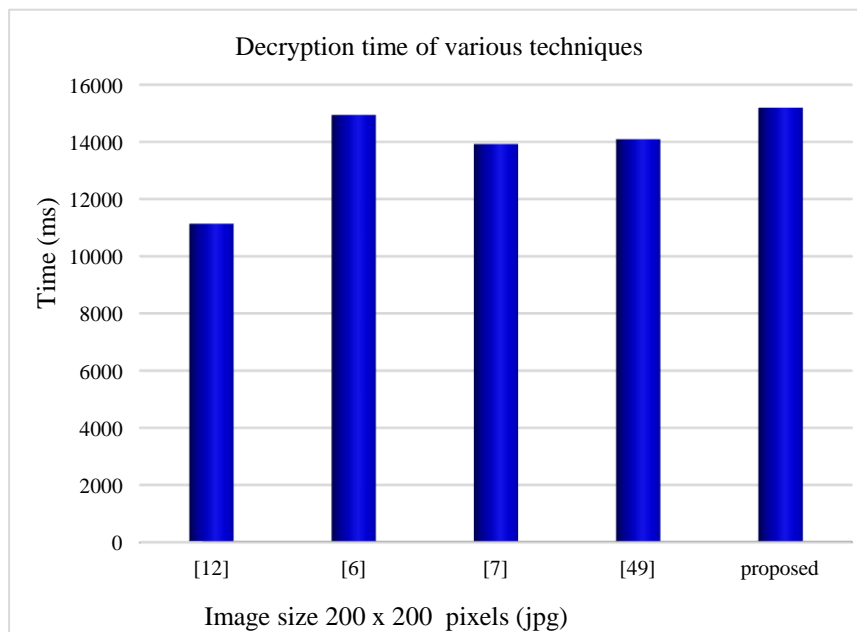
**Figure 4.7:** Time Requirement of Encryption and Decryption Operations by the Proposed Technique.

Moreover, considering the time requirement of encryption and decryption processes, the proposed technique has been compared with some other techniques proposed in [12], [6], [7] and [49] and the result of comparison has been shown in Fig. 4.8 and Fig. 4.9, respectively. Here to compare the techniques, images of same pixel sized i.e., 200 x 200 has been considered as the input although their sizes are different namely, ‘jpg’ (20.7KB), ‘png’ (64.2KB), ‘bmp’ (117KB), ‘tif’ (78.2KB) and ‘gif’ (18.7KB). The figure shows that techniques proposed in [12], [7] and [49] require faintly less time than the proposed technique.

Where the technique proposed in [12] is only VC for RGB and RGBA color model, the technique proposed in [6] is VC followed by steganography, the technique proposed in [7] is steganography followed by VC and the technique proposed in [49] is based on deep learning algorithms i.e. firstly it compresses the image applying SAE and then encrypts this one using chaotic logistic map. Although the proposed technique requires slightly more overall execution time than several compared techniques, it is not so high and a quiet reasonable one. Recalling that for the sake of providing secured image transmission over public medium, the proposed technique successively combines several techniques i.e. VC, steganography and OTP altogether. That’s why, it requires more overall execution time.



**Figure 4.8:** Comparison in Case of Encryption Time Requirement among Various Techniques.



**Figure 4.9:** Comparison in Case of Decryption Time Requirement among Various Techniques.

## 4.6 Security and Statistical Analysis

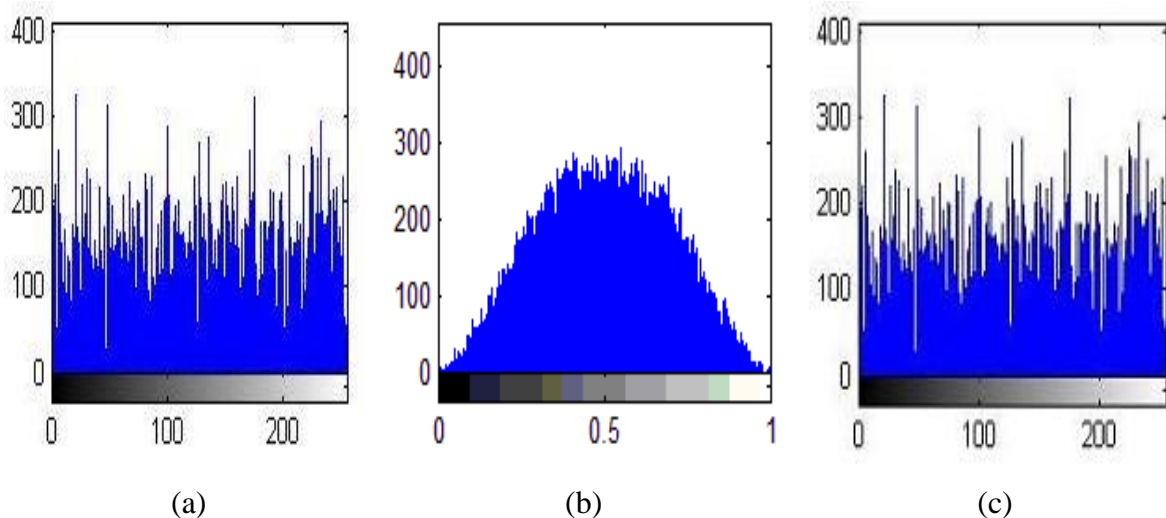
### 4.6.1 Histogram Analysis

To prevent the leakage of information to an opponent, it is beneficial if the cipher image bears little or no statistical similarity to the plain image. An image histogram illustrates how

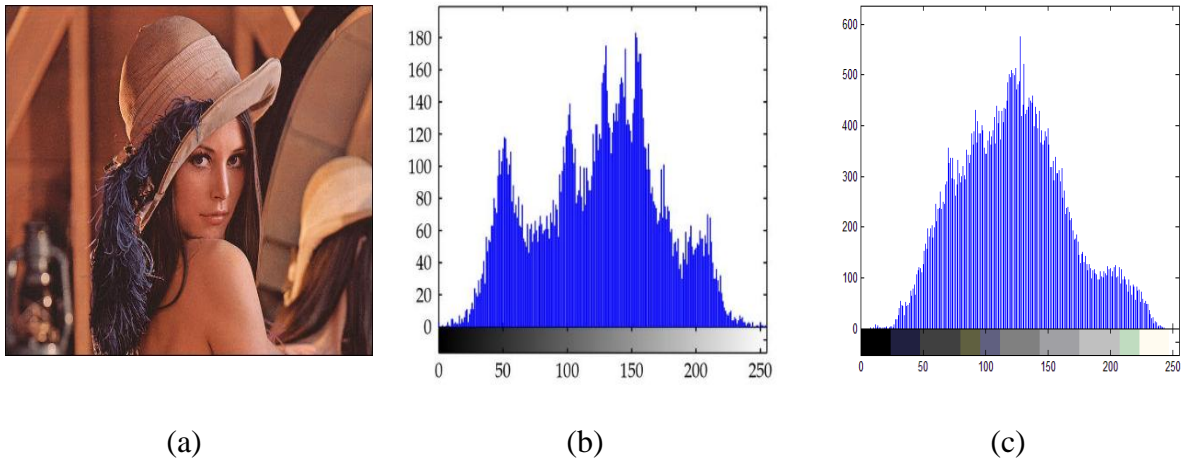
pixels in an image are distributed by graphing the number of pixels at each color intensity level. The histogram of the encrypted image is uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption.

Histogram of an image is used to plot the frequency distribution of its pixel values. Usually in an input image, the frequency distribution of pixel values remains imbalanced. But within the cipher image, because of the exploitation of encryption techniques, the distribution of pixel values exists uniformly. Thereby an adversary is unable to extract any useful information from the cipher image [17]. The proposed encryption technique also generates the cipher image with a uniform distribution of pixel values. For the input image of Fig. 4.1 (a), the histogram plot of both the original input image and the cipher image are presented in Fig. 4.10 (a) and Fig. 4.10 (b), respectively. Also presented of Fig. 4.1 (d) a benchmark Lena image in Fig. 4.11 that shows the histogram plot of the original input image and the cipher image in Fig. 4.11 (b) and Fig. 4.11 (c) respectively.

By comparing histogram plots i.e., by analyzing Fig. 4.10 and Fig. 4.11, it can be observed that there are significant differences between the original input image and the cipher image. It guarantees that the proposed encryption technique completely changes the characteristics of the input image. Finally, after decryption, the histogram of the retrieved image is shown in Fig. 4.10 (c). Here analyzing histogram plots it is also noticed that both the retrieved image and the original input image possess almost alike characteristics.



**Figure 4.10:** Histogram Plot for the Image of Fig. 4.1 (a): (a) Input Image, (b) Encrypted Image, and (c) Retrieved Image.



**Figure 4.11:** Histogram Plot for the Image of Fig. 4.1 (d): (a) Lena image, (b) Input Lena Image, and (c) Encrypted Lena Image.

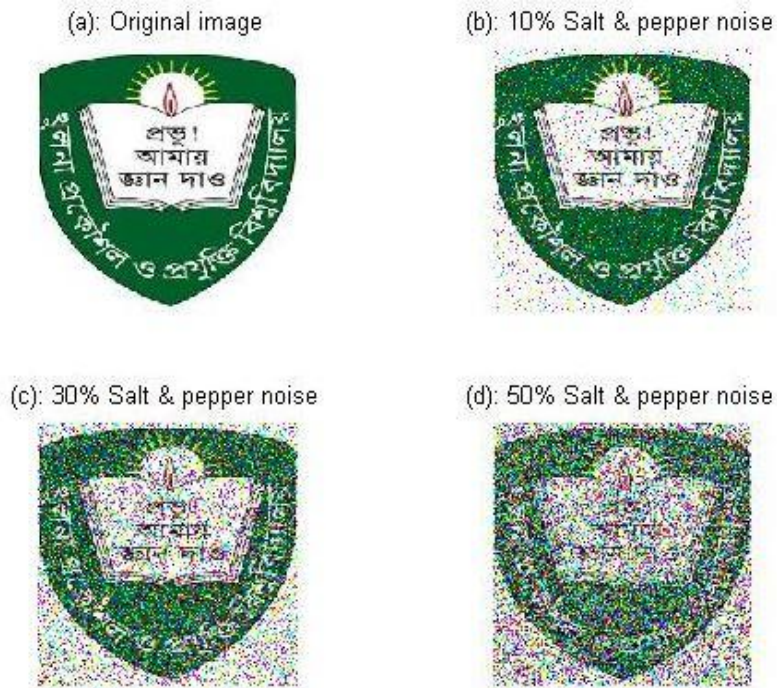
Two simple and very common attacks in the domain of internet are ‘Salt and Pepper noise attack’ and ‘chosen-plaintext attack’. For the image of Fig. 4.1 (a), Fig. 4.1 (d) and Fig. 4.1 (e) these attacks are simulated and described below.

#### 4.6.2 Salt & Pepper Noise Attack

Salt and pepper noise is an impetuous noise which sparsely occurs with white and black pixels of an image [17]. Corruption of image by salt and pepper noise happens because of defective memory locations in hardware, dyeing down of signal in communication links, wounding of channel decoder, transmission over noisy channels, multi path wireless communication [18, 19] etc. Generally, the damaged pixels set the value either minimum as 0 or maximum as 255 for salt and 0 ~ 8 for pepper noise [20].

To verify the strength of the proposed technique against this attack, the tempering of the cipher image is arranged with distinct levels of salt and pepper noise attacks namely, 10%, 30%, and 50% and their corresponding retrieved images are shown in Fig. 4.12 (b), Fig. 4.12 (c), and Fig. 4.12 (d), respectively for the image of Fig. 4.1 (a).

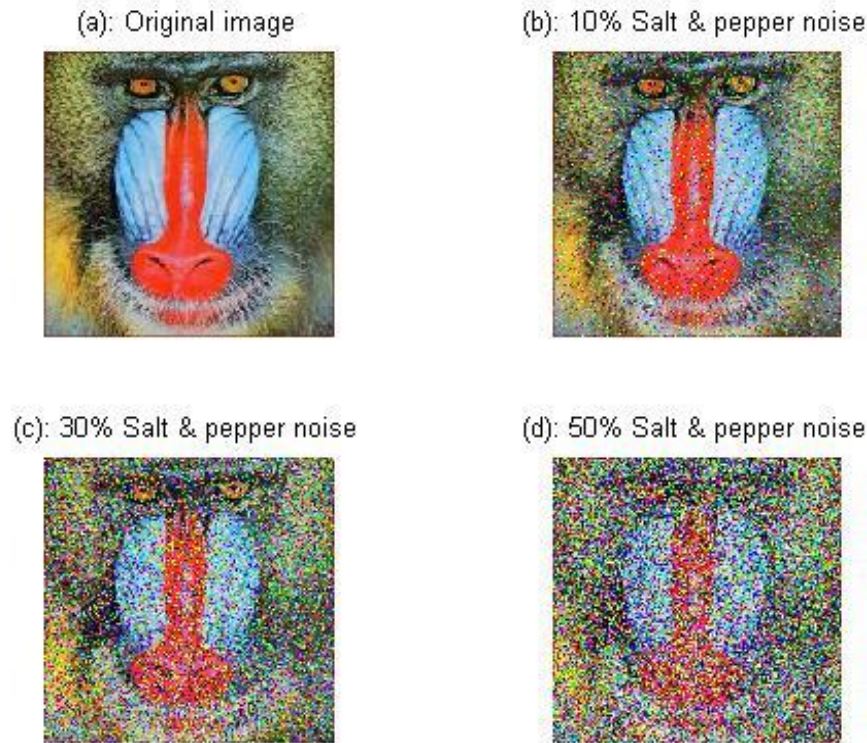
Also presented salt and pepper noise attacks with the level of 10%, 30%, and 50% of Fig. 4.1 (d) a benchmark Lena image that shown in Fig. 4.13 and the image of Fig. 4.1 (e) a baboon image that shown in Fig. 4.14.



**Figure 4.12:** (a) KUET Image. Salt and Pepper Noise Attacked KUET Image: (b) 10%, (c) 30% and (d) 50%.



**Figure 4.13:** (a) Lena Image. Salt and Pepper Noise Attacked Lena Image: (b) 10%, (c) 30% and (d) 50%.



**Figure 4.14:** (a) Baboon Image. Salt and Pepper Noise Attacked Baboon Image: (b) 10%, (c) 30% and (d) 50%.

From these figures, it is noticeable that while the tempering of cipher pixels increases, the amount of corrupted output also increases. However even after these tempering, the cipher images are perceptually identifiable. This ensures that the proposed technique is capable to survive in noisy channels and defective storages where salt and pepper noise attack with different noise density may exist.

#### 4.6.3 Chosen-Plaintext Attack (CPA)

In chosen-plaintext attack (CPA) the attacker somehow obtains the corresponding cipher image for a chosen input image of its' choice [16, 17]. In the proposed technique to generate the OTP key to be used for both encryption and decryption purpose, a random secret key is generated in binary, where the length of the key is equal to the number of LSBs within each chunk of each share. As secret random value is used to generate the key value, in fact, no two different images will use the same random value. Thereby apparently every image will employ a distinct key value. Although the intruder may have subsequent access to the targeted chipper



image, in no way the image as well as its key value is related to any other chipper image. Thus, the proposed encryption technique can survive the attack.

#### **4.7 Result Analysis and Discussion**

This thesis describes an multi stage secured technique that applied to several color images which shows its larger capacity for the secrecy of image than other techniques without loss of imperceptibility. From the analysis of the encrypted image we can observe that encryption technique has completely changed the characteristics of the original image. Still after decryption, decrypted image and the original image shows similar characteristics. Image characteristics are analyzed from various aspects such as histogram analysis, salt and pepper noise attacks. Apart from this operational speed or executional time of proposed technique also analyzed both for large or small images and real time environment, it is found that this technique performs far better than other existing techniques.

# CHAPTER V

## Conclusions

The chapter draws the summary of the thesis and also discussed some possible future works based on the outcome of the present work.

### 5.1 Summary of the Work

The proposed multi-stage encryption technique enhances the level of secrecy of image by combining VC, steganography and OTP consecutively. Thus, it accumulates advantages of cryptosystems not relying on specific key/keys with the strength of the cryptosystem relying on a specific key. According to the result of simulation although the time requirement of the proposed technique is alike or slightly higher than other related techniques, intuitively the level of its secrecy is certainly higher than those techniques. The underlying reason is that for encryption at first it adopts VC, then steganography and finally OTP technique where OTP technique cannot be cracked. While the encryption completes, the ultimate cipher image generated by the proposed technique is so confusing that it is quite impossible for any entity to guess the input image from the cipher image. The security and statistical analyses also ensure that it is almost impossible for the intruder or attacker to mount any form of attack on it. Thus, the proposed technique possesses good imperceptibility and high-level security.

### 5.2 Future Perspectives

A few potential future directions of works are available from the present study. In this study, only static images are considered. In future it might be implemented on the live system in the real time application server. Another future of improvement is to incorporate an appropriate image compression technique to decrease the size of ciphertext with the proposed image encryption technique. Expected that through compression, the capacity of the image will be reduced which will lead to decrease the time requirement of encryption and decryption processes of the proposed technique.

## REFERENCES

- [1] M. Naor and A. Shamir, "Visual cryptography", in Proc. of Advances in Cryptology–EUROCRYPT'94, pp. 1–12, Springer Berlin/Heidelberg, 1995.
- [2] G. Huayong, M. Huang and Q. Wang, "Steganography and Steganalysis Based on Digital Image", International Congress on Image and Signal Processing, Vol. 1, pp. 252–255, IEEE, 2011.
- [3] M. Paunwala and S. Patnaik, "Biometric template protection with DCT based watermarking", Machine Vision and Applications, Vol. 25, No. 1, pp. 263–275, 2014.
- [4] D. Aeloor and A. Manjrekar, "Securing Biometric Data with Visual Cryptography and Steganography", International Symposium on Security in Computing and Communication, pp. 330–340, Springer Berlin, 2013.
- [5] P. Marwaha and P. Marwaha, "Visual Cryptographic Steganography in Images", International Conf. on Computing, Communication and Networking Technologies, pp. 1 - 6, IEEE 2010.
- [6] M. Pramanik and K. Sharma, "Analysis of Visual Cryptography, Steganography Schemes and its Hybrid Approach for Security of Images", International Journal of Emerging Technology and Advanced Engineering(IJETAE), ISSN 2250-2459, ISO 9001:2008, Vo. 4, No. 2, February 2014.
- [7] V.L. Reddy, A. Subramanyam and P.C. Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats", International Journal of Advanced Networking and Applications Vol. 02, No. 05, pp. 868-872, 2011.
- [8] S. Patil and A. Kumar, "Modified One Time Pad Data Security Scheme: Random Key Generation Approach", International Journal of Computer and Security Vol. 3, No. 2, 2009.
- [9] E. Walia and P.J. Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, Vol. 10, No. 1, pp. 4–8, April 2010.
- [10] J. Jesalkumari and R.R. Sedamkar, "Modified Visual Cryptography Scheme for Colored Secret Image Sharing", International Journal of Computer Applications Technology and Research, Vol 2, No. 3, pp 350 – 356, 2013.
- [11] F. Liu and CK. Wu, "Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners", IET Information Security, Vol. 5, No. 2, pp. 121–128, 2011.
- [12] M.T.I. Siyam, K.M. Rokibul Alam and T. Al Jami, "An Exploitation of Visual Cryptography to Ensure Enhanced Security in Several Applications", IJCA ISSN: 0975 – 8887, Vol. 65, No.6, March 2013.
- [13] P.V. Parmar, S.B. Padhar, S.N. Patel, N.I. Bhatt and R.H. Jhaveri, "Survey of Various Homomorphic Encryption algorithms and Schemes", International Journal of Computer Applications, Vol. 91, No. 8, 2014.
- [14] "MATLAB 9.3" Retrieved on October 15, 2017, from [https://www.mathworks.com/academia/student\\_version.html](https://www.mathworks.com/academia/student_version.html).

- [15] A. Simmonds, P. Sandilands and L. van Ekert, “An Ontology for Network Security Attacks”, Lectures Notes in Computer Science, Vol. 3258, pp. 317-323, 2004.
- [16] B. Surekha, and D.G.N. Swamy, “A Spatial Domain Public Image Watermarking”, International Journal of Security and Its Applications Vol. 5, No. 1, January 2011.
- [17] S. K. Ghosal, “A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique”, International Conference on Scientific Paradigm Shift in Information Technology & Management (SPSITM 2011) in collaboration with IEEE, Kolkata, pp. 123-129, January 2011.
- [18] X. Li, T. Zeng and B. Yang, “Detecting LSB matching by applying calibration technique for difference image”, in Proc. 10th ACM Workshop on Multimedia and Security, Oxford, U.K, pp. 133–138, 2008.
- [19] H.W. Tseng and H.S. Leng, “A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number”, Hindawi Publishing Corporation, Journal of Applied Mathematics, Vol. 2013, No. 13, pp. 1-8, 2013.
- [20] M. Wherate, S. Sherekar and V.M. Thakre, “Two Layer Security Using Visual Cryptography and Steganography”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 5, No. 4, pp. 92-95, April 2015.
- [21] P. Bharti and R. Soni, “A New Approach of Data Hiding in Images using Cryptography and Steganography”, International Journal of Computer Applications, Vol. 58, No. 18, pp. 1-5, 2012.
- [22] Y. Chen and j. Chen, “A Novel Blind Watermarking Scheme Based on Neural Networks for Image”, IEEE Transactions, pp. 548-552, 2010.
- [23] H. Xu and C. Shujuan, “An Adaptive Image Watermarking Algorithm based on Neural Network”, IEEE Computer Society, 4th International Conference on Intelligent Computation Technology and automation, pp. 408-411, 2011.
- [24] Y.H.C. Wu and C.C. Chang, “A novel digital image watermarking scheme based on the vector quantization technique”, Computers & Security, vol. 24, pp. 460–471, 2005.
- [25] Y. Wang and A. Pearmain, “Blind image data hiding based on self-reference”, Pattern Recognition Letters, vol. 25, no. 15, pp.1681–1689, 2004.
- [26] H. Mathkour, G. Assassa, A. Muharib and I. Kiady, “A Novel Approach for Hiding Messages in Images”, International Conference on Signal Acquisition and Processing, pp. 89 – 93, 2009.
- [27] A. Bamatraf, R. Ibrahim, M. Najib and B. M. Salleh, “Digital watermarking algorithm using LSB”, International Conference on Computer Applications and Industrial Electronics, PP. 155 – 159, December 2010.
- [28] V. Rijmen, and B. Preneel, “Efficient Color Visual Encryption for Shared Colors of Benetton”, Euro crypto, Rump Session, Berlin, 1996.
- [29] E. R. Verheul and H.C.A. Tilborg, “Constructions and properties of k out of n visual secret sharing schemes”, Designs, Codes and Cryptography, 11(2): pp. 179-196, 1997.
- [30] S.M.M. Karim, M.S. Rahman and M.I. Hossain, “A New Approach for LSB Based Image Steganography using Secret Key”, Proceedings of 14<sup>th</sup> International Conference on Computer and Information Technology, IEEE Conference Publications, pp. 286 – 291, 2011.

- [31] A.A. Shejul and U.L. Kulkarni, “A Secure Skin Tone based Steganography (SSTS) using Wavelet Transform”, *International Journal of Computer Theory and Engineering*, Vol.3, No.1, pp. 16- 22, 2011.
- [32] J. Kiernan and R. Agrawal, “Watermarking Relational Databases”, *Proc. 28th International Conference on Very Large Databases VLDB*, 2002.
- [33] Y. Li, V. Swarup and S. Jajodia, “A Robust Watermarking Scheme for Relational Data”, *Proc.13th Workshop Information Technology and Systems (WITS)*, pp. 195-200, December 2003.
- [34] Y.K. Meghrajani and H.S. Mazumdar, “Hiding secret message using visual cryptography in steganography”, in *Proc. 12th IEEE India International Conference Electron., Energy, Environ., Commun., Comput., Control*, New Delhi, India, pp. 1–5, Dec. 2015.
- [35] M. Aziz, M. H. Tayarani and M. Afsar, “A cycling chaos-based crypticfree algorithm for image steganography”, *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1271–1290, Springer, 2015.
- [36] E. Avci, T. Tuncer and D. Avci, “A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain”, *Arabian Journal for Science and Engineering*, Springer, 2016.
- [37] M. Nakajima and Y. Yamaguchi, “Extended Visual Cryptography for Natural Images”, in *Proceedings of WSCG*, pp. 303-310, 2002.
- [38] P. Saha, S. Gurung and K.K. Ghose, “Hybridization of DCT based steganography and random grids”, *International Journal of Networking and Security Application (IJNSA)* 5(4), 2013.
- [39] K. Samseriya, S. Bahadure, S. Doble and K Purohit, “Secrete Sharing by Visual Cryptography: A Review”, *International Journal for Research in Applied Sci. & Engineering Technology (IJRASET)*, ISSN: 2321-9653, Vol. 5, Issue X, October 2017.
- [40] S.I. Rosaline and M.A. Raj, “Adaptive Pixel Pair Matching based Steganography for Audio files”, *IEEE Explore*, ISBN: 978-1-4673-5301-44, Jan 2013.
- [41] Sample images (accessed on October 05, 2017) from <http://sipi.usc.edu/database>.
- [42] D.S. Laiphrakpam and M.S. Khumanthem, “Cryptanalysis of symmetric key image encryption using chaotic Rossler system”, *Elsevier, Optik*, Vol. 135, pp. 200-209, 2017.
- [43] D.S. Laiphrakpam and M.S. Khumanthem, “A robust image encryption scheme based on chaotic system and elliptic curve over finite field”, *Springer, Multimedia Tools and Applications*, pp. 1–24, May 2017.
- [44] S.S. Al-amri, N.V. Kalyankar and S.D. Khamitkar, “A Comparative Study of Removal Noise from Remote Sensing Image”, *International Journal of Computer Science*, Vol. 7, Issues 1, pp. 33-36, 2010.
- [45] G. Judith and N. Kumarasabapathy, “Study And Analysis of Impulse Noise Reduction Filters”, *An International Journal of Signal and Image Processing (SIPIJ)*, Vol. 2, No.1, March 2011.

- [46] S.Rohith and K.H. Bhat, "A simple robust digital image watermarking against salt and pepper noise using repetition codes", *International Journal on Signal and Image Processing*, Vol. 3, No. 1, 2012.
- [47] X. Wang, S.A. Okamoto, N.L. Ishigo and R.R. Lear, "Multi-stage watermarking process and system", U.S. Patent 7,184,571, February 2007.
- [48] F. Liu, J. Tang, Y. Song, Y. Bi, and S. Yang, "Local structure based multi-phase collaborative representation for face recognition with single sample per person", *Information Sciences*, Vol. 346, pp.198-215, June 2016.
- [49] F. Hu, C. Pu, H. Gao, M. Tang, and L. Li, "An image compression and encryption scheme based on deep learning", *arXiv preprint arXiv: 1608.05001*, 2016.
- [50] F. Hu, J. Wang, X. Xu, C. Pu and T. Peng, "Batch Image Encryption Using Generated Deep Features Based on Stacked Autoencoder Network", *Mathematical Problems in Engineering*, Vol. 2017, ID 3675459, pp. 1-12, 2017.
- [51] Z. Li, and J. Tang, "Weakly supervised deep metric learning for community-contributed image retrieval", *IEEE Trans. on Multimedia*, Vol. 17, No. 11, pp. 1989-1999, 2015.
- [52] Z. Li, and J. Tang, "Weakly supervised deep matrix factorization for social image understanding", *IEEE Trans. on Image Processing*, Vol. 26, No. 1, pp. 276-288, 2017.

## **Publication in Progress**

### **Journal**

Arindom Mondal, Kazi Md. Rokibul Alam, G. G. Md. Nawaz Ali, Peter Chong and Yasuhiko Morimoto, “A Multi-Stage Encryption Technique to Enhance the Secrecy of Image” 1st revised version submitted to KSII Transactions on Internet and Information Systems (TIIS), 2018.