Color Image Encryption using Advanced Visual Cryptography

A thesis submitted towards the fulfillment of requirement for the award of the degree of

Master of Engineering

In

Electronics and Communication Engineering

Submitted by:

MANPREET SINGH

Roll No: 801361015

Under the Guidance of:

Dr. AJAY KAKKAR

Assistant Professor

ELECTRONICS AND COMMUNICATION ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

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

PATIALA – 147004 (PUNJAB)

JUNE 2015

CERTIFICATE

Certified that the thesis entitled ***"Color Image Encryption using Advanced Visual Cryptography"*** being submitted by **Mr. Manpreet Singh** to the **Department of Electronics and Communication Engineering, Thapar University, Patiala** in the fulfillment of the requirements for the award of the degree of **"Master of Engineering"** is a record of bona fide research work carried out by him. He has worked under my guidance and supervision and fulfilled the requirements for the submission of this thesis which has reached the requisite standard. The matter presented in this thesis does not incorporate any material previously published or written by any other person except where due reference is made in the text.

The results contained in this thesis have not been submitted in part or full to any other institute or university for the award of degree or diploma.

Dr. Ajay Kakkar
Assistant Professor,
Department of ECE,
Thapar University,
Patiala (P.B) – 147004
India

DECLARATION

I hereby declare that the thesis report entitled **"Color Image Encryption using Advanced Visual Cryptography"** is an authentic record of my study carried out as requirement for the award of degree of ME (Electronics and Communication Engineering) at Thapar University, Patiala, under the supervision of **Dr. Ajay Kakkar**, "Electronics and Communication Engineering Department" during master's degree.

The matter presented in the thesis has not been submitted to any other institute or university for the award of degree or diploma.

Date: 07/07/2015

Manpreet Singh
Roll No. 801361015

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

Date: 07/07/15

Dr. Ajay Kakkar
Assistant Professor, ECED

Countersigned by:

Dr. Sanjay Sharma
Professor and Head, ECED
Thapar University, Patiala
Date:

Dr. S. S. Bhatia
Dean of Academic Affairs
Thapar University, Patiala
Date:

ACKNOWLEDGEMENT

I know nothing about wisdom, meditation and good deeds; I know nothing about Your excellence. Guru Nanak is the greatest of all; He saved my honor in this Dark Age of Kali Yuga. All the victory and success belongs to the Supreme God.

Knowledge is like electric wave which pervades everywhere but it shines like a spark only at Teacher. I would like to thank Dr. Ajay Kakkar, Assistant professor, Electronics and Communication Engineering Department, under the guidance of whom, this course of thesis has been completed successfully. It was lucky to work under his supervision and guidance. He has vast knowledge about the current trends in the field of education and is a morally supporting personality. One can learn a lot from him.

Dr. Sanjay Sharma, Head of Department, Electronics and Communication Engineering and P.G Coordinator Dr. Amit Kumar Kohli, are both the personalities one can inspire from. They help student in every possible way through thick and thins so that he can continue pursuing journey towards success. I am thankful to them for their support throughout this course.

Also, I am thankful to my research fellows and classmates for their discussions in order to clear the concepts in this study.

Parents are above all, they brought you here and show the beautiful creation of God which we call mother nature, our Earth. Support of family is by par the most influencing factor for achievements. I am proud to be the son of Ideal parents, who sacrificed their joys to raise me up, chase my dreams, and fulfill their hopes. I bow down my head to my parents for their love and affection towards me, for always prioritizing me above everything else in their lives.

I am presenting before you the result of endless nights without sleep, strenuous hard work, determined and gritty solutions of me fighting with myself and I acknowledge that this has been possible only because of Supreme God – '*Waheguru*'

"There is no such phenomena as random,
It's us who are incapable to understand"

Manpreet Singh

TABLE OF CONTENTS

ABSTRACT

Secured and timely transmission of images or graphical data is always an important aspect for an organization. In the encryption process the failure to decode images properly and processing time are directly related with the security of cryptographic model in a network. The use of strong encryption algorithms almost makes it impossible for a hacker to get access to the hidden data inside the image which is being encrypted. Cryptography is an essential component of an organization in order to keep the information safe from various competitors. It helps to ensure the privacy of a user from others. Secured and timely transmission of images are always an important aspect for an organization. In present scenario most of the information is being collected, processed and stored by the computers and further transmitted across the networks, therefore, there is a need to protect the graphical data in order to keep the data confidential. Keeping in view the importance of visual data for secure data transmission this work incorporates the use of image encryption. Current aspects of cryptography as well as the related terms including the visual cryptography approach are discussed in the beginning of this thesis. Literature review for data encryption and visual cryptography has also been discussed. Observations have been presented and problem is formulated. Then a modified image encryption scheme has been presented that meets the objectives such as no pixel expansion and zero contrast loss. After presenting the proposed scheme, its results and comparison with other schemes has been discussed. Finally, the thesis has been concluded and the possible future scope of the proposed scheme has been mentioned.

LIST OF ABBREVIATIONS

DES	Data Encryption Standard
IBM	International Business Machines
TDES	Triple Data Encryption Standard
IDEA	International Data Encryption Algorithm
RSA	Ron Rivest, Adi Shamir and Len Adelman
DSA	Digital Signature Algorithm
MIT	Massachusetts Institute of Technology
PGP	Pretty Good Privacy
PKI	Public Key Infra Structure
AES	Advance Encryption Standard
ISO	International Organization for Standardization
ANSI	American National Standards Institutes
IEEE	Institute of Electrical and Electronics Engineers
MSIS	Multiple Secret Image Sharing
VC	Visual Cryptography
VCRG	Visual Cryptograms of Random Grids
RVCS	Reversing based Visual Cryptography Scheme
GRVCS	Grayscale Reversing based Visual Cryptography Scheme
MVC	Multi-Secret Visual Cryptography
TVC	Tagged Visual Cryptography
P-LTVC	Probabilistic Lossless Tagged Visual Cryptography
VSS	Visual Secret Sharing
DNA	De-oxy Ribose Nucleic Acid
SI	Secret Image
HVC	Halftone Visual Cryptography
RGB	Red-Green-Blue

LIST OF FIGURES

LIST OF TABLES

LIST OF PUBLICATIONS

1. M. Singh, A. Kakkar, “Binary plane approach in visual cryptography,” *Proceedings of National conference on Role of Information and Technology in Management and Engineering*, vol. 1, no. 1, pp. 62-65, Mar. 2015.
2. M. Singh, A. Kakkar, “Image encryption scheme based on Knight’s Tour Problem,” *4th International Conference on Eco-friendly Computing and Communication Systems*, Sponsored by Elsevier, Jun. 2015. (communicated)

CHAPTER 1

INTRODUCTION

This chapter covers the core concept, related terms and the uses of Cryptography. It plays an important role in secure data transmission. Cryptography has been evolved from the term data security. It can be extended from textual data to images and videos, so the word visual cryptography came into existance.

1.1 FOUNDATIONS OF CRYPTOGRAPHY

With the development in the field of information and technology over the period of time, new possibilities for communication among us are enlarged. E-Commerce being fast and more reliable method of providing services, emerged as one of the most powerful way of interaction between end users like us and government agencies, banking fields and other organisations [1]. The platform is managed electronically without the need of sending any paper transactions. Other most remarkable breakthroughs include internet and digital mobile networks like GSM and CDMA. All of these services are used by billion of people throughout the globe [1].

These technologies are successful because of the congenital advantages of the digital systems [3]. More insensitivity towards noise than the analog counterpart allows the data transfer over longer distances with lesser probability of data corruption. Quality and data integrity is maintained, which means there would be lesser number of errors in digital systems. Apart from these advantages which digital systems offer, there are plenty of vulnerabilities alongside [2]. The unsecured channels can be easily hacked and unauthorised data modification can occur. This can lead to compromise of user's privacy and security. Digital systems are very complex and are hard to debug. Packet capturing can result in data hacking.

For a traditional e-mail experience, one can check if the contents of mail are already read out by the intruder or there occurred any temperament in the contents of the mail by looking at the read flag on the mail. These are tests that assume the extension that manipulation of the message may have left some traces behind. These are not far better approaches to ensure

data integrity, hence there exists a need to develop a system that can protect itself from the stage of transferring data through storing data [2].

Cryptography or Cryptology: It is the science behind the whole process of secure data transfer with protected or no access to un-authorised destinations [4].

Cryptanalysis: It is the process that focus its aim to defeat the principle of cryptography. It studies the possiblities of breaking encryption without knowing credentials [4]. An overview about this can be found in David Kahn [5]. Noteworthy point here is that the security issues and problems related to verification of data are not new. These are present since the day humanity begin to understand. However, current scenario involving large information technology structure made it necessary to put faith in cryptography and made it a necessary perspective for information interchange.

Rapidly increasing internet connectivity as more and more devices are getting connected globally also grow the number of potential sources of attack [4]. Trespassing personal limits of someone or eavesdropping critical data transfer over networks increased since the past few years [5]. This uncontrolled growth of communication systems and networks made it much more difficult to maintain the security, integrity and quality of information being transferred every second. Result of this being creation of viruses, worms, malware etc [5]. All this in return put forward the need of secure and reliable network which can be met to extent only through cryptography or cryptology.

1.2 GOALS OF CRYPTOGRAPHY

Among many of the benefits gained by the use of cryptography in the field of data transmission over different channels, below is the list of most important ones, which are essentials.

1. **Confidentiality:** It is the service offered that provides the data secrecy. Genuine access is maintained and any un-authorised data access is forbidden. Term is similar to privacy in common context [6].
2. **Authentication:** This is the process described as Identification. Parties indulged in the process of communication needs to verify there identities prior to exchange of information [5].

3. **Integrity:** All the data transferred among the users must maintain the integrity. In other words, any kind of action performed on data like addition, deletion or kind of manipulation must be visible to each user. This limits the fake insertions by intruders [4].
4. **Non-repudiation:** For a dispute scenario when a party disagree about the data it tranfered, there must be a system or service that can resolve this issue. Thus the denying of action must be checked and valid action must be taken against committer [6].

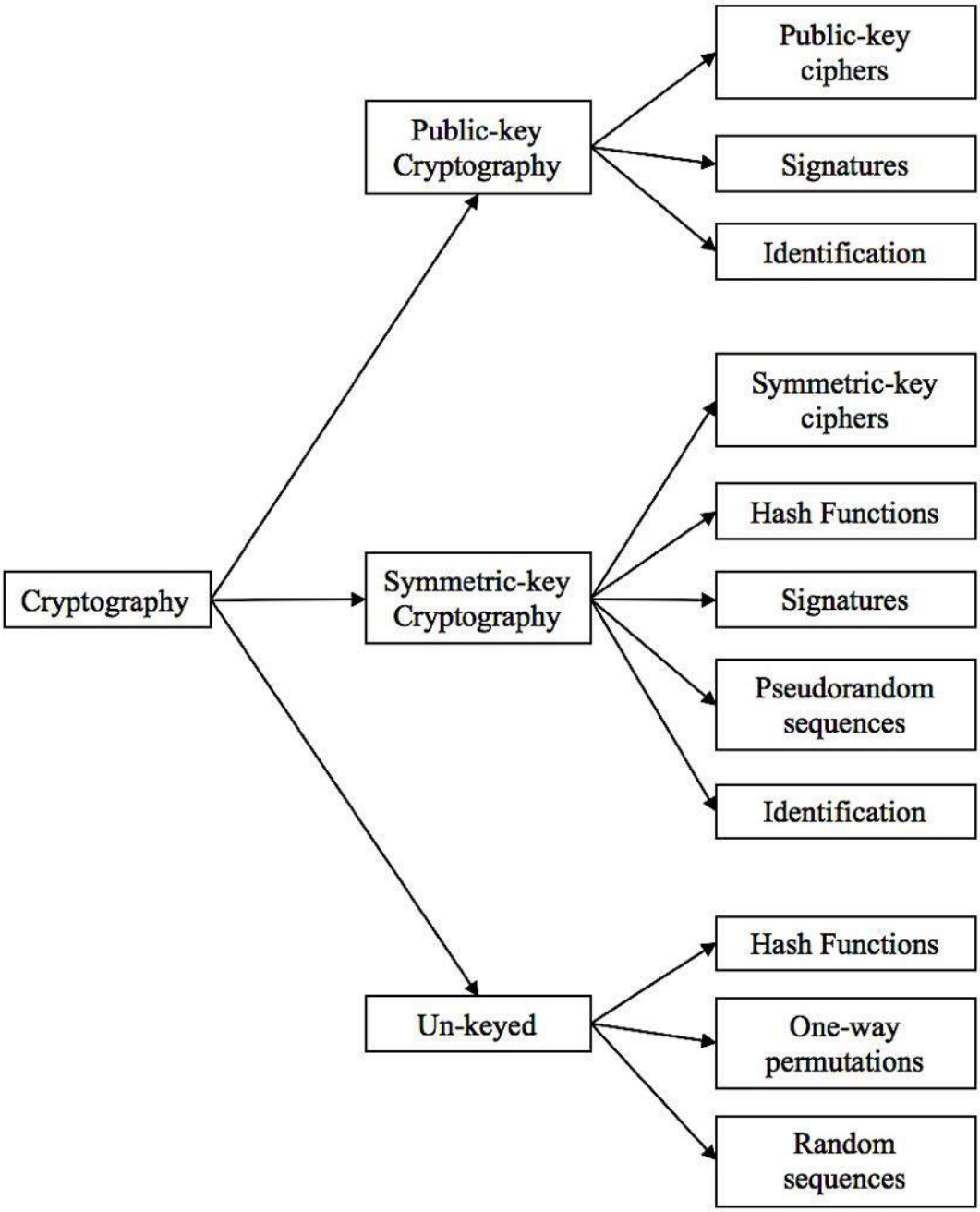


Figure 1.1: Classification and branching of Cryptography.

1.3 LEXICON

The concept of cryptography is built on rigorous definitions that are evolved from fundamental concepts.

- **Alphabet of definition**, denoted by A, it is the space consisting of all possible messages like a dictionary, no message can be outside this set [6].
- **Message space**, denoted by M, consists of the messages that are required to be sent. It is a subset of alphabet of definition [4].
- **Plaintext,** denoted by P, it is an element of message space M in the pure form i.e., plaintext is completely understandable and is the actual information to be sent [6].
- **Ciphertext,** denoted by C, may or may not be a member of same alphabet of definition for message space M and is the string obtained after plaintext is encrypted. It belongs to it's own ciphertext space [6].
- **Key,** denoted by K, comprises of a string which is significant for the conversion process of a plaintext to ciphertext and vice-versa [5].
- **Encryption,** denoted by E, is the process of converting plaintext into ciphertext such that it no longer stays recongnizable and true information is hidden beneath [4].
- **Decryption,** denoted by D, is the inverse process of encryption, where ciphertext is processed to reveal the plaintext or actual data [4].

Figure 1.2 shown below, represents a simple encryption process comprising of key components required to achieve cryptographic data security.

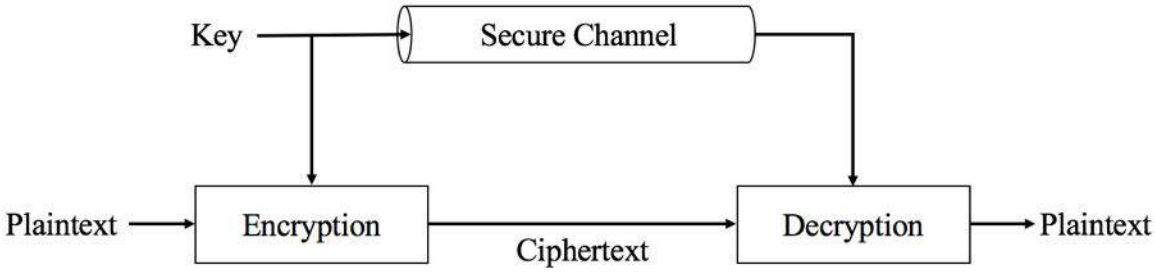


Figure 1.2: Elementary Cryptographic Model

The most important point to take into consideration is that the key is sent through a secure channel. As without key, it is extremelly dificult or ideally impossible to obtain plaintext or true information from ciphertext. Another aspect of cryptography is that it always acknowledge the fact that ciphertext will be the subject of cryptanalysis and hence encryption technique must be more strong [5].

Example 1.1: Consider Alice and Bob wants to communicate with message space $M = \{m_1, m_2, m_3\}$ being message space and ciphertext space $C = \{c_1, c_2, c_3\}$ as ciphertext space. Since 3 messages can have $3! = 6$ permutations possible which becomes key space being $K = \{1, 2, 3, 4, 5, 6\}$, hence it could be possible to denote each encryption function or transform as $E_1, E_2 \ \ldots \ E_6$ [7].

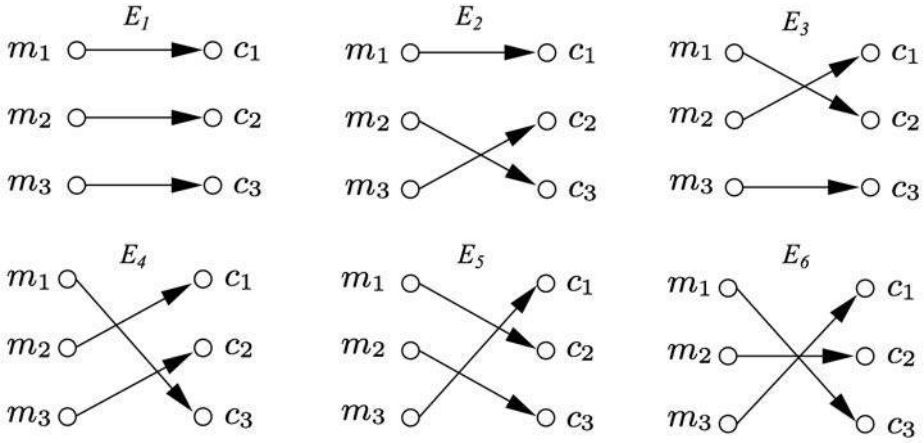


Figure 1.3: Simple encryption scheme

From figure 1.3, say Alice used E_5 as encryption function or transform, then the message space M's element will be mapped as $\{m_1 \rightarrow c_2,\ m_2 \rightarrow c_3,\ m_3 \rightarrow c_1\}$. To retreive the original message Bob has to just reverse the arrows of encryption scheme E_5 . Hence, this formed a very basic encryption model that clarifies the basic concept of cryptography [7].

1.4 KERCKHOFF'S PRINCIPLE

According to Kerckhoff [9], cryptographic system must built on the assumption that the system's working can be compromised. In other words, the principle of working for the system can be known to the adversary, hence the system should not require secrecy. Thus this principle states that system should be still secure even if intruder has its copy of the system. The key must be kept secure, while not worrying about the system. This was reformulated by Shannon under the name of Shannon's maxim [8]. The main highlights of Kerckhoff's principle are as follows:

- If not mathematically, the system should be atleast unbreakable in practice even if adversary acquired its knowledge.
- Key generation and modification at will should not be a problem and system should be compatibility with other services like telegraph etc.
- System must be portable, easy to handle and learn to use.

1.5 STANDARDS

There a large number of cryptographic techniques out there. Mainly these are classified as Public key and Private key cryptography. Few noteworthy algorithms that actually became standard are shown in figure 1.4.

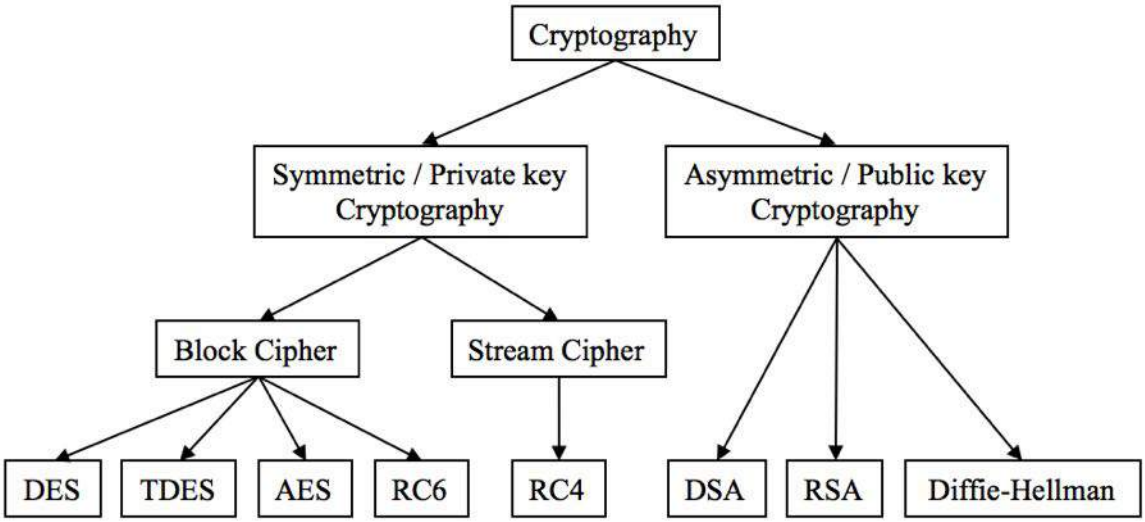


Figure 1.4: Taxonomy of cryptographic standards

- **Symmetric or Private Key Cryptography:** It is an encryption scheme which comprises the feature by which the encryption key, denoted by e and decryption key, denoted by d can be retrived from one another with least computational complexity. In common context, if both the encryption key and decryption key pair, commonly denoted by (e, d) are both equal i.e., $e = d$, such an alogrithm is called Symmetric. It also makes the use of same private key for complete implemenation [4].

- **Asymmetric or Public Key Cryptography:** If the computational complexity of obtaining the decryption key d from encyption key e is very large ideally infinite, the technique used is called Asymmetric. Also noteworthy to mention here that both the keys are different. Generally encryption is done using public key while deciphering requires private key. Here $e \neq d$ rule is obeyed [5].

- **Block Cipher:** An encryption technique in which the message or plaintext is first divided into fixed length strings (length t) and then strings are encrypted one block at a time [4].

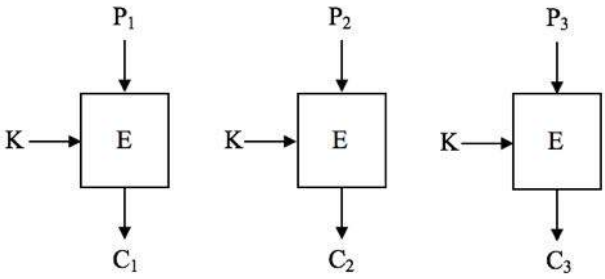


Figure 1.5: Block cipher in ECB (Electronic Code Book) Mode

Electronic Codebook Mode (ECB) is easiest way to encipher plaintext when the length of the message exceeds the desired block length. At first, the plaintext is distributed into n-bit blocks, then these are independently encrypted. This can be seen in figure 1.5 above.

Encryption: $C_i = E_K(P_i)$ Decryption: $P_i = D_K(C_i)$

There are other modes as well like Cipher Block Chaining mode (CBC), and Offset Codebook mode (OCB) mode etc.

- **Stream Cipher,** is the primitive form of block cipher with block length $t = 1$, thus individual symbols are encrypted one at a time. This elimimnates the error propagation problem commonly seen in block ciphers [4].

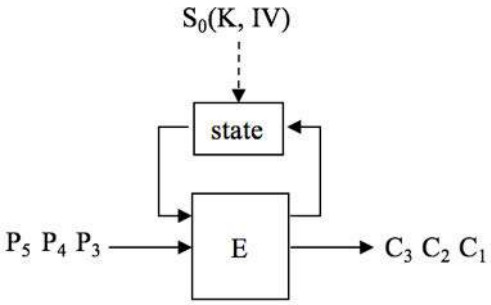


Figure 1.6: A Stream Cipher Mode

In stream cipher, plaintext or message symbols are processed one bit at a time and are encrypted. This process is iterated till the whole message is encrypted in accordance to the internal state and is controlled using key K and public Initalization Value (IV). In figure 1.6, P_i represents the plaintext while C_i represents ciphertext [5].

1.6 HASH FUNCTIONS

Hash functions are also known as message digests or one-way encryption [16]. These are the schemes which does not require any key for its use. In return a fixed length value known as hash is generated depending upon the message contents. This hash is the digital fingerprint for the message and plays important role in ensuring integrity of the message.

The problem associated with public key system for data verification is that the dimensions of resultant message becomes around two times of the original. This issue can be addressed using hash. Most important aspect of this approach is that even a single bit data change can result in completely different hash value and thus forgery can be detected.

1.7 HYBRID CRYPTOGRAPHY

One can understand from the name that hybrid cryptography involves the use of two or more cryptographic techniques [17]. One technique may provide better security in one aspect while other can provide in different scenario. Merging the two separate techniques to obtain a new scheme that can allow far better handling and security is always desired. A Public-key system cannot provide aggregation among the intermediate nodes as there is no knowledge of the private key at the end node. So, to achieve better security, symmetric and asymmetric systems are used in congestion.

Therefore, key is transmitted by asymmetric method while the data by symmetric, by this asymmetric method allows verifying the identity of the receiver while actual data is encypted using private key. Nowadays, key is generated with the help of public key cryptosystem while it is used as the key in AES algorithm to obtain confidentiality of the data being transmitted.

1.8 VISUAL CRYPTOGRAPHY

Visual Cryptography is an effective and efficient way of sharing secrets among the trustworthy parties. The biggest problems with which most of the cryptographic algorithms have to deal with is trust. Visual cryptography basics lie in the power of distributing a single secret into multiple shares or so called transparencies which when stacked together makes it possible to see the original secret otherwise nothing is revealed [19].

1.8.1 Secret Sharing

Secret means anything which is forbidden to be known or seen. Secret sharing is the method of distributing a secret in a manner that each participant gets a piece of secret, yet cannot recognise the true knowledge hidden beneath it. Any share itself does not explain anything to the viewer until or unless all of the shares are clubbed together. Stacking these shares reveals the actual image or secret [17].

In a secret sharing technique, each of the hidden piece of secret is disintegrated into number of smaller parts called as shares and is distributed to n number of persons. Now if any specified k number of persons put their shares together, actual secret information is uncovered. If less than k shares are laid upon, nothing is revealed. This is the typical example of (k, n) -threshold scheme for secret sharing as defined by Shamir [18]. According to Shamir, if one consider as the desired secret and this is required to be allocated or shared with n number of parties, a scheme called as (k, n)-threshold divides the D among n parts $D_1, D_2, \dots, D_n$ if following conditions are satisfied:

1. Knowing k or more parts of D_i may minimise the computation complexity of D,
2. Knowing $k - 1$ or lesser number of D_i parts are incapable of computing D.

Thus, visual cryptography is a scheme that puts effort in solving the secret sharing problem. This deals with hiding secrets inside of images. Then those images are encoded without requiring any computation. Decoding requires stacking of transparencies only [19].

Visual cryptography is worth value as it incorporate within it the perfect secrecy by making use of one time pad and is far easier to encrypt and decrypt the secret. This scheme is perfectly secure. This is closely related to one time pad. This makes visual cryptography above the known cryptographic schemes which are secure conditionally [17].

Lagrange's Interpolation forms the base for secret sharing scheme by Shamir [18]. According to it, for a given set of points $(x_i, y_i)\ \forall\ i = 0, 1, \dots, k - 1$, the polynomial for Lagrange interpolation can be structured using:

$$P(x) = \sum_{i=0}^{k-1} y_i \prod_{i \neq j} \frac{x - x_i}{x_j - x_i} \tag{1.1}$$

For a given secret, the sharing can be done on the basis of interpolation scheme. Let's denote Galois Field $(q > n)$ by $GF(q)$, then by choosing proper coefficients i.e., $\alpha_0, \alpha_1, \alpha_2 \dots \alpha_{k-1}$ among the $GF(q)$, following polynoimial can be constructed:

$$f(x) = s^* + \sum_{i=0}^{k-1} \alpha_i x^i \tag{1.2}$$

where $s*$ denotes the secret key. The coffients belong to the range $[0, q)$ according to [18]. Let's say $s_i = f(\alpha_i), i = 0, 1, 2, \dots, n$ are nothing but the shares and can be distributed among different persons.

For reconstruction of the original secret image, say k participants provide their individual shares $s_i, i = 0, 1, 2, \ldots, k$ to the Lagrange's interpolation polynomial to recreate the original secret.

$$P(x) = \sum_{i=1}^{k} s_i \prod_{i \neq j} \frac{\alpha - \alpha_i}{\alpha_j - \alpha_i} \tag{1.3}$$

where algebraic operations are performed over Galois Field GF(q):

$$P(\alpha_i) = s_i, \quad i = 1, 2, \ldots, k, \quad s^* = P(0) \tag{1.4}$$

Therefore, actual secret $s*$ can be obtained [18]

1.8.2 Foundations of Visual Cryptography

Image sharing is an approach dealing with images instead of secret sharing. The secrets here are in the form of hidden images. Every secret is given a number and are provisioned with specific coding method for each source of secret. In (k, n) secret image sharing scheme, the required image is splitted among n parts or so called shares, similar to the secret sharing mentioned previously, k parts are required to reveal the concealed image otherwise nothing is revealed [18].

The concept of visual cryptography was braught forward originally by Moni Naor and Adi Shamir [19]. Visual cryptography makes use of human visual system by the sense that stacking of k transparencies together, human eyes can readily able do the decryption process. This makes it possible to understand the system without any requirement or knowledge of cryptography and this fact make it even more popular. For the case of electronic prints or images, the secret can be dealt directly or can be printed on transparencies and stacking is all required further to know results.

According to Naor and Shamir [19], the presumption was that the whole message or image may consist of pixels that are black and white, therefor only two levels will exist. Also the white pixel will be transparent while black will be printed as such. This brings the problem of contrast ratio. The process was lossy in the terms of contrast ratio and this could have created a problem while human visual system decodes the secret. Contrast is an important parameter to determine the clarity of the imaging process. The relative distance among the Hamming weight of black and white pixels enlarged the contrast loss of revealed image.

Hamming Weight, is the count for number of potentially non-zero elements in an array of symbols or elements defined over Galois Field [8].

Later approaches pay more attention over contrast loss by dealing with grayscale and coloured images instead of purely black and white images by using digital halftoning [20]. Size variations of dots and the distance among them creates an illusion that can allow human eyes to merge the dots so that it appears as a continuous tone image. It is worth mentioning that halftoning process is irreversible, the original image can never be reconstructed from halftone image.

Consider the case of (k, n) secret sharing, for a given image, if n are the total number of transparencies generated, and any k of them reveals the secret. There will be nothing revealed unless the number of stacked transparencies is below k. Each pixel makes its presence among n shares. The shares contain m number of binary, so called sub pixel group, that are closely packed. This is Boolean matrix of dimensions $n \times m$ denoted by S. Thus $S = (s_{ij})_{m \times n}$ where $sij = 1 \; or \; 0$.

Important parameters involved in the scheme are [19]:

- $\boldsymbol{m}$: sum total of number of pixels included in a secret share, which counts for the loss in resolution after recovered secret is obtained to that of original image.
- $\boldsymbol{\alpha}$: represents the relative difference associated with the weight of combined shares from black and white pixel actual image or in other words the contrast loss.
- $\boldsymbol{\gamma}$: size of matrices C_0 alongwith C_1, where C_0 points to the part or sub-pixel pattern of the shares of white pixel and C_1 refers the black part or sub-pixel.

For $ORed$ m-vector V, the associated Hamming weight $H(V)$ interpreted as follows [19]:

- If $H(V) \leq d - \alpha m$ for a maintained level $1 \leq d \leq m$, and the relative difference, $\alpha > 0$, then the interpreted pixel is surely black.
- Share construction can clearly be illustrated by a $(2,2)$ visual cryptography scheme or so called $(2, 2)$-VCS. Below are 2×2 matrices required for this process,

$$C_0 = \{ \text{ every matrix obtained after permutating } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \}$$

$$C_1 = \{ \text{ every matrix obtained after permutating } \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \}$$

This approach results in problem called, pixel expansion, where a single pixel in actual image ends up into four pixels. The shares resulted, can be created in accordance to as follows [19]:

- For a white colored pixel in the original or actual image, to generate both shares, choose same pattern of all four pixels.
- For a black pixel in original image, select complementary pairs of pattern. This can be seen in the figure 1.7

Figure 1.7: Black pixel share variations

After superimposing the transparencies and aligning the sub-pixels correctly, the black pixels are Boolean $ORed$ among the rows of the matrix. The possible representation of combination of different pixels can be seen in figure 1.7.

The most advantageous fact about this visual cryptography is that the individual secret share is not capable of regenerating the secret image no matter how hard the computation power is applied.

Figure 1.8 shown on next page, gives the practical view and analytical results of $(2, 2)$ visual cryptography scheme. It depicts the secret or original image, its multiple shares generated and the final recovered image. Image used is Thapar University Logo and is copyright of the respective owner.

The major issue in figure 1.8 $(2, 2)$-VCS is the pixel expansion problem. This results in large sized share images which are cumbersome to manage. This pixel expansion problem can be removed using size invariant visual cryptography.

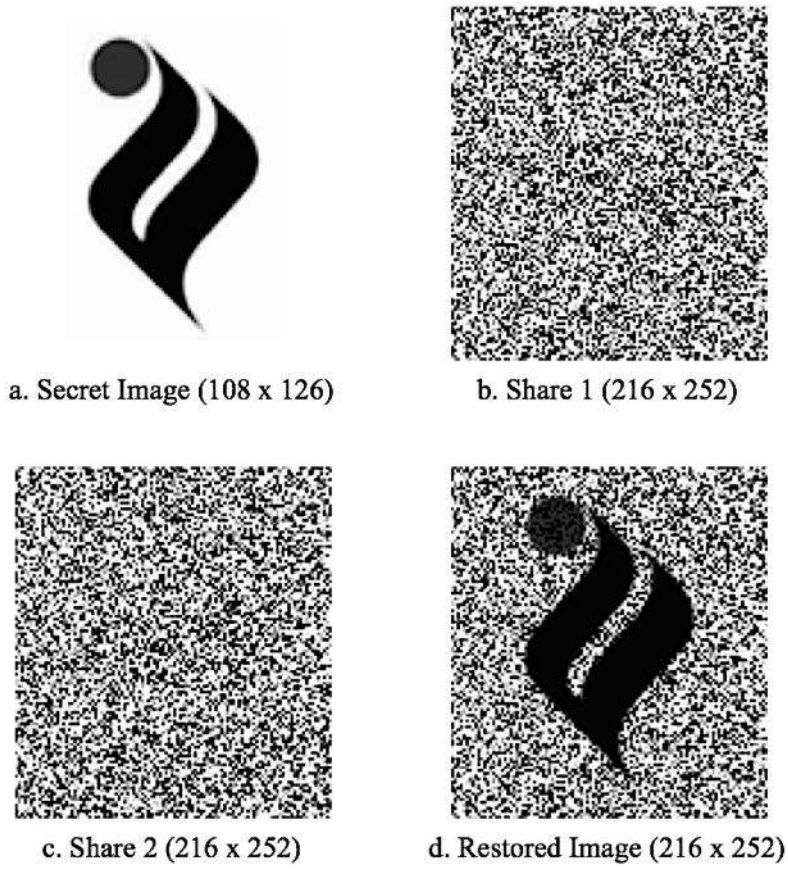


Figure 1.8: $(2, 2)$-VCS encryption process results

1.8.3 Size Invariant Visual Crytpography

Initially stated by Ito et al. [20], to eliminate the pixel expansion issues that arise in the traditional visual cryptography, which results in bigger sized shares that the actual size of original image. These oversized shares are difficult to manage and hence there was a need to define a new type of visual cryptography which maintains same size of shares as that of original image. Ito's scheme eliminates the need of pixel expansion. As defined previously that m, which is the number of total pixels in shared sub-pixels, is one in Ito's approach. This scheme is also (k, n) visual cryptography with a change that $m = 1$ here. To describe the structure or architecure of size invariant scheme, consider a Boolean vector V such that $V = [v_1, v_2, \dots, v_n]^T$, where v_i denoted the i^{th} share image's pixel color. For $v_i = 0$, the corresponding pixel will be white otherwise for $v_i = 1$, the pixel will be black.

For image reconstruction to take place, $ORing$ operation is done as mentioned in section 1.8.2. This Boolean OR operation is applied on pixels in vector V. Probability difference

by which black pixels can be revealed from black as well as white pixels among the secret or actual images forms the root for recovery of secret. Similar to the section 1.8.2, here also needs to form two matrices C_0 and C_1 as follows [20].

$$C_0 = \{ \text{every matrix obtained after permutation of columns of } \begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \dots & & & \\ 1 & 0 & 0 & 0 \end{bmatrix} \}$$

$$C_1 = \{ \text{every matrix obtained after permutation of columns of } \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & & & \\ 0 & 0 & 0 & 1 \end{bmatrix} \}$$

As stated earlier, this scheme does not require pixel expansion, hence the m will always be one and n depends on the type of technique used like for $(2, 3)$ the k will be 2 and n will be 3. Most important property for any of the visual cryptography technique is the contrast. Better the contrast, easier will be the recovery of secret by human vision [19].

The contrast related to this scheme can be determined by finding $\beta = | p_0 - p_1 |$, where p_0 and p_1 refers to the probabilities of retrieving a black or dark pixel from white and a black pixel respectively for secret image [20].

By making use of C_0 and C_1 along with the contrast $\beta = 1/3$, Boolean matrices of dimension $n \times m$ can be obtained as S_0 and S_1:

$$S_0 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \text{ and } S_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (1.5)$$

One of the column of S_0 is selected in order for white pixel to be shared, and one column of S_1 is selected for sharing black pixel. This particular column vector $V = [v_1, v_2, \dots, v_n]^T$ specifies the pixel color of associated shared secret or image. For $v_i = 1$, black color is interpreted otherwise for $v_i = 0$, white is interpreted. For example, if white pixel needs to be shared, then one column among S_0must be following [20],

$$V = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \quad (1.6)$$

This way, the i^{th} element give knowledge about the color saturation of the group of pixels for the i^{th} secret or shared image [20]. For this $(2, 3)$-VCS example, V for white pixel in all the three shares. Similarly black pixels can also be evaluated. This process is followed for obtaining $(2, 2)$-VCS in figure 1.9 and $(3, 3)$-VCS in figure 1.10 as shown below:

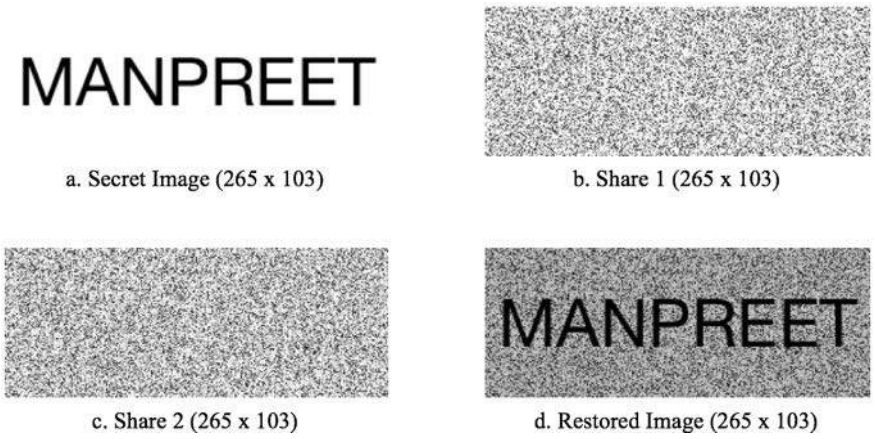


Figure 1.9: Size invariant $(2, 2)$-VCS scheme results

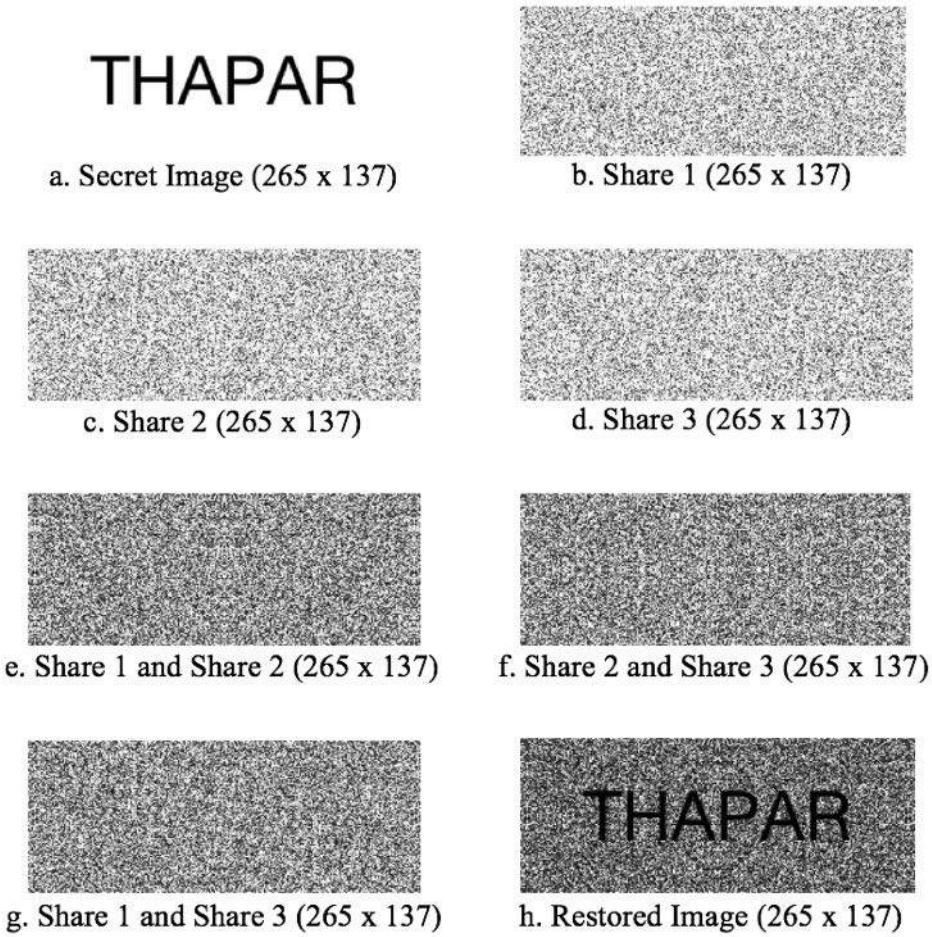


Figure 1.10: Size invariant $(3, 3)$-VCS encryption scheme results

The scheme mentioned in figure 1.10 also provide support for (k, n) or (n, n) threshold schemes. Another example of the mentioned technique extended to $(3, 3)$-VCS is shown next.

1.9 ANALYTICAL ASPECTS

This section deals with analysis of some common aspects that are primarily attached to visual cryptography. These act as limiting factors and tradeoffs for achieving the maximum without pushing the system too far.

1.9.1 Optimal Contrast

Optimal contrast in secret sharing techniques under visual cryptography is always desired. This is because of the capabilities of human visual system that cannot recognise the secret image if contrast loss is more. That becomes hard to focus among the valued pixels if the contrast is low. An approach built on the base of coding theory helps in providing the optimal limits between contrast ratio and sum total of number of sub-pixels. Optimal contrast $(2, n)$-VCS is tested under the Hamming distance approach as well the sub-pixel trade-off. There are schemes available that provides (k, n) optimal contrast by calculating upper limits of contrast. Given below is a table as depicted in Hofmeister [21] that shows some calculated contrast solutions for optimum results.

Table 1.1: Optimal contrast solution values for (k, n) visual cryptgrapy schemes

k/n	2	3	4	5	6	. . .	10	. . .	50	. . .	100
2	1/2	1/3	1/3	3/10	3/10	.	5/18	.	25	.	25/99
3		1/4	1/6	1/8	1/10	.	1/12	.	13/196	.	625/9702
4			1/8	1/15	1/18	.	1/35	.	1161/65800	.	425/25608

1.9.2 Robustness

Primitive visual cryptography made use of nothing more than black and white pixels or binary images. No matter whatever the changes are done the image will still have only black and white pixels. Black pixels will remain black and white as white. This property of resistance against the change no matter how much moderation or alteration is done on images will remain [19].

This robustness makes the binary images resilient to attacks that are commonly applied on images. These attack can be as small as stretching, compressing, trimming or skewing images. One can visualise that after applying these attacks on binary images, their is nothing the pixels can shift their color to. The black pixel will stay black while the white one as such. There is no color present in between them which they can take value of. This makes the binary images robust against such attacks [20].

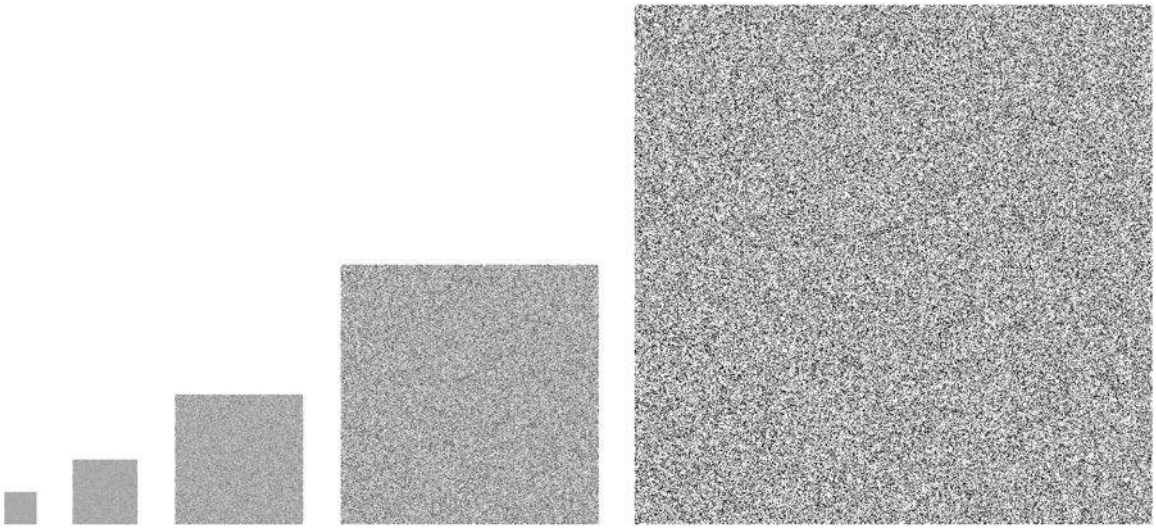


Figure 1.11: Different sizes of same secret

Figure 1.11 shows different sizes of the same secret share. This makes the fact strong that resizing or scaling reveals mothing from a share or transparency. These images can be skewed as well yet these don't provide any clue about the secret. This clearly shows the robust nature of visual cryptography under stated attacks.

1.9.3 Security

Security is one of the most important concern in any kind of cryptographic technique. For visual cryptography, the security is all about randomness that makes the shares look as random or non-deterministic as possible. According to the Naor and Shamir in [19], a random set of pixels are selected. Then, it is required to be found that whether that set should represent black pixel or white in the original secret. If selected pixel is white, every white pixel occurrence is replaced by that pattern otherwise black.

This gives the most important aspect of visual cryptography i.e., until or unless all the shares that are necessary, aren't stacked together and aligned in order, no actual secret can be revealed. No matter how much powerful the computation can be.

This basic rule is verified using the concept of perfect secrecy by Shannon [8]. Remembering perfect secrecy theorem, following two conclusions are derived:

- A cipher system uses a transform T that converts a message space M into ciphertext space C.
- For every element t_i in T i.e., $t_i \in T$, there exists an a priori probability p_i, that is responsible for selection of t_i,
- Also every message has a priori probability associated with it.

Theorem: $(2, 2)$ is a perfectly secure secret sharing scheme [22]

Proof: Consider $(2, 2)$ secret sharing scheme with binary images. Since there are only two colors, either black or white for a pixel value. If white denotes 0 and black refers to 1, then message space M is given as:

$$M = \{0, 1\} \tag{1.7}$$

where $m_0 = 0, m_1 = 1$ are the elements of message space M

Considering all the possibilities for share generation, whole cryptogram space can be seen as:

$$C = \{[1,1,0,0],[0,0,1,1],[1,0,0,1],[0,1,1,0],[1,0,1,0],[0,1,0,1]\} \tag{1.8}$$

If c_j represents the element of ciphertext space C, where $0 \leq j \leq 5$, and every c_j is equally likely. Now, as the message probability is also equally likely, this means, $p(m_0) = p(m_1) = 0.5 \; or \; 1/2$.

Now important thing here is, any share c_j can merge with same kind of share to generate a white pixel or any share c_j can merge with its complementary or opposite share to give result in black pixel, thus

$$p(m_0 / c_j) = p(m_1 / c_j) = 0.5 \, or \, 1/2 \tag{1.9}$$

Hence, this clarifies the fact that for every i or j,

$$p(m_i / c_j) = p(m_i) = 0.5 \, or \, 1/2 \tag{1.10}$$

This verified the theorem and hence states that visual cryptograpy is a secure scheme

1.9.4 Complexity

The most significant problem in visual cryptography is pixel expansion, which results in unnecessarily increase in the dimensional size of secret image shares. Another tradeoff exists, in the search of improving contrast of the secret share image, the dimensional size

of the share is demanded large. This results in large computational complexity while performing image processing [19].

This increase in processing time and complexity practically limits the use of visual cryptography. The share size problem becomes even worse while maintaining the high resolution of the detailed images [20].

As the number of shares associated to a particular secret increases, so does increases the requirement of resources, therefore the management of shares become problem. Large bandwidth requirements are there to limit the use of visual cryptography. These issues are always the concerns of many. Only solution of this can be the optimum scheme, and many schemes are providing near optimum results nowadays [23].

This way visual cryptograpy is easier to understand. One can decide whether to go with the traditional cryptographic solutions or to turn towards the visual cryptography. An extended approach of visual cryptography will be discussed in Chapter 3.

1.10 SECURITY CONSTRAINTS

In previous sections, different kinds of cryptographic techniques are shown. Several issues have been already discussed in those sections like in visual cryptography complexity. There are issues in other techniques as well which are required to be taken care of in order to take maximum throughput from these schemes. There are few scenarios in which attackers or so called adversary can affect the data. These attacks are mentioned below [17, 24].

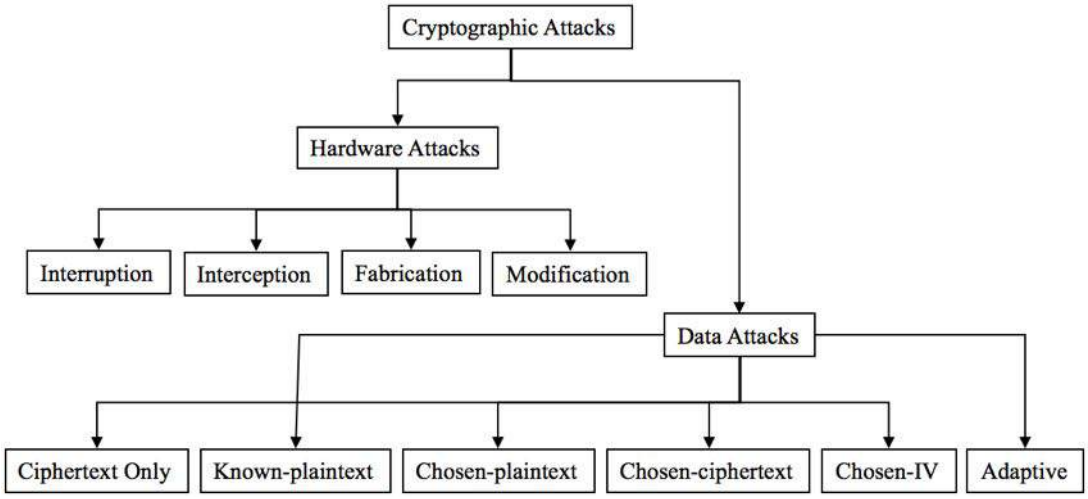


Figure 1.12: Various cryptographic attacks

Figure 1.12 shows some major attacks possible on ciphertext. There are two types of attacking scenario, they deal with acquiring the data and then cryptanalysis. These are explained below.

1.10.1 Data Attacks

This sections presents some most important types of attacks that are applied over the data. These determine the security threshold of the encryption scheme and are as follows:

- **Ciphertext-only Attack:** It the most common attack of all, in which the adversary obtains a copy of encrypted text and tries to crack it [17].
- **Known-plaintext Attack:** This is one step advanced attack, here adversary acquire plaintext and it's corresponding cipher text and tries to resolve the relation between them. [4]
- **Chosen-plaintext Attack:** These are the attacks that only works if the plaintexts have some definite structure or form [6].
- **Chosen-ciphertext Attack:** Under this attack scenario that adversary should know better about how the already sent plaintext is decrypted at the target ends [7].
- **Chosen-IV Attack:** Choose-IV stands for chosen-Initialisation Value attack. The initial value present in header can be used to modify the contents of ciphertext and one can depict the type of encryption was done. [5].
- **Adaptive Attack:** When the selection of given block depends on the results of past data, the attack is known as adaptive [6].

Computational Security, for a given encryption scheme provides n-bits of security if an attack requires computationally exhaustive search for more than 2^n values.

1.11 KEY LENGTH AND IT'S SIGNIFICANCE

For any cryptographic scheme, length of the key is always significance. By an example, it can be seen. For single bit, there are two values i.e., 0 and 1. In other words, if length is increased by a single number the key values increase by twice the actual number. Thus, if key length is 64 bits, the total number of permutations or key values exist can be 2^{64} while if key length is increased by 1 i.e., it becomes 65. the key values become 2^{65} that means twice that of 2^{64}. By this fact, it becomes clear that larger the key, harder will be guessing

and breaking the key. Brute-force attacks made it compulsory to have larger key lengths so that it is not possible to find key as easy as it may appear [25].

Table 1.2: Minimum security requirements [25]

Attacker	Hardware	Min. security
Hacker	PC	52 bit
	PC(s) / FPGA	57 bit
	Malware	60 bit
Small organization	PC(s) / FPGA	62 bit
Medium organization	FPGA / ASIC	67 bit
Large organization	FPGA / ASIC	77 bit
Intelligence agency	ASIC	88 bit

Table 1.2 represents the minimum key length requirements for protecting the scheme from various adversary types present.

- **Brute-Force Attack,** is hit-and-trial method of acquiring passwords or usernames. Computer tries each and every possibility of alphanumeric symbols and proceed until it is successful in breaking the encryption [17].
- **Session Key,** is the key generated for some small session. The system automatically generates new key after each node and this step is repeated. It provides protection against brute-force attacks as the computation complexity is very large [17].

1.12 ADVANTAGES AND LIMITATIONS OF CRYPTOGRAPHY

As a matter of fact, each coin has two sides. If there exist Pros then there must be some cons as well. This is applicable to cryptography as well. This section presents some advantages and limitations of symmetric key, public key, and visual cryptography.

Advantages of Symmetric / Private Key Cryptography

In this section, a few advantages of symmetric key cryptography are presented. These are most important ones.

- **Simple:** Private key cryptography is very simple to implement. All it requires is data and a key. The same key is used on both the ends to encrypt or decrypt message or plaintext [17].
- **Robustness:** Same key can be used by a single user if only he is going to access the data. Generating new keys is not mandatory if the data access is limited to him only [5].
- **Less Complexity:** Since same is used for both processes, the techniques are fast. These have little or less computational complexity, so it is suitable for long messages [6].
- **Efficient:** Symmetric encryption is efficient in the sense that it does not waste resources in creating public and private keys separately. This is very easy to implement and requires far less resources compared to public key crypto systems [4].
- **Limited Damage:** In a case if a key is compromised, then only those participants are affected which were linked to that key, however since other participants use separate keys for there communication, this prevents from mass leakage of data [6].

Limitations of Symmetric / Private Key Cryptography

This section shows the negative side of symmetric key cryptography. These can determine the usage of this approach in common context.

- **Secure channel:** Symmetric key systems face a problem of key transmission over to the destination using a secure channel. Lacking that may led the compromise of key and may affect the whole communication. So need of secure channel is a negative point here [7].
- **Large Key Database:** As multiple participants require multiple symmetric keys, the number of keys increases linearly. This increases the size of database to personally store more keys. Also there are chances one can forget the key or may confuse it with someone else [5].
- **Integrity Question:** There is always a lack of integrity in symmetric key encryption. Anyone who can access the key can change or modify the contents and there will be no information about the modifier. This can create dispute among the participants about data surety [5].

Advantages of Asymmetric / Public Key Cryptography

Public key cryptography has many features to show and remarkable are the things one can do using asymmetric key cryptography. Advantages of public key systems are as follows:

- **Convenience:** Since there is no longer required to seed private keys to other participants, just public keys are made open and private keys are kept safe [17].
- **Authentication:** Public key systems make it possible to sign documents that can be certified or verified. This helps in ensuring the authenticity of the document [7].
- **Integrity:** Since the one with private key can modify the document and not the public key bearer. Thus any forging can be detected and those who own private keys can be brought to justice [5].
- **Non-repudiation:** An amazing advantage is proof of non-repudiation. In a case the issuing party tries to deny a signed document, this scheme won't let that happen. As the singing party is bounded to the document as only that party can create the document using private key and not the others with a public key [4].

Limitations of Asymmetric / Public Key Cryptography

The other side of coin, this section shows some of the limitations which public key systems offer.

- **Key Authentication:** The public keys must be verified. There is no surety prior to the checking that whether the key may work or is it the intended key for the given document [7].
- **Slow:** This system is far slow as compared to the private key systems. Thus it cannot be used to decipher bulk messages [6].
- **Resource Limitations:** Public key crypto systems make use of more resources as compared to the private key systems [7].
- **Mass Infringement:** Once a person detects the private key, he can read all the intended messages and even can mass forge the documents to create misleading or chaos [6].
- **Irreparable Damage:** If the private key is lost, there is nothing a person can do. All the messages becomes useless without decryption and the damage done is irreparable [4].

Advantages of Visual Cryptography

In this section advantages and features of visual cryptography are discussed and these are as follows:

- **Human Visual System:** The biggest advantage of visual cryptograpy is that it requires no computers or any machine to recover the secret hidden. Human eyes are far more capable of doing this. However, new schemes are there which increase the resolution and contrast at the cost of complexity and making it no longer possible for human vision system to decode it, yet these require little computing power as compared to any public or private key systems [18].
- **Perfectly Secure:** Visual cryptography is nearly a perfect sharing scheme. It is not possible to retrieve any useful information from one single share or the number of shares to be stacked are less then the desirable amount, there is no method to obtain secret no matter how much computing power is present [19].
- **Robustness:** Any scaling, skewing, streching, compressing or trimming actions does not provide any information hidden in a secret. The pixels that are black will stay black and similarly white. Visual cryptography can withstand these mentioned attacks perfectly [22].

Limitations of Visual Cryptograhy

No system is perfect, hence visual cryprography also has few limitations and these are jotted down as follows:

- **Contrast Loss:** This is the most significant problem related to visual cryptography. The contrast is divided among the number of shares. Since the lesser the contrast, lesser will be the human eye capability to distinguish between random pixels and secret pixels. Hence, contrast loss is directly linked to number of shares and increases with increase in share count [21].
- **Pixel Expansion:** Single pixel is shared among multiple images. This creates cumbersome approach to deal with. Due to this, pixel size is increased un-necessarily [23].
- **Larger Size Shares:** Traditional visual cryptography schemes create shares that are larger than the dimensions of actual or secret image itself. These larger shares themselves, hard to handle, as perfect alignment is tough in bigger shares case [22].

1.13 ORGANIZATION OF THIS THESIS

In this thesis, starting from the basics of cryptography through the advancements in the field of visual cryptography are shown. The aim of this thesis was to study various algorithms provided already in literature and then to design an approach that can be easier to operate yet more secure and easier to implement. There is a proposed image encryption algorithm which drives the thesis and is discussed in detail in chapters 4 and 5. Following is the outline of this thesis and the main contribution of each chapter:

- In Chapter 1, the core foundations of both traditional and visual cryptography are discussed. The terminology involved alongwith standards are mentioned. Also the outline of thesis is drawn.
- In Chapter 2, work done by various researchers has been studied to observe best possibilities; so as to find the gaps and then to draw the conclusion. This section mentions some of the relevant papers that helped in achieving the targetted results.
- In Chapter 3, critical analysis of advanced version of visual cryptography has been done. Further, taken into account is the process of replacement of traditional visual cryptography by new more efficient, secure and fast algorithms.
- In Chapter 4, the proposed work is discussed. A modified image encryption algorithm has been developed and all the necessary steps and the path followed is shown in this chapter. Finally the key parameters on which the proposed algorithm works is discussed. Extended version of the proposed methodology is also mentioned in this chapter.
- In Chapter 5, the results of simulation, its comparison among other schemes and the dependent factors have been discussed.
- In Chapter 6, the last and final chapter that shows the concluding remarks of the proposed work and the scope for the future work is discussed.

CHAPTER 2

LITERATURE REVIEW

This section introduces the research work done by various scholars in the search for development of secure and better cryptographic algorithms for data as well as images. The literature review has been carried out by dividing the work in two categories that are i) Data encryption and ii) Visual cryptography. Observations have also been discussed and conclusions are drawn. Finally, problem formation is discussed and objectives are determined.

2.1 DATA ENCRYPTION LITERATURE

This section involves workdone in the field of data encryption or simply the field of cryptography. Observations from this section are also discussed at the end.

N. Koblitz *et al*. [26] concluded the powers of elliptic curve crytpography, multiplicative group comprising of finite field was used to find elliptic curves. These systems were far better in terms of security than the analog counterparts. Only problem faced was the structure has finite field as a multiple group which makes the computation quite large.

M. J. Wiener [27] worked to unveil the security backdoors of short RSA exponents. The attack was made possible by finding numerator and denominator based on continued fractions in realtime. RSA algorithm was later replaced by the Data Encryption Standard (DES) and even later by Advanced Encryption Standard (AES) due to its small key space.

L. Ham *et al*. [28] proposed a triple layered identity module. The base of this module was framed on discrete logarithms. The first layer incorporates user identity verification, while second layer was process of digital signature. Finally the third layer was key distribution approach. The system was designed in such a way that each user was required to visit a Key Authentication Center (KAC) and prove its identity, only then the key was allocated to the user. Limitation of this approach was that the process was very lengthy and not suitable for quick access.

H. M. Sun *et al*. [29] designed a dual RSA scheme, the new variant could produce two key pairs with same public as well as private exponents. This scheme brings a blind signature technique along with authentication. However, the disadvantage of this dual RSA scheme was its computational complexity, which was large.

Halkidis *et al*. [30] showed the architectural risks posed on the security pattern. They designed an algorithm to deal with the missing security patterns for key unlocking. The estimation could be done after designing phase, which reduced the cost of implementation. The risk of software system can now be extracted autonomously. These backdoor attacks can be counteracted if the algorithms can verify key checksums after each iterations.

Q. G. Bin *et al*. [31] proposed a scheme to encrypt images by making use of DES alongwith simple chaotic sequence. Firstly chaotic sequence forms the base for generation of key after being fed to DES. This process increases the key space. Thus, security is increased to a large extent. The problem associated with this scheme was the coding complexity, which involves conversion between keys and chaotic sequences.

Z. Yun *et al*. [32] researched in the field of chaotic algorithms. They proposed a new improved version to the DES combined with chaotic encryption. The comparison to the solo DES and Chaos modified visual cryptography approach was also discussed. However the accuracy of the resulted image obtained after decryption through their proposed approach was limited.

S. Zhou *et al*. [33] worked for utilising DNA sequence for creating encrypting scheme for big images. The proposed scheme was successful in reducing encryption time. Scheme makes use of original DNA sequence as a key. Firstly, the original image was scrambled or shuffled to make it appear like less correlated to the actual one. Then the process of pixel replacement is applied. It utilise three templates for XORing with the secret share on bit by bit basis. However the key generation for this could be more difficult due to the length of DNA sequences. Hence key management was tough.

S. F. Mare *et al*. [34] showed a process of sending data using RSA along with DES and Steganography. They also managed to combine two cryptography technique together with steganography. This joint solution could withstand different types of attacks and was

capable of standing against reverse engineering. Advantage of this approach is the reliability as it covers most of the aspects like security and robustness. However the structural differences among these schemes play vital role in allowing hackers to crack the encryption scheme.

X. Li *et al*. [35] developed a novel tool for encryption authentication convertible method without the need of hash functions. This allows the recipient to decrypt the message and check its authenticity without disclosing to the public. The converted signature was required in order to check authenticity even if signature was lost. However, for the scenario of lost key, there was no method to check genuineness of the message.

K. Sakiyama *et al*. [36] built a theoretical scheme for differential fault analysis to ensure optimality. These analysis were performed on AES. These were active attacks to produce an error in operation and to pull the secret information. These attacks could be reduced further to achieve optimality. However, these attacks require far more time than the conventional ones to retrieve information.

Pavan *et al*. [37] expanded the hill cipher technique to image steganography. They modified hill cipher to hide the text message behind an image. The key was encrypted inside the cover image and scrambled accordingly which allows the elimination of key distribution overheads. However, hill cipher could be easily hacked by these days machines.

Y. Zhou *et al*. [38] introduced a new parametric Gray code, the NKP Gray code, very robust technique that has the potential to be used for bit plane extraction, image demonising and image encryption. However, the technique has limitation that it involves cumbersome workload to convert images back forth between other radix and radix 2.

H. Jo *et al*. [39] designed a database security mechanism for safely managing the connectivity with Open Data Base Connectivity. The scheme is different form traditional as it makes the use of Graphics Processing Unit (GPU) for computation processes. The integration of approach with Cuda technology and MySQL connectivity. The limitation of their design was that if the system lacks GPU, the appraoch turn outs to be very slow.

R. U. Ginting *et al*. [40] designed a more secure scheme for image hiding, which was based on RC4 stream cipher algorithm and chaotic logistics map. The also designed algorithm works as converting the external key into initial value. Then this initial value was used to generate a key stream with the help of chaotic logistic map function. This is then processed by permutation and the result was then XORed with bytes stream of digital image. The problem was the encryption time. More encryption time results in less hacking time.

A. Anees *et al*. [41] explored the drawbacks of substitution-box for highly correleated data. They also designed a novel scheme for chaotic substitution to adress this issue. Their approach is strong in matter of encryption. However, the limitation of their work is the structure of algorithm is complex for implementation view point.

M. Zanin *et al*. [42] proposed a novel scheme which they call as P-box method. Their approach avoids round-off errors for floating point operations. They also combined their P-box approach with chaotic S-box for logistic map. However the comlexity of designing method is large.

S. Nagaraj *et al*. [43] worked in the field of Euler's Totient theorem, and developed a data encryption scheme for adding signature keys before transmission of data. This key can be verified as well at the reciever side. Limitation of this approach is that it can be prudent to attacks easily.

2.2 OBSERVARTIONS FROM DATA ENCRYPTION REVIEW

From the literature review, following observations have been drawn for data encryption:

- Key management is poor in many approaches, thus key handling is tough for some schemes. Moreover, a single key is incapable of providing fully secure encryption if the key length is small.
- Processing time for highly complex encryption algorithm is very large and hence performance is compromised. Optimum hardware is necessary for keeping all primitives under limits.
- Many schemes are vulnerable to data attacks, hence they are easier to break.

2.3 VISUAL CRYPTOGRAPHY LITERATURE

This section involves workdone in the field of visual cryptography, observations from this section have also been drawn.

S. Cimato *et al*. [45] brought forward the color (k, n)-TVC scheme, that was optimal in the sense of contrast ratio. The proposed scheme was a subset of other canonical schemes. These canonical schemes also holds on the symmetry properties. But, this scheme was vulnerable to attacks and also introduced interference among the participating secret images.

R. Youmaran *et al*. [46] enhanced the work done by Chang *et al*. [44]. The proposed visual cryptography scheme enables colored images to be hidden inside the secret shares by making use of color coding table. Best thing about this scheme was its lossless ability to retrieve original secret. But, the scheme suffers the pixel expansion to a great extent.

Z. Wang *et al*. [47] extended their previous work in the field of halftone visual cryptography. They successfully merged the pixels of secret image into n shares by simple mechanism of error diffusion. The quantization error was minimized by simply distribtuing the error among the neighboring pixels. Advantage of this approach was that the interference among the pixels was absent. However, the approach was applicable to halftone images only and not on colored images.

Z. Wang *et al*. [48] extended their previous work [47] in the field of halftone visual cryptography. They successfully hide the meaningful secret into n binary images. They efficiently introduced error diffusion to achieve contrast rich images in the end. However, the security of the approach can be compromised as the interference among the images is can result in potential detection of secret.

H. C. Wu *et al*. [49] proposed an approach for encryption of color images. This scheme made use of halftone technique as the base, with color coding table for converting colors to grayscale levels. Finally a secret coding table was also utilised to create two meaningful shares. However, this requirement of two separate conversion tables is additional problem. Also the conversion also takes time and limits the realtime use of approach.

Z. Wang *et al*. [50] modified the Halftone Visual Cryptography (HVC) scheme that was built on the technique of digital half toning process. The concept could be easily implementable. The limitation of this process was that there exists a tradeoff among the quality of the share and contrast ratio.

F. Liu *et al*. [51] worked the direction of creating a simple OR and XOR visual cryptography as an application of $(2, 2)$-VCS. It allows a participant to receive multiple share images. Pixel expansion achieved optimality in the sense that the contrast loss was justified. Still there was room for improvement in their work as access structure for obtaining minimum average pixel expansion was still a problem.

I. Kang *et al*. [52] proposed a new concept in the field of visual cryptography. System they named were Visual Information Pixel (VIP) system. It worked on the approach of synchronization as well as error diffusion. Results were rich in saturation and overall aesthetics of the secret. This scheme also holds on to the pixel information. But the approach has time constraints as it could take more time in encryption process due to the color management of the system.

S. Katta [53] proposed an approach in which the image was divided into its binary format. Each pixel is divided among three full shares in such a way that combining two particular half shares can reveal the actual secret. So this scheme was an extention to the $(2,3)$-VCS. The major limitation of this scheme was that there were unnecessary shares being created. As the actual image coulb have been retrieved from two half shares only, there was wastage of bandwidth for digital transmission.

N. S. Alex *et al*. [54] worked in the field of halftone visual cryptography. It starts with obtaining meaningless shares as cover images and then permutating with the actual secret to gain the encrypted image, which is finally error diffused to obtain the secret shares that are distributed is the whole process. This process is somehow more lengthy then the traditional and obtained shares can bleed information if analysed properly.

D. Wang *et al*. [55] worked in dynamic visual cryptography. The scheme they proposed allows the shares to have a lateral shift between them. When both the shares are stacked together in the same alignment, only then the secret is revealed otherwise not. The

limitation of this scheme was that in and only if the shares are stacked in the same degrees then only decryption could take place. So perfect alignment was required for this scheme to work.

F. Liu *et al*. [56] enhanced the approach of extended visual cryptography. They worked to produce a third share by mixing cover images with other random shares. Experimental results shown by the scheme was better than the norman visual techniques. But the need to generate completely random shares for overlapping process could result in complexity of the scheme.

P. Chiu *et al*. [57] developed a pixel zero expansion scheme for threshold visual systems. Their scheme optimised the encryption process of binary images. They designed the method that counts darkness as the parameter to measure quality of the image. They further provided the algorithm for balancing density. As the matter of performance, the share handling was considered as a major issue in their work.

Y. Hou *et al*. [58] worked on the concept of progressive visual cryptography. This designed approach results in un-expanded pixel shares. The likelihood of obtaining one of the two complementary colors i.e., black or white was equal, which comes out to be $1/n$. However, the image obtained after decrypting certainly lacks the quality.

T. Chen *et al*. [59] proposed a unique random grid visual scheme that provides two main advantages, which were, zero pixel expansion and also user friendly. The limitation of their work was that the information could possibly leak into other shares that were being generated. When these leaked shares combine they result in distorted outputs.

R. Wang *et al*. [60] worked in the field of tagged visual cryptography. This approach is an extended version of traditional visual cryptography, in which, addition to the secret shares generated, an extra tag value t is also provided. This tagged value t depicts the minimum number of shares necessary for decryption to take place properly. This approach is collectively known as (t, n)-Tagged Visual Cryptography. Only issue associated with this approach is that if in case the value t is lost, then it would be very difficult to obtain the secret again.

S. Lin *et al*. [61] enhanced the research in the field of (t, n)-Tagged Visual Cryptography. They proposed a new methodology in which the generated transparencies can further regenerate more transparencies. This change allows the n to be increased drastically. The benefit of doing this is that it no longer requires the original transparencies to be used for generating secret. Since the n is increased continuously, the pixel expansion is the major issue involved.

M. Iwamoto [62] proposed a two visual secret sharing schemes. First scheme was named as Unconditionally Secure (US) acheme while the other as Weakly Secure (WS). The concept shows that the color image encryption using WS scheme achieves more vivid and brighter images as compared to the US scheme. The major issue involved was the weak security for WS scheme and contrast loss for US scheme.

S. J. Shyu *et al*. [63] implemented the linear programming for creating a novel and better Region Incrementing Visual Cryptography Scheme (RIVCS) in terms of efficiency. The proposed approach minimises the associated pixel expansion issues. The overall structure of this approach was complicated to be used in general.

S. Shyu [64] worked in the field of Random Grid (RG) visual cryptography. Author showed the potential of using visual cryptograms for random grids. The main feature of this work was the elimination of pixel expansion process. However random grid implementation is complex in terms of resource utilisation.

K. Lee *et al*. [65] worked for creating a scheme to utilise binary secret shares which were easy to handle. The scheme they proposed consisted of two phases. First phase results in creation of meaningless shares while second phase ends up in adding secret covers through stamping process. However, the aftermath shows that the quality improvement has small increment only.

D. Wang *et al*. [66] worked on an approach for grayscale n Reversing based Visual Cryptography (RVCS) with least possible pixel expansion. They also proposed an approach to obtain optimalilty in contrast Grayscale RVCS (GRVCS) which uses the basis matrices of perfectly black nRVCS. However, this scheme could not be used on color images. Hence this approach was limited to grayscale images only.

R. D. Prisco *et al*. [67] improved several schemes to know the upper limits of radom grid visual schemes. By carefully examining these results obtained from random grids, they provided new schemes for the deterministic model. These schemes can only perform well under the case of smaller key lengths and not on large keys.

N. Askari *et al*. [68] designed a fresh approach towards the visual cryptography by improving the secret share quality levels. The scheme could suppress the pixel expansion problem and contrast loss factors. The only problem associated with this work was the dimensional size of the original shares increased, therefore handling the large sized shares was difficult.

X. Wang *et al*. [69] designed an efficient scheme for multiple secret sharing scenario. The Tagged Visual Cryptography (TVC) they proposed could be capable of covering tagged images through randomly selected shares. This Probabilistic Lossless TVC (P-LTVC) solves the potential security problem of LTVC. There was structural imbalances present in the scheme which leds to potential leak of information from one secret into other.

D. Ou *et al*. [70] worked on an approach to take over the pixel expansion problem by designing a new approach by making use of $2^n \times n$ matrix for constructing (n, n) XOR based visual cryptography. The scheme's resulting images are however shows loss in contrast ratio.

P. Chiu *et al*. [71] introduced the concept of user friendly threshold scheme for visual cryptography. They eliminated the inter image interference problems in the previous schemes for non-computer aided decryption environments. The problem this technique braught was pixel expansion. Also the contrast quality was low.

X. Yan *et al*. [72] proposed a new halftone visual scheme with the use of minimum auxiliary dark pixels or black pixels being distributed homogenitically. This process requires embedding of secret share among the meaningful secret shares. This also requires the error diffusion process. The limitation of this approach is that the size of the secret shares increases to large extent. So handling of shares is tough.

C. Yang *et al*. [73] throws light on a strong threshold (n, n) Multi Secret Image Sharing (MSIS) scheme without leaking partial secret information from $(n-1)$ or fewer shared images. This process re-allocate pixels without disturbing the intensity levels. Proposed modified (n, n) -MSIS scheme could restrict attacks. Also they discussed further enhancement for the randomness of shared images. However, the proposed system still offers the pixel expansion problem.

C. Yang *et al*. [74] worked in ratio invariant visual cryptography scheme. They designed aspect ratio invariant cryptographic approach to handle the distortion. However the approach has a limitation that extra pixels were required. The pattern designing is a complex part of the scheme.

2.4 OBSERVATIONS FROM VISUAL CRYPTOGRAPHY REVIEW

From the literature review, following observations have been drawn for visual cryptography:

- Most of the secret sharing schemes suffer with pixel expansion problem which generates multiple shares, therefore require more bandwidth. This also causes contrast loss issues.
- Memory requirement is large for storing multiple shares of a same image. Hence, there is a room for improvement in memory aspect.
- Using single sided encryption, the resultant image could be filtered instead of decryption depending upon type of noise and filter used. By this way one can save a lot of time, however the scheme may have inferior quality.

2.5 MOTIVATION AND PROBLEM FORMATION

From the observations drawn in the previous section, it has been found that there are problems such as pixel expansion, contrast loss, lack of efficient key management system, computation complexity, and vulnerability to attacks. Also the images being transmitted over the channel can be the potential source of leakage of privacy of the users. These issues support the fact that image encryption is one of the favorable topic for consideration in today's world. There is a need to develop a visual cryptographic model which has better performance and more accurate picture quality. There must be a single encrypted image that requires no multiple shares to be transmitted in order for retrieving the original secret

image. This preserves numerous resources like size for storage and bandwidth during transmission. The computation complexity must be less. For conserving the designer's manpower, it would be better if the encryption unit can be used as decryption also. This not only saves time in building the decoding unit, but also helps in creating a universal architecture for encoding and decoding. All these necessary and noteworthy observations are taken into account while designing the proposed approach for this thesis.

2.6 OBJECTIVES

From observartions, the following objectives have been drawn:

- To analyse various visual cryptography schemes and study the performance as well as the associated issues with these schemes.
- To develop a modified image encryption algorithm based on Knight's Tour Problem which meets the desirable characteristics like lossless encryption, easier key management, no contrast loss and zero pixel expansion.
- To compare the proposed scheme with the existing ones.

CHAPTER 3

ADVANCED VISUAL CRYPTOGRAPHY

Advanced Visual Cryptography gives an overview of the developments that separate it from the traditional limits of visual cryptography. This evolved technique allows misguiding the people who are not intended to view secrets. Although everyone can see the shares as meaningful but this is done to trigger suspense in their mind that encryption has been done while revealing the true information to only those who are worthy. These techniques incorporate all the features which are present in traditional visual cryptography. This chapter includes the techniques studied in literature review and shows some of the evolutions of visual cryptography

3.1 HALFTONE IMAGING

Halftone is the process of transforming the coloured or grayscale digital images into binary black and white images [75]. This process is done by comparing the pixel value of the colored or grayscale image with a predetermined threshold level. If the pixel face value is more then the specified threshold, then corresponding pixel is assigned white color in the new image, and if it is below the threshold, black is assigned. This way the whole image is converted into halftone image. This can be seen in the images printed in the newspapers and magazines and is shown in figure 3.1.

Figure 3.1: Halftone image of a cat's eye [75]

The benefit of doing digital halftoning results in better contrast and high image quality after the process of visual cryptography is applied. In Halftoning, the disk size varies accordingly and the density increases in reference to the characteristics of the actual image [76].

3.2 ERROR DIFFUSION

Error Diffusion is the next step in digital halftoning process [54]. The scanning of image is done row-by-row and pixel-to-pixel. Beginning with defining a threshold, the pixel values are compared to the threshold. Once the quantization error is computed, its value is added to the next unprocessed pixel and this process is followed until the whole image is converted into the halftone. Error diffusion process is an area operation as the effect of an operation done over a pixel affects the entire image. This accounts for the requirement of buffering [80].

The benefit of error diffusion over the typical halftone process is that is enhance the edges of the image. It helps in text recognization more superior than the simple halftone image [54]. Shown below in figure 3.2, is a comparison between a regular grayscale image and its error diffused halftone counterpart.

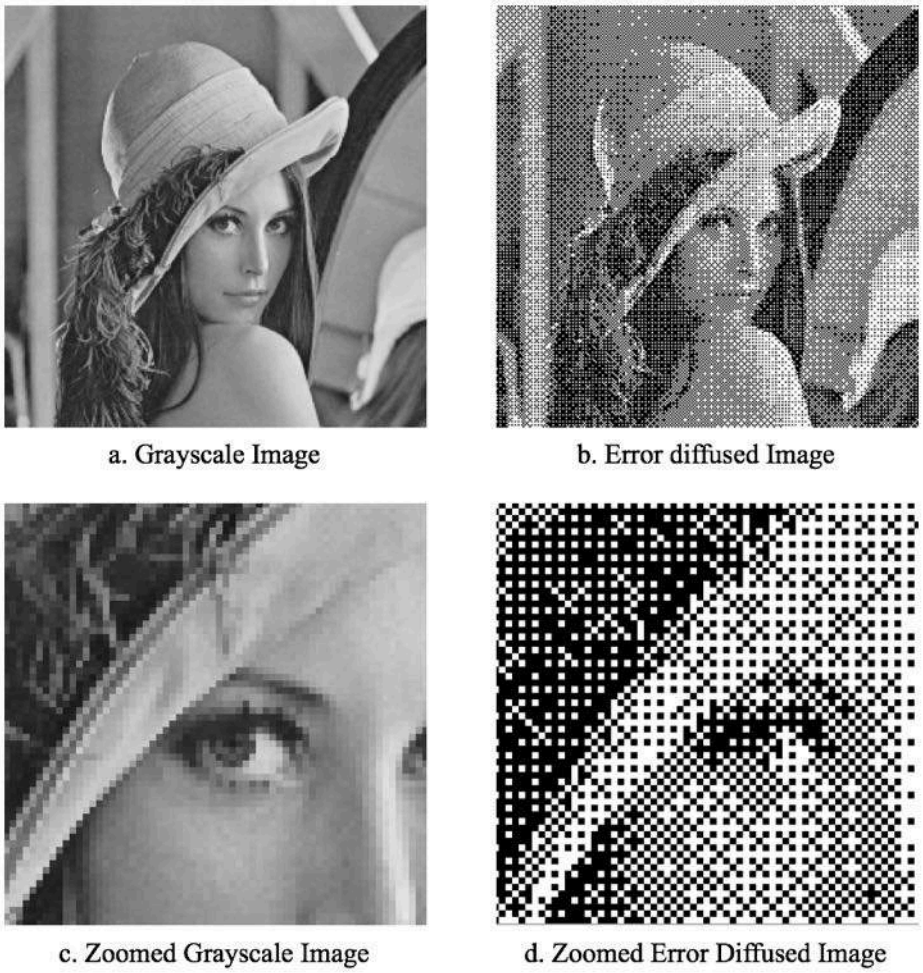


Figure 3.2: Comparison between grayscale and error diffused halftone images

Comparison between grayscale image and error diffused halftone image has been shown in figure 3.2a and figure 3.2b respectively. Figure 3.2c and figure 3.2d shows the 4× zoomed of these two images respectively.

3.3 EXTENDED VISUAL CRYPTOGRAPHY

Extended visual cryptography is an approach which is modified in such a way that the shares generated of a secret image shows some meaning in contrast to the random noise like image. This was a key characteristic of traditional visual cryptography [47]. These meaningful looking shares are actually fake shares which points the share stalker towards useless information while they think they have got something meaningful. These are like masks beneath which the actual secret information is hidden. When these multiple shares incorporates some cover image, are combined together, reveal the actual hidden secret image [61].

For a general computation, this scheme is denoted as

$$C_c^{c_1,c_2,\dots c_n}, where\ c, c_1, c_2 \dots c_n \in \{b, w\}, \quad (3.1)$$

These are the group of matrices which are used to find the shares, if c_i represents the color of i^{th}cover image while c being the color of actual secret image. For the implementation of this scheme, 2^n number of pairs of these collections are needed to be generated, with each one of them containing every possibility of occurance of black and white pixels together in n number of the actual images [47].

Nothing is known about the pixel face value in the secret image. The only thing that matters is either black pixel or white pixel. There is no probability density about the distribution of these black and white pixels as one can have no idea about how frequently the white pixel occur or the black one [61].

Necessary conditions to take care of for this extended visual cryptography to work are as follows:

- The images which are used as cover image, once are encrypted, must reveal the actual secret image beneath them when are superimposed.
- No matter how much inspection is done on the shares, nothing should be revealed about the secret image.

- The secret image hidden underneath should not be altered and must be recognisable after decryption.

A simple example depicting $(2, 2)$-Extended visual cryptography is shown below. The $C_c^{c_1,c_2}$ matrices can be generated by every possible permutation of the columns of the given matrices as in [47]:

$$S_w^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} and\ S_b^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad (3.2)$$

$$S_w^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} and\ S_b^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad (3.3)$$

$$S_w^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} and\ S_b^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad (3.4)$$

$$S_w^{ww} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} and\ S_b^{ww} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad (3.5)$$

However, the contrast is just ¼ of the original secret image.

Visual example presenting $(2, 2)$-Extended visual cryptography is shown below:

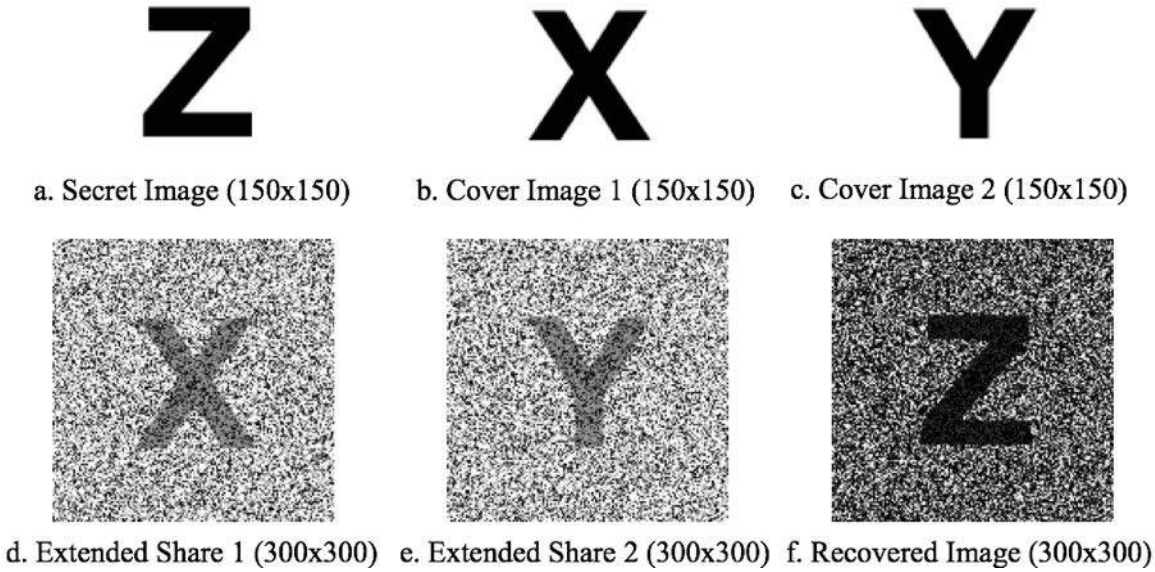


Figure 3.3: (2, 2)-Extended visual cryptography results

Figure 3.3a. shows the actual original secret image that is required to be sent. Figures 3.3b and 3.3c shows the meaningful cover images used in this process respectively. Figures 3.3d and 3.3e shows the secret shares images that are generated and finally, figure 3.3f shows the actual decrypted secret image. Thus, it clarifies the fact that the shares which are transmitted, appear as meaningful to the audience while they are just the cover images.

3.4 CHEATING IMMUNE VISUAL CRYPTOGRAPY

Mostly, cryptanalysis results in breaking the secure appearing visual cryptography scheme. Several methods for cheating the traditional as well as extended visual cryptography are present in [76, 77]. There are methods discussed for protection against cheating in [76] which focuses on the identification of the participants to prevent them from cheating. Also, Yang *et al*. [78] worked in this field and proposed two methods for cheating prevention. One method focuses on online authority that can verify the participants while the second method involves overlaying two shares to reveal a code in the form of verification image. But this method requires extra pixels to be added to the main secret image.

There is another prevention scheme by Horng *et al*. [77], in which the attacker need to know the pixel distribution among each of the shares. If he is capable of finding this distribution then cheating can be done. Horng's approach actually prevents this from happening by making the distribution non-recognisable to the intruder.

3.5 DYNAMIC VISUAL CRYPTOGRAPHY

The logic behind the dynamic visual cryptography is to increase the overall capacity of the visual scheme. If two or more shares are being used in a scheme, there is power to hide two or more secrets. This rule drives the visual cryptography's dynamism. This increases the capacity of the scheme and still maintains the size of shares in the optimal range.

3.5.1 Multiple Secret Sharing

Wu *et al*. [79] introduced the Multiple Secret Sharing (MSS) scheme. They successfully covered two secret images into two separate shares. If shares are denoted by S_1 and S_2, the primary secret image was recovered when S_1 overlapped S_2. The other secret image was revealed when S_1 was rotated in counter-clockwise 90 degrees angle as shown in figure 3.4.

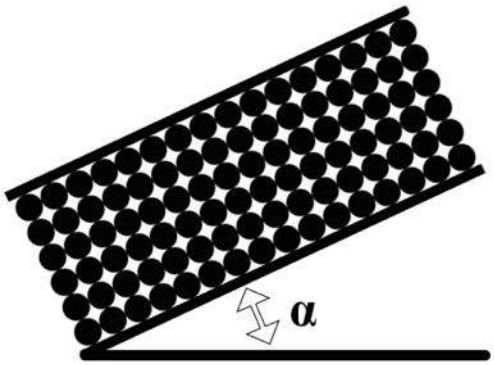


Figure 3.4: Angular adjustment among shares

Due to the fact that the secret share can be rotated only through 90, 180 and 270 degrees actually limit the number of secret images which can be hidden inside the shares. Further, researches have made it possible to hide secrets in such a manner that whenever new transparencies were stacked, new secret image was revealed [80] and is shown in figure 3.5

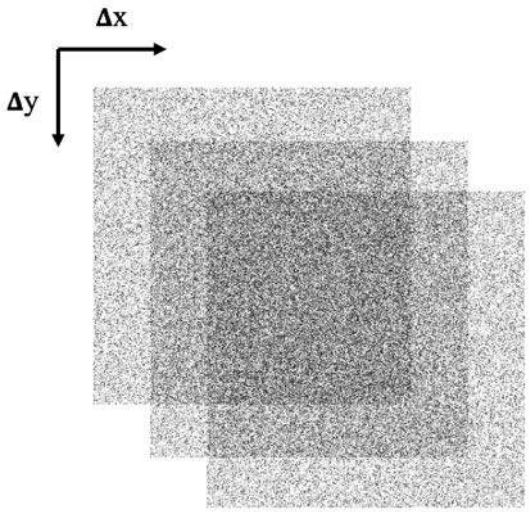


Figure 3.5: Stacking process of multiple shares

This approach was further enhanced by making it independent of limited angles of rotation between the secret shares [81]. This was made possible using circular shares. When secret share S_1 was stacked over S_2 and with any one of them rotated clockwise through an angle which lies between 0 and 360 degrees, the secret image was revealed.

3.5.2 Contrast Based Joint Visual Cryptography

The idea behind the contrast based joint visual cryptography is evolved from building a scheme in which multiple shares could be made along with a single master key [82]. This master key when overlaps the secret share, should recover the secret and if the same key is

swiped horizontally or vertically reveals the second hidden secret. This process could be done by first copying the black pixels from the first secret onto the corresponding positions of the blank image. Then for the second image, the black pixels could be copied onto the blank space left on the share after copying the first secret. This makes the combined secret possible. The rest of the space is just overlapped by the patterns of corresponding to the white pixels. The involved mathematics can be seen as [82]:

$$b_{w,w}^{w} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \tag{3.6}$$

$$b_{w,b}^{w} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \tag{3.7}$$

$$b_{b,w}^{w} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \tag{3.8}$$

$where, b_{s_1,s_2}^{c} \in \{0,1\}$ represents the pixel value corresponding to the pixel s_1 belonging to share $S_1$and pixel $s_2$belonging to share $S_2$and $c \in \{0,1\}$ is the corresponding pixel of the cover secret image.

Consider two secret images and one master key. Using the scheme, corresponding share are created. These two shares will be merged together in such a spatial way that they do note intersect. To reveal the hidden secret image beneath the common share, master key should be stacked onto different parts of the share and the secrets could be revealed. Shown below in figure 3.6 is an example of Joint Contrast visual cryptogaphy.

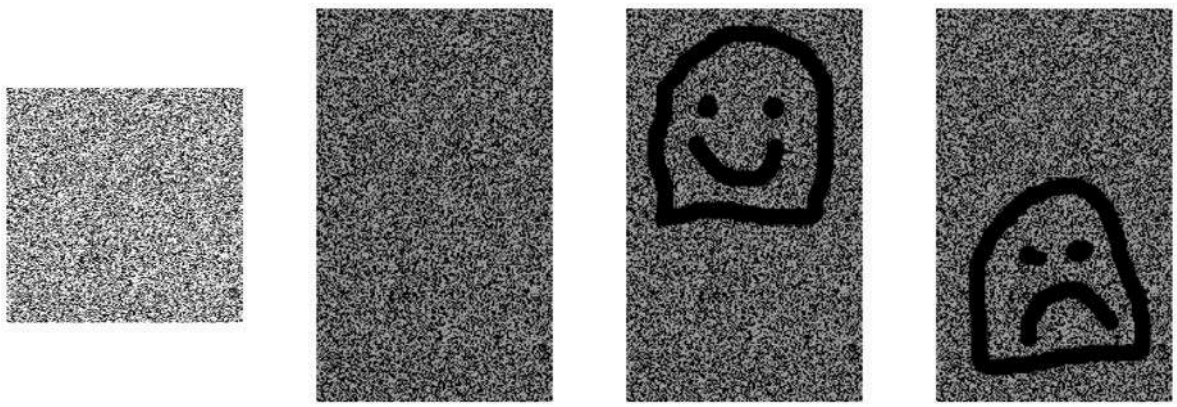


Figure 3.6: Joint contrast visual cryptography results with two secrets [22]

Figure 3.6a shows the master key, figure 3.6b depicts the combined share and next two figures 3.6c and 3.6d are the revealed secrets. Secret 1 can be revealed after overlaying the master key on the upper portion of common share and similarly the lower portion reveals the secret 2.

Disadvantage of contrast based joint visual cryptography is that once the share 1 has black pixels than that space can no longer be used for inserting any more secrets. This issue makes space management quite tough. Hence these schemes were replaced by modern visual cryptography.

CHAPTER 4

PROPOSED METHODOLOGY

After discussing the various schemes present in literature, there is a need to develop the technique which has nothing to do with sending multiple shares for a secret image. Proposed approach saves resources like bandwidth, memory space for storage, eliminate cover images and most importantly provides lossless image encryption. It is designed from ground up and can perform optimally to ensure the best image quality and far better security by making use of two keys. The proposed algorithm can be extended to more advanced form also, thereby allowing users to control additional parameters like image plane extraction and introduction to the third type of key in addition to the already present two keys.

4.1 KNIGHT'S TOUR PROBLEM

Knight's Tour Problem (KTP) is considered to be one of the oldest problems in chess and computer algorithms. The puzzle is all about moving the knight thoughout the chessboard of dimension (8 x 8) in 63 moves covering each square only single time. If starting from a sqaure, the knight approaches the same place as beginning after traversing through entire chessboard, the path traversed is called knight's closed tour otherwise it is open tour.

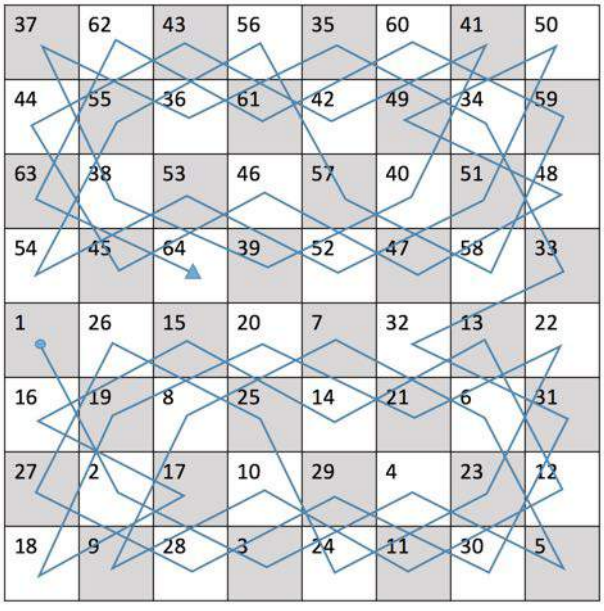


Figure 4.1: Knight's open tour on a chessboard (8×8)

Figure 4.1 shows the valid moves for the solution of knight's tour problem in a typical chessboard. Each square is marked with the positioning order of knight on chessboard. Starting from place indicated as 1 to moving the square marked with value 64. This problem is solved with 63 moves. Here one square is visited only one time.

4.2 EULER'S SOLUTION

According to Leonhard Euler [83], knight's tour problem, as mention in section 4.1, on a chessboard of dimension 8×8 can be solved if the following conditions are fulfilled:

- The values present in squares, on both the sides of the line joining the centres between them, should have the difference of 32.
- Half of the total values present should lie on one side of the chessboard and rest on the other side.

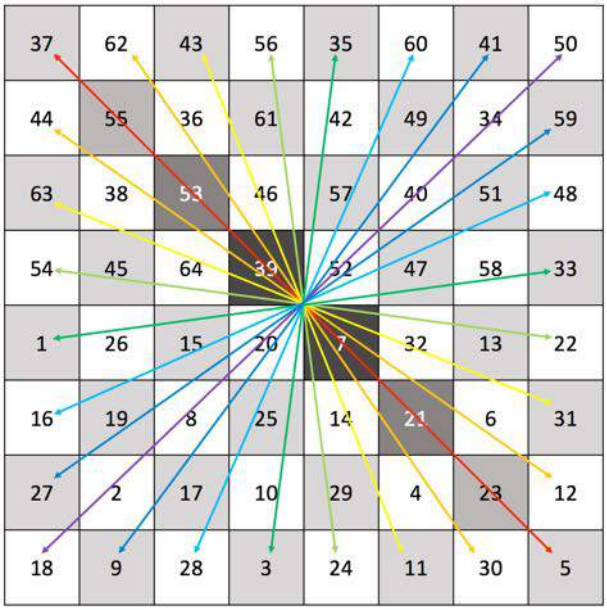


Figure 4.2: Euler's solution to an Open Knight's Tour

Figure 4.2 verifies the Euler's conditions for knight's tour. It can be seen that the lines joining the square has a difference value of 32 for the exactly opposite squares.

4.3 WARNSDORF'S RULE AND SCHWENK'S RULE

Warnsdorf's rule [84] also known as 'heuristic' approach, is a method of finding a knight's tour. According to this rule, the knight is moved forward in such a way that minimum number of paths are possible in the forward direction. While calculating the forward paths, prevention must be there to avoid revisiting the same square.

There are few variations of this knight's tour problem which involve in addition to the typical chessboards of regular size i.e., 8×8, irregular (non-rectangular) boards of dimension $m \times n$. Schwenk [85] proved a theorem to show the possibilities of knight's tour only on certain dimensional chessboards ($m \times n \; for \; all \; m \leq n$) until or unless one of the following conditions are verified.

- m and n can acquire odd face value;
- $m = 1, 2, or \; 4$;
- $m = 3$ and $n = 4, 6 \; or \; 8$.

Using these rules, approximate number of trials possible are 1.305×10^{35} [77] for an 8×8 chessboard. For this reasons, this key space increases drastically with the size of the chessboard over which the tour is made.

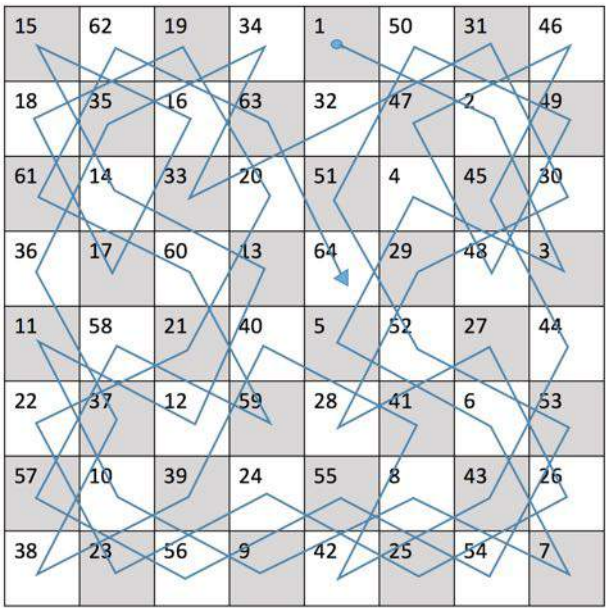


Figure 4.3: Another Open Knight's Tour according to Warnsdorf's and Schwenk's Rule

This approach is very helpful while scrambling the data, which forms the first part of the designed methodogy. The checkerboard box numbers actually indicate the sequence followed by the knight and once the solution is found every stage where Knight has moved is saved. These saved states basically are used to place the pixels from original position to final positions in the randomized image.

4.4 PROPOSED APPROACH

Beginning with the block diagram of the proposed approach to have a clear understanding of the working principle. The block diagram presented in the figure 4.4 provides the layout of the designed methodology. Work of each block is discussed below in detail.

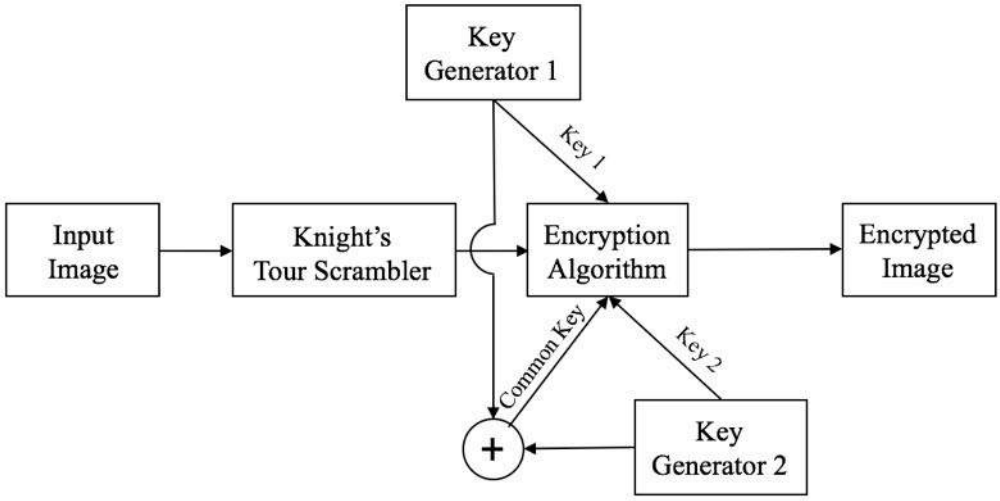


Figure 4.4: Block diagram of proposed approach

a) Input Image: Input Image is the actual digital image data that needs to be encrypted. This image can be grayscale or RGB Coloured. In case the image is RGB coloured then it requires that each of the colour plane i.e., Red, Green and Blue, should be processed individually and then recombined back to obtain the encrypted image.

b) Knight's Tour Scrambler: This block provides the first layer of image encryption. knight's tour scrambler is used to initally scramble or randomize the image data to some extent. This block requires the knight's tour as explained in the section 4.1. User has the flexibility to choose any knight's tour method to randomize the data at pixel level.

Figure 4.5: 'Lenna' before and after Knight's Tour Scrambler after one iteration

Figure 4.5 shows the result of application of knights tour scrambler on the input image. The result can be further enhanced if the scrambling is done iteratively.

c) Key Generator: In the proposed appraoch, two keys are required of variable length. They can be as long as possible and can have only positive integer values. However, the point to be taken into consideration is that both the keys should have same length. Also a common key is used, which is nothing but the Modulo-2 addition of Key 1 and Key 2. A Typical example of the keys can be

Key 1: [10, 20, 30, 40, 50, 12, 15, 24, 25, 30, 12, 24, 25, 15, 20, 60]

Mod-2 Addition or ⊕ Operation

Key 2: [60, 91, 13, 92, 64, 10, 28, 55, 96, 97, 16, 98, 96, 49, 81, 15]

Common Key: [54, 79, 19, 116, 114, 6, 19, 47, 121, 127, 28, 122, 121, 62, 69, 51]

d) Encryption Algorithm: This is the main part of the proposed approach. Encryption process is performed in three parts namely Image Padding, Checkerboard Generation and Common-Key XORing (Optional).

a. **Image Padding:** In encryption algorithm, the key values for both the keys are checked, if they are an integral multiple of the dimensions of the image to be encrypted. For example, at the beginning, key1 value is 10 and key2 value is 60. Now, the image is checked for dimensions. If the vertical length is divisible by key1 value, there is no need of padding zeros vertical. Similarly for the horizontal axis, the length is checked and padding is done, if necessary. Let the dimensions of the image be 600×600 pixels and the key1 value be 50 while key2 value be 64. Here, vertical length is divisible exactly by key1 value i.e., 600 / 50 = 12; therefore there is no need of padding extra zeros on vertical axis. While the key2 value is 64, which does not divide the horizontal length completely, i.e., 600/64 = 9.375, hence zeros are required to be padded along the horizontal axis only. The number of zeros to be padded along any required axis can be found by:

$$[KeyValue - Mod(DimLen, KeyValue)]$$

where, DimLen is the length of the dimension of vertical and horizontal axis of the image and KeyValue is the value of key1 or key2, Mod(DimLen, KeyValue) gives the remainder of the division among DimLen and KeyValue. So, for the KeyValue

of 64, number of zeros to be padded along horizontal axis will be (64 - 24) = 40, which gives new dimension of 600 + 40 = 640 that is completely divisible by 64. One might wonder that what can be the point of zero padding for completely divisible length with KeyValue, the answer being, that is done to make Checkerboard possible.

b. **Checkerboard Generation:** The Dimensions of the image are checked, if they are exactly divisible by the KeyValue (as mentioned earlier). After the verification is over, a checkerboard with boxes exactly the size obtained after division of Image Dimension with KeyValue are made. Key1 is applied along vertical axis and Key2 along horizontal. Thus, a matrix of boxes are formed, as shown in figure 4.6, where KeyValue1 and KeyValue2 are elements of Key1 and Key2 respectively.

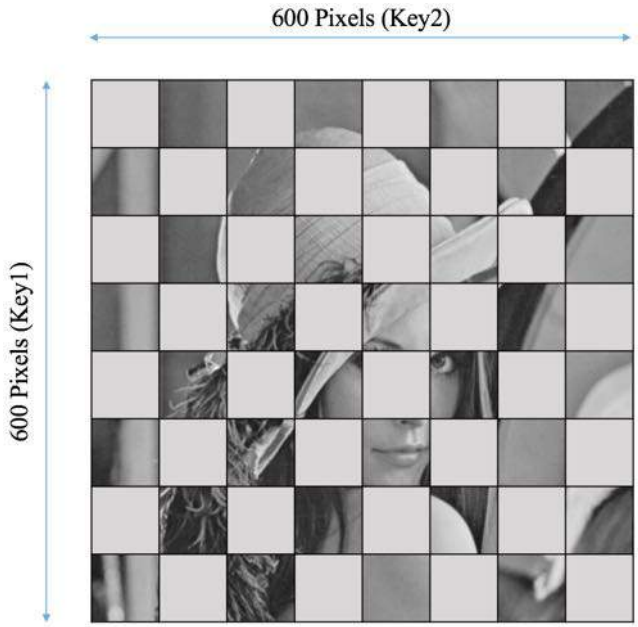


Figure 4.6: Checkerboard on image of 'Lenna' with KeyValue1 = KeyValue2 = 8

It shows that if the KeyValue = 8 in both Key1 and Key2, the image is divided into 8 boxes along vertical and 8 boxes on horizontal axis. Each box is of dimensions 75×75 (as $600/8 = 75$), where the image's actual size being 600×600 pixels. Here one can see that Knight's Tour scrambler is not used.

The shaded boxes can be viewed as an alternate boxes as shown in the Figure 4.6 are flipped horizontally and vertically to obtain an inverted mirror like image of the actual one. This can be seen in figure 4.7 as:

Figure 4.7: Checkerboard image with alternate position boxes flipped

It clearly shows the division of image being done according to the KeyValue and is flipped. Once a KeyValue is applied, the next KeyValue is used and this process continues till the whole Key1 and Key2 are used. Shown in figure 4.8, is an image with the result of recursive flipping done using both the keys on 'Lenna' image.

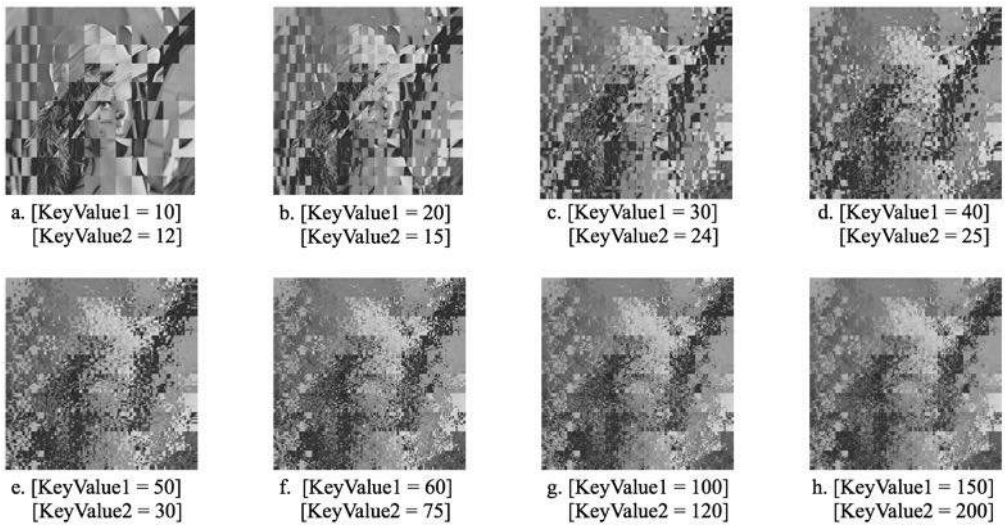


Figure 4.8: Various obtained images after application of Keys

Figure 4.8 shows the result of encryption process after applying the Key1 = [10, 20, 30, 40, 50, 60, 100, 150] and Key2 = [12, 25, 24, 25, 30, 75, 120, 200] each according to the corresponding values. These values are applied one after the other or in continuous order.

c. **Common-Key XORing:** This is an Optional step. It is important to discuss that this step can be applied after each time the Checkerboard is generated i.e., it was

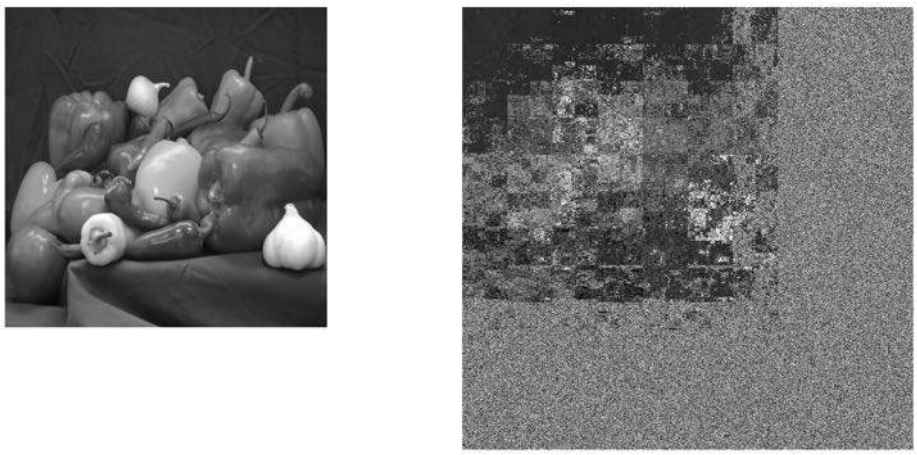
intentionally not shown in checkerboard generation concept while it can actually be used along with the second step side-by-side. At first, the common key is generated as defined earlier by Modulo-2 addition or Bit-wise XORing the Key1 and Key2 values correspondingly. Once the common key is obtained, it is simply XORed or Modulo-2 added to the actual pixel values of the image. For example, shown in figure 4.9b, is the pixel values of image after the checkerboard generation of figure 4.9a and it is XORed Bit-wise with the common key in figure 4.9c so as disguise the actual as much as possible. This step can repeated each time the checkerboard is generated and with the same KeyValues being used for common key.

Figure 4.9: Application of complete algorithm on ‘Peppers’ Image

d. **Irregular Key Case:** For the case if the applied keys i.e., Key1 and Key2 does not divide exactly the dimensions of the image to be encrypted, in that case, as mentioned earlier, zero padding will be done according to the KeyValues. For Key1 the padding will be done along vertical direction while for the case of Key2 along horizontal direction. However, it is important to mention here that the dimensional size of encrypted image thus obtained will be more then the original image.

In other words, the final resultant image which is in encrypted form is bigger in dimensions to the original image. Also instead of zero padding the original image, one can fill the necessary padding with random data ranging the dynamic range of the image i.e., 0 – 255. This will appear as random noise in the encrypted image and confuses the undesired recipient even more.

Figure 4.10b shows the irregular key case, in which the KeyValues are not an integer multiple of dimensional size of the image in figure 4.10a. There will be zero padding required at first to allow the key to perform the defined operation.



a. b.

Figure 4.10: Original image and its encrypted image as a result of irregular key.

Thus, a modified image encryption scheme have been developed that meets the pixel expansion problem, eliminates the contrast loss, efficiently manage the storage space as single image has to be stored, and is a lossless scheme. Hence, all the objectives discussed in chapter 2 have been achieved.

CHAPTER 5

RESULTS AND DISCUSSION

By working on the proposed approach, following results have been computed. Starting with the irregular key case, in which the padding is required, when the KeyValues are not the integral factors of the image dimensions.

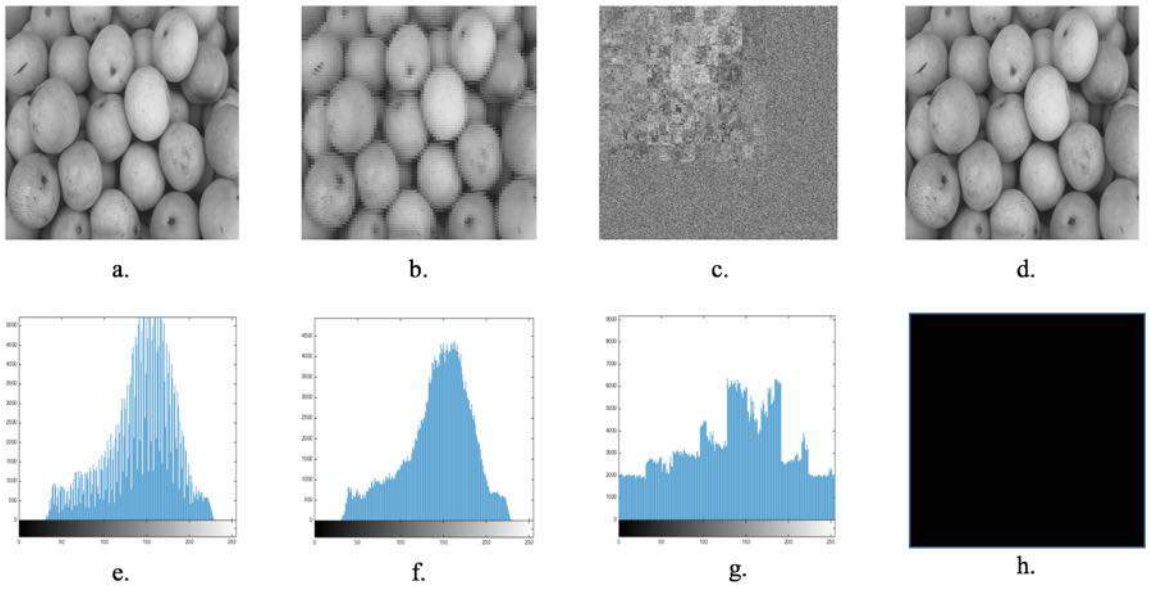


Figure 5.1: Application of proposed encryption approach on 'Pears' Image

Figure 5.1a shows the actual image to be encrypted. Figure 5.1b shows the resultant image obtained after the Knight's Tour Scrambler. Figure 5.1c shows the encrypted image as the result of proposed approach. Figure 5.1d represents the original decrypted image which is same as figure 5.1a. Figure 5.1 e, f and g shows the histogram of original image, Knight's Tour Scrambler and encrypted image respectively. Figure 5.1h shows that decrypted image in figure 5.1d is same as original image in figure 5.1a as there exist no difference in them as shown in figure 5.1h. So, the proposed scheme is a lossless encryption technique.

For the colored image to be used, the process is same as for grayscale images only difference is that RGB colored image is treated by working on its individual planes one-by-one.

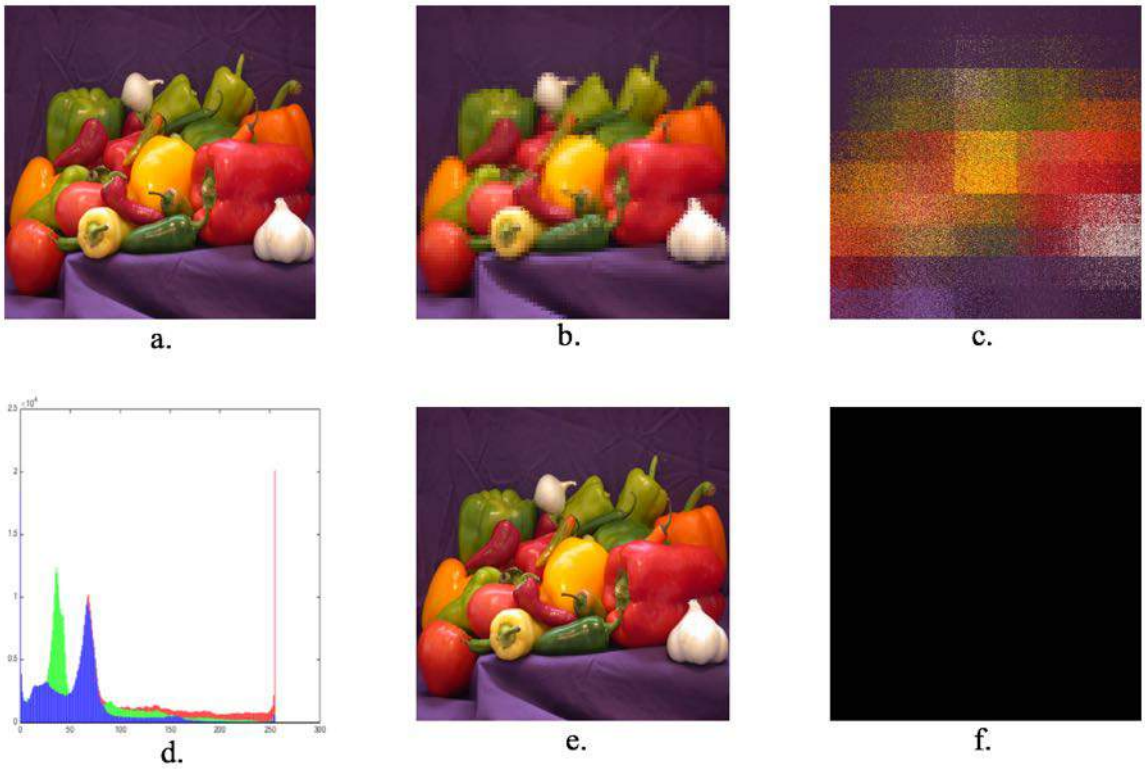


Figure 5.2: Proposed Approach on Colored image ‘Peppers’

The above figure 5.2a shows the original image, figure 5.2b shows the Knight’s tour scrambler applied on figure 5.2a, figure 5.2c depicts the encrypted image resulting by the application of proposed technique, figure 5.2d shows the RGB colored Histogram of both the original and decrypted image and figure 5.2e shows the obtained image after decryption, which is same as the original image. Lastly, figure 5.2f shows the difference between actual image and encrypted image, which shows that there is no error in decryption process and hence the scheme is lossless.

5.1 PERFORMANCE ANALYSIS OF PROPOSED APPROACH

This section provides the details regarding performance of the proposed approach which is discussed is chapter 4.

5.1.1 Correlation Coefficient

Correlation coefficient determines the degree of similarity among two variables. It can be one of the strongest parameters to judge the quality of encryption algorithm. The scheme can be marked as excellent if the image encrypted by it appears totally random i.e., there

exists nothing common between it and original image. In terms of correlation coefficient, the value of this coefficient must lie closer to zero.

$$Correlation\ Coefficient\ (\rho) = \begin{cases} 1(full) \\ 0(zero) \\ -1(anti) \end{cases}$$

If the correlation coefficient (ρ) is unity, the system is a failure. It cannot provide encryption, as original image and resultant image are both same. If the value of ρ is equal to zero (0), there exists nothing common in between the output image and original one. However, $\rho = -1$ means the encrypted image is negative of the original. Hence, for best results, the value of correlation coefficient must lie near to zero (0).

Let α and β represents the original image and its encrypted version respectively. Mathematically, correlation coefficient can be given as:

$$C.C = \frac{Cov(\alpha,\beta)}{\sigma_\alpha \times \sigma_\beta} \quad (5.1)$$

where, $Cov(\alpha, \beta)$ represents the covariance among the actual and encrypted, σ represents the Standard deviation of respective image.

$$\sigma_\alpha = \sqrt{VAR(\alpha)} \quad (5.2)$$

$$\sigma_\beta = \sqrt{VAR(\beta)} \quad (5.2)$$

where, VAR denotes the Variance of the respective image.

$$VAR(\alpha) = \frac{1}{N}\sum_{i=1}^{N}(\alpha_i - E(\alpha))^2 \quad (5.3)$$

N is the total number of pixels in an image, i.e., $N = Height \times Width$ of the image, while E denotes the $Expected\ or\ mean$ value of the image.

$$Cov(\alpha,\beta) = \frac{1}{N}\sum_{i=1}^{N}(\alpha_i - E(\alpha))(\beta_i - E(\beta)) \quad (5.4)$$

5.1.2 Time Consumption

Time taken for the complete encryption process and decryption process can be obtained by recording different iterations of the algorithm. Time consumption plays a major role in quality assessment of an image encryption algorithm. Lesser the time taken to encrypt and decrypt images, better is the encryption algorithm. Also, the encryption time is related to the hacking time. More is the encryption time, lesser is the time taken by the hacker to crack the system.

Thus, the readings for performance analysis is shown in table 5.1.

Table 5.1: Performance results of proposed scheme on various data sets.

Data Set	Variance(β)	SD(σ)	Covariance(α, β)	CC(ρ)
Chessboard	0.2500	0.5000	0.0011	0.0045
Pyramid	0.2500	0.5000	0.0005	0.002
Model	0.0490	0.2213	0.0037	0.0789
Gamer	0.0469	0.2165	0.0237	0.583
Cameraman	0.0590	0.2430	0.0332	0.5618
Airplanes	0.0154	0.1240	0.0053	0.3447
Fruits	0.0383	0.1956	0.0224	0.5854
Hills	0.1060	0.3256	0.0830	0.783
Baboon	0.0262	0.1618	0.0071	0.2714
Lenna	0.0351	0.1874	0.0110	0.3131

Table 5.1 encloses results of proposed approach after its application on ten data sets. The graphs of these results are shown as:

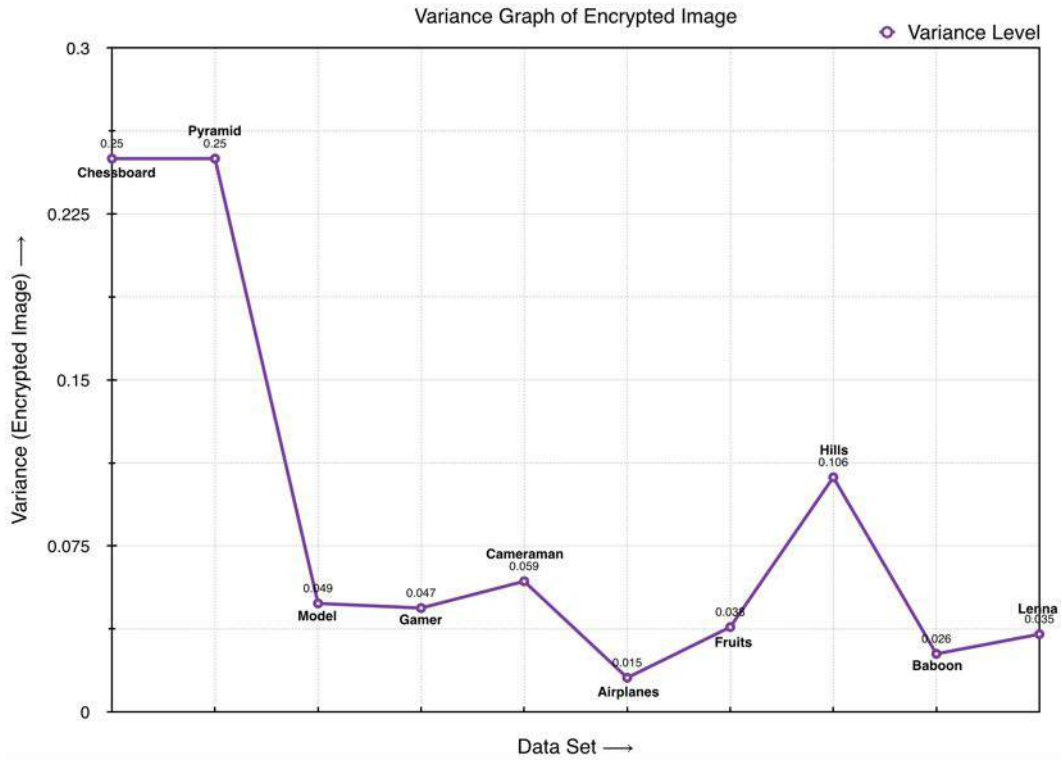


Figure 5.3: Variance curve for data set in table 5.1

Figure 5.3 shows the variation in the variance of encrypted data sets. It depicts the non-linear increments and decrements in the variance values. Highest variance is achieved by Chessboard and Pyramid data sets while the lowest is obtained by Airplanes image.

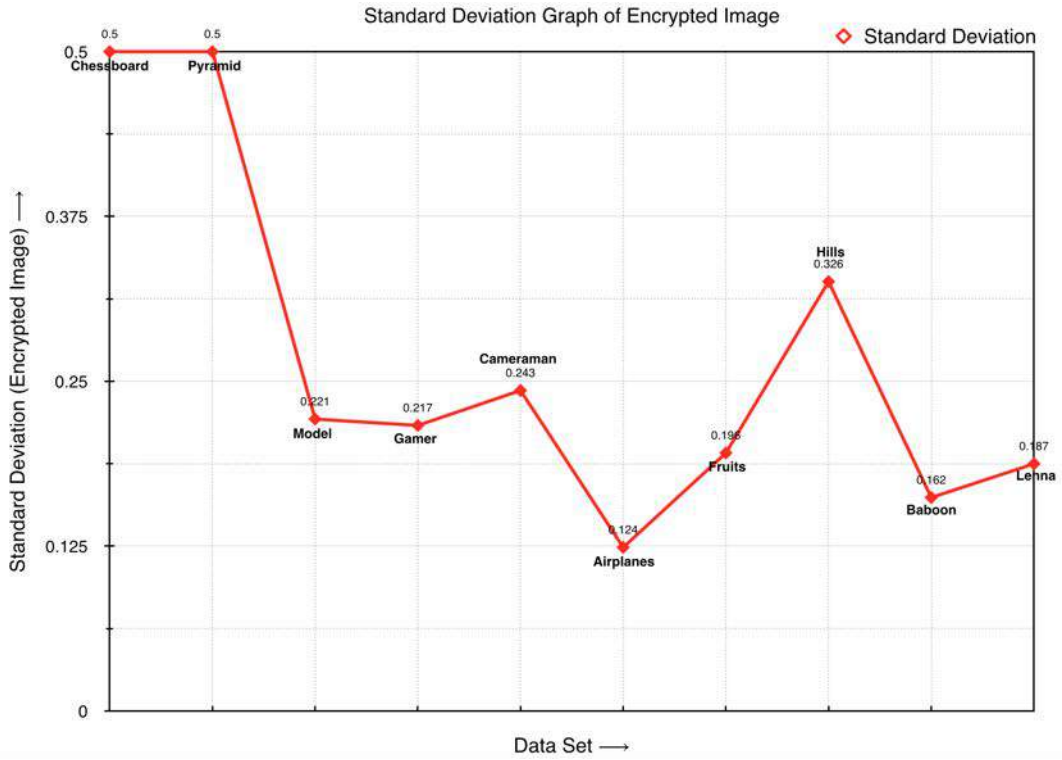


Figure 5.4: Standard deviation curve for data set in table 5.1

Figure 5.4 represents the variation in Standard deviation for the data sets. Since Standard deviation is obtained from variance of the encrypted data set, therefore both the graphs have symmetry between them.

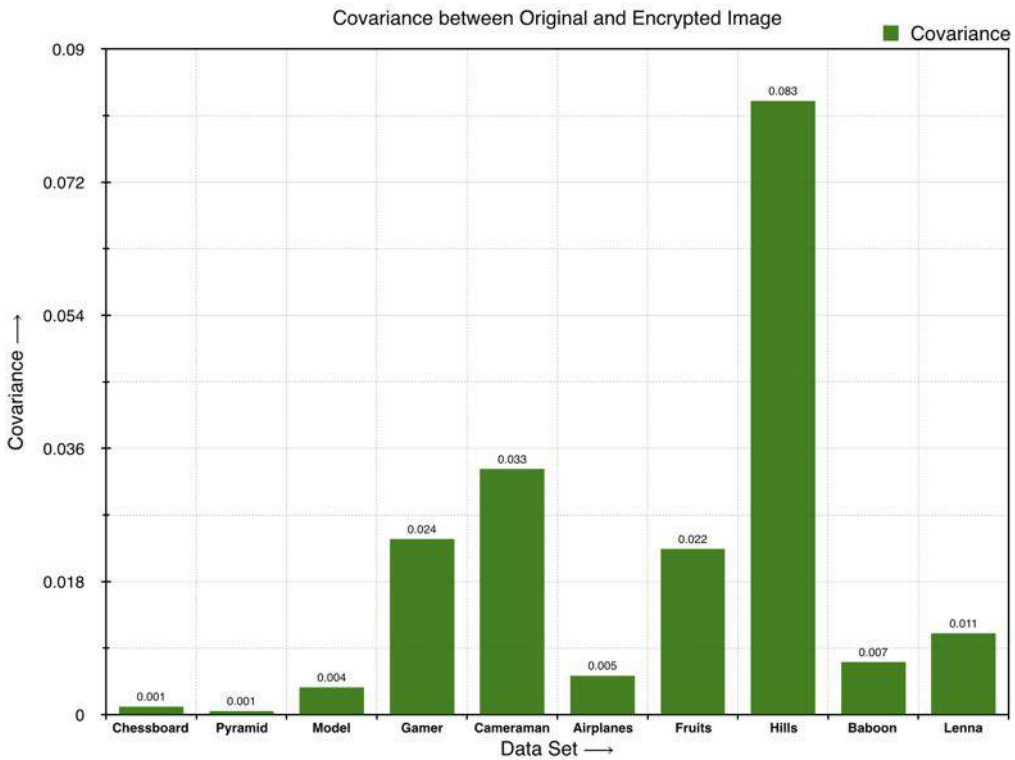


Figure 5.5: Covariance chart for data set from table 5.1

The figure 5.5 shows the Covariance levels for the data set. These variations occur due to the difference in number of pixels that lie closer to either low pixel value or extremely high.

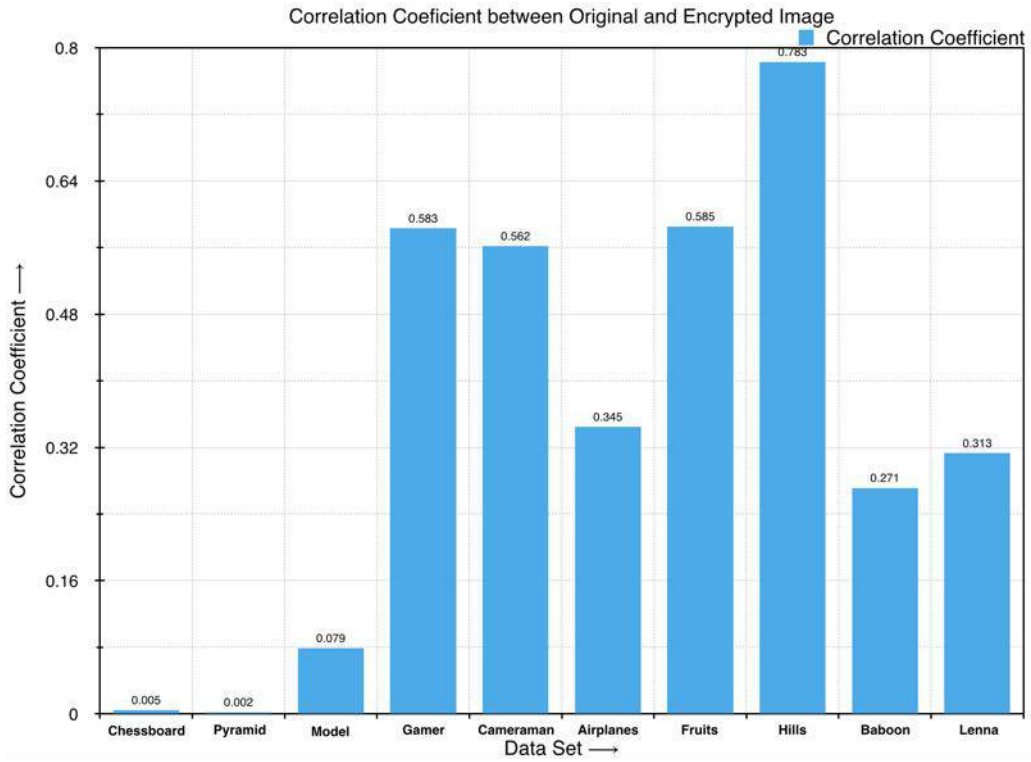


Figure 5.6: Correlation coefficient graph of different encrypted images

Correlation coefficient varies per image. The results shown in figure 5.6 verifies the fact that if the images contain large area of black or white pixels, the correlation may give false positive. Shown below in figure 5.7, is hills image and its encrypted image, which shows false positive for correlation.

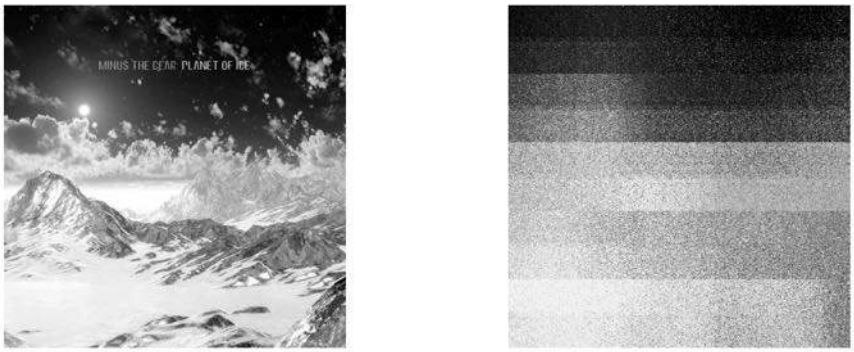


Figure 5.7: Hills image on left and its encrypted image on right side.

This is clear from figure 5.7 that false positive in correlation coefficient can occur if the majority of pixels lie near the extremities. This encrypted hills image had shown a correlation coefficient value of 0.783, which may give rise to the conclusion that the original image can be easily detectable from encrypted image. However, the practical results are totally justfied to the proposed algorithm.

Encryption and decryption time increases according to the size of the image data. Larger or heavier the file is, more it will take time to encrypt.

Table 5.2: Encryption and decryption time for proposed work on various data sets

Data Set	File Size (KB)	Enc. Time (sec)	Dec. Time (sec)
Chessboard	1	0.80508	0.73551
Pyramid	4	0.90006	0.74450
Model	67	0.91819	0.73162
Gamer	98	0.90658	0.73174
Cameraman	140	0.92480	0.71413
Airplanes	156	0.90641	0.71901
Fruits	183	0.91687	0.76193
Hills	215	0.94015	0.74020
Baboon	258	0.90389	0.74719
Lenna	474	0.89407	0.76106

Table 5.2 includes the variation of encryption and decryption time according to the file size, while its graph is shown in figure 5.8.

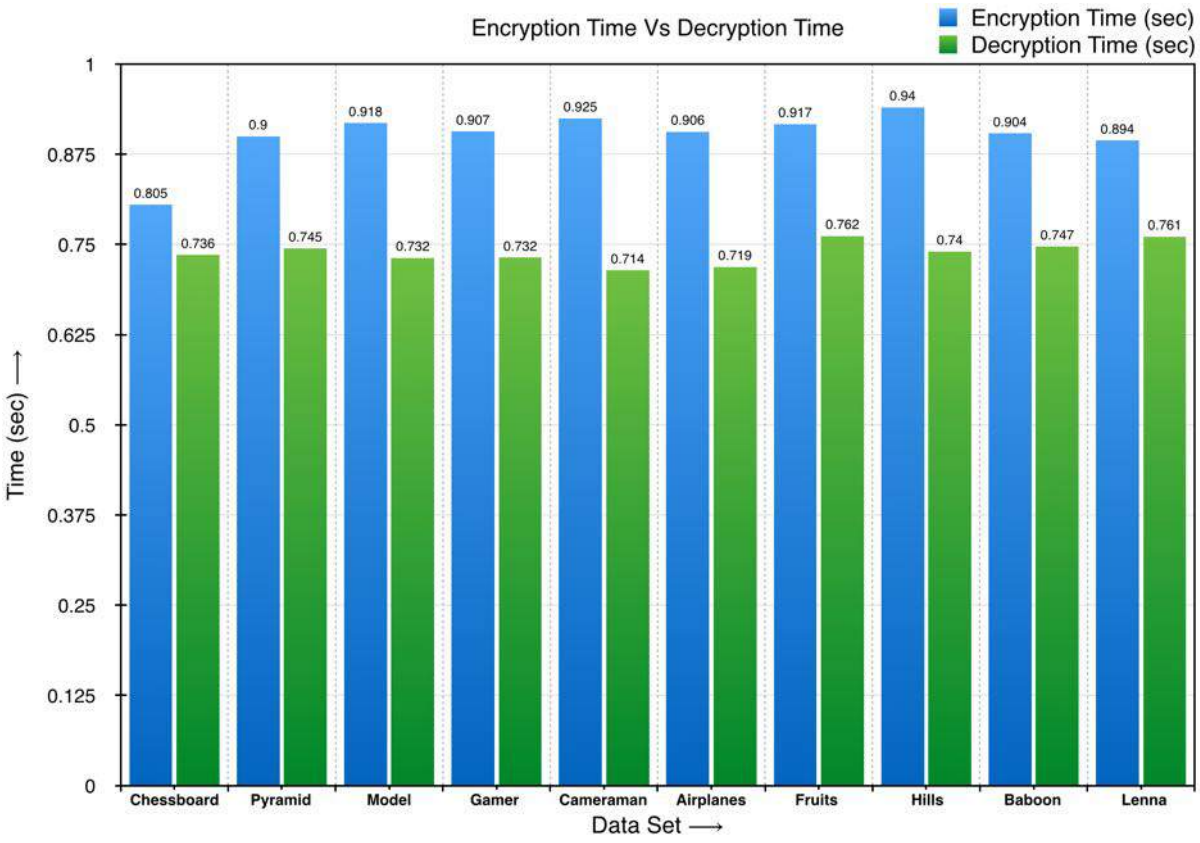


Figure 5.8: Graph depicting encryption and decryption time from table 5.2

5.1.3 File Size Comparison

With encryption process, the size of file is also increased than the original file size. Table 5.3 shows the increase in file size after encryption process.

Table 5.3: File size comparison between original and encrypted file for proposed work

Data Set	Input File Size (KB)	Encrypted File Size (KB)
Chessboard	1	79
Pyramid	4	87
Model	67	171
Gamer	98	229
Cameraman	140	307
Airplanes	156	285
Fruits	183	325
Hills	215	338
Baboon	258	341
Lenna	474	617

This table can be visualized by ploting a graph of table 5.3 values, which can be seen in figure 5.9

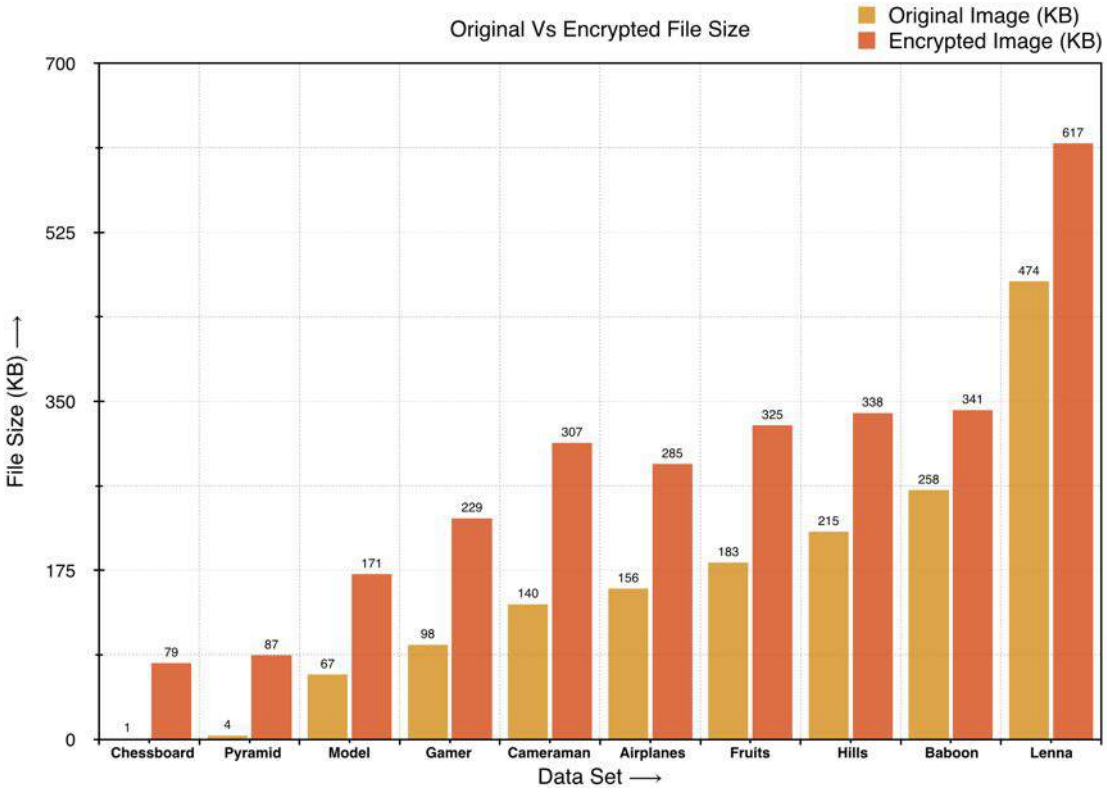


Figure 5.9: Original file size vs encrypted file size chart

5.2 COMPARISON WITH EXISTING SCHEMES

This section compares the proposed approach with other already existing schemes in literature like AES, DES and Triple-DES (TDES).

5.2.1 Time Comparison

This section compares the encryption and decryption time for AES, DES, TDES and proposed approach. Shown in table 5.4, are the values of encryption time in seconds among different schemes.

Table 5.4: Encryption time comparison among different schemes (time in seconds)

File Size (KB)	DES	TDES	AES	Proposed
1	0.40242	0.98336	0.82231	0.80508
4	0.41190	0.99784	0.90912	0.90006
67	0.46614	1.01720	0.92415	0.91819
98	0.50019	1.08931	0.93631	0.90658
140	0.51334	1.10031	0.91387	0.92480
156	0.53045	1.50382	0.96211	0.90641
183	0.56167	1.98931	0.96725	0.91687
215	0.55932	2.00157	0.99711	0.94015
258	0.56382	2.19882	1.00211	0.90389
474	0.61837	2.26394	1.01892	0.89407

From table 5.4, it is clear that the most time consuming approach is Triple-DES or TDES, while the least time consuming is DES. However, DES suffers a lot from security issues. The small key space offers less security. TDES scheme is equivalent to 3 rounds of DES and hence, the key space is undoubtedly large enough to provide better security model than DES. But this security comes with the compromise of encryption time.

Most recent standard AES is more secure and more faster in operation than TDES. AES is nearly twice the time faster than TDES but it is slow as compared to DES. The security benefits of AES overcome the large encyption time drawback it posses. The proposed approach has faster encryption rate than TDES. It can be seen in figure 5.10 that the proposed approach is faster than AES in some cases.

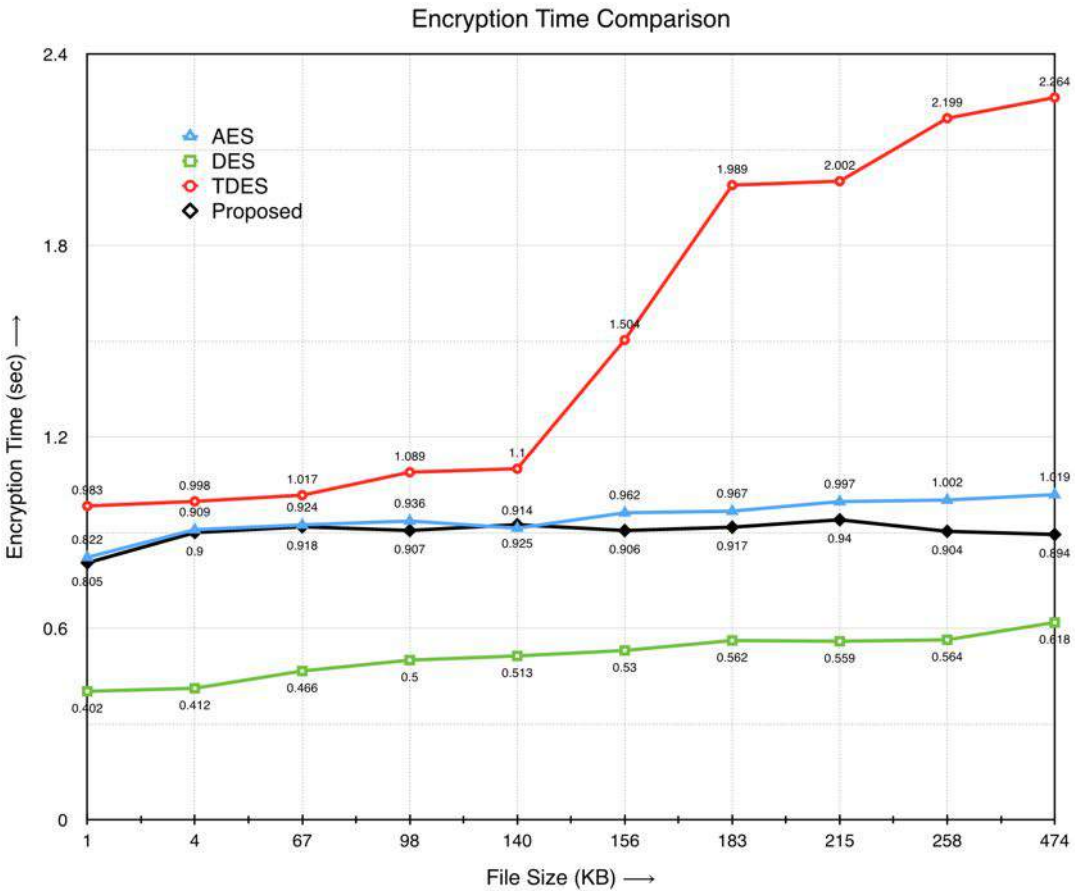


Figure 5.10: Encryption time comparison between various schemes.

Similarly, the decryption time has been evaluated and the results have be concluded in table 5.5 as shown below:

Table 5.5: Decryption time comparison among various schemes (time in seconds)

File Size (KB)	DES	TDES	AES	Proposed
1	0.61721	0.91758	0.71087	0.73551
4	0.76610	0.94412	0.73078	0.7445
67	0.64934	0.92834	0.79118	0.73162
98	0.78792	0.96261	0.78892	0.73174
140	0.79762	0.99172	0.8011	0.71413
156	0.83445	1.21881	0.81191	0.71901
183	0.82882	1.20366	0.84173	0.76193
215	0.81721	1.4662	0.85881	0.7402
258	0.83398	1.49001	0.89161	0.74719
474	0.85877	1.64221	0.88786	0.76106

The visual representation of table 5.5 is shown in figure 5.11 which is shown as

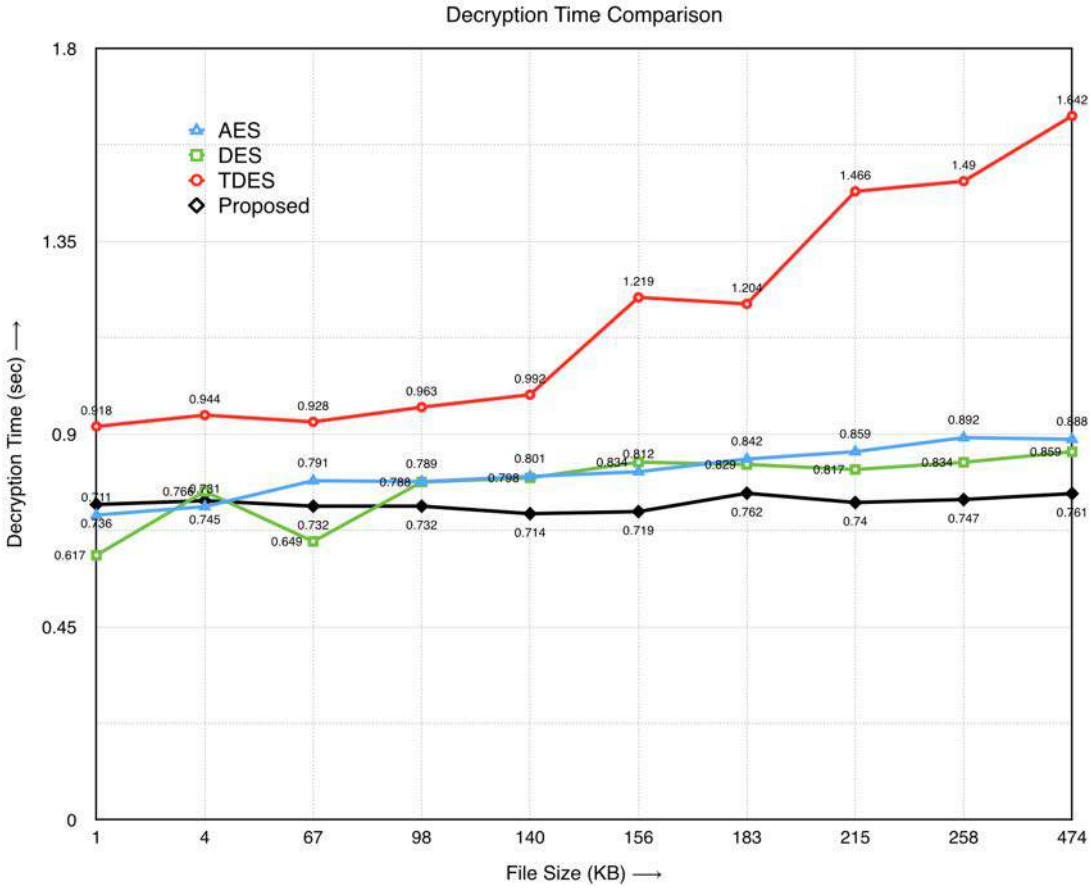


Figure 5.11: Decryption time comparison between various schemes.

From figure 5.11 it can be seen that the proposed approach performs with consistancy. The rate of decryption of data is well maintained in limits.

5.2.2 Throughput Calculation

The general formula for throughput calculation for cryptography is given as:

$$Throughput = \frac{Total\ Plain\ text}{Total\ Encryption/Decryption\ Time}$$

Selecting encryption or decryption at denominator can result in corresponding throughput.

$$Total\ Plain\ text = \sum 1 + 4 + 67 + 98 + 140 + 156 + 183 + 215 + 258 + 474$$
$$= 1596\ KB$$

a. Throughput calculation for DES

Since total file size will be same for all the participating schemes, hence only total encryption time is required for calculations.

$$Total\ Encryption\ Time = \sum 0.402 + 0.411 + 0.466 + 0.500 + 0.513 + 0.530 + 0.561 + 0.559 + 0.563 + 0.618 = 5.127\ sec$$

$$Encryption\ Thoughput = \frac{1596\ KB}{5.127} = 311.29\ KB/s$$

$$Total\ Decryption\ Time = \sum 0.617 + 0.766 + 0.649 + 0.787 + 0.797 + 0.834 + 0.828 + 0.817 + 0.833 + 0.858 = 7.791\ sec$$

$$Decryption\ Thoughput = \frac{1596\ KB}{7.791} = 204.85\ KB/s$$

b. Throughput calculation for TDES

Again, only requirement is for encryption or decryption time. File size will be same.

$$Total\ Encryption\ Time = \sum 0.983 + 0.997 + 1.017 + 1.089 + 1.100 + 1.503 + 1.989 + 2.001 + 2.198 + 2.263 = 15.145\ sec$$

$$Encryption\ Thoughput = \frac{1596\ KB}{15.145} = 105.38\ KB/s$$

$$Total\ Decryption\ Time = \sum 0.917 + 0.944 + 0.928 + 0.962 + 0.991 + 1.218 + 1.203 + 1.466 + 1.490 + 1.642 = 11.765\ sec$$

$$Decryption\ Thoughput = \frac{1596\ KB}{11.765} = 135.65\ KB/s$$

c. Throughput calculation for AES

Following the similar pattern as of DES and 3DES, we have:

$$Total\ Encryption\ Time = \sum 0.822 + 0.909 + 0.924 + 0.936 + 0.913 + 0.962 + 0.967 + 0.997 + 1.002 + 1.018 = 9.453\ sec$$

$$Encryption\ Thoughput = \frac{1596\ KB}{9.453} = 168.83\ KB/s$$

$$Total\ Decryption\ Time = \sum 0.710 + 0.730 + 0.791 + 0.788 + 0.801 + 0.811 + 0.841 + 0.858 + 0.891 + 0.887 = 8.114\ sec$$

$$Decryption\ Thoughput = \frac{1596\ KB}{8.114} = 196.69\ KB/s$$

d. Throughput calculation for Proposed Approach

Calculating the encryption and decryption time first, we get

$$Total\ Encryption\ Time = \sum 0.805 + 0.900 + 0.918 + 0.906 + 0.924 + 0.906 + 0.916 + 0.940 + 0.903 + 0.894 = 9.016\ sec$$

$$Encryption\ Thoughput = \frac{1596\ KB}{9.016} = 177.01\ KB/s$$

$$Total\ Decryption\ Time = \sum 0.735 + 0.744 + 0.731 + 0.735 + 0.714 + 0.719 + 0.761 + 0.740 + 0.747 + 0.761 = 7.386\ sec$$

$$Decryption\ Thoughput = \frac{1596\ KB}{7.386} = 216.08\ KB/s$$

Throughput calculated for these schemes can be presented visually. Figure 5.12 shows the encryption throughout comparison between these schemes while figure 5.13 represents the decryption throughput.

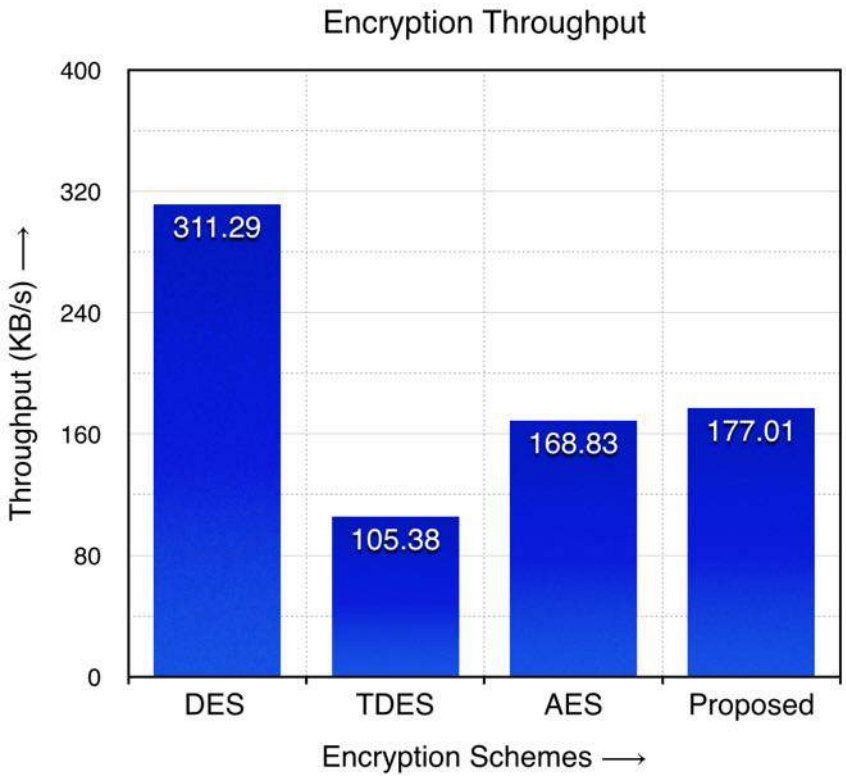


Figure 5.12: Encryption throughput comparison chart

From figure 5.12, it is clear that DES offers the maximum throughput among these schemes. Also, TDES offers the lowest throughput, while the proposed approach offers higher throughput than both TDES and AES schemes.

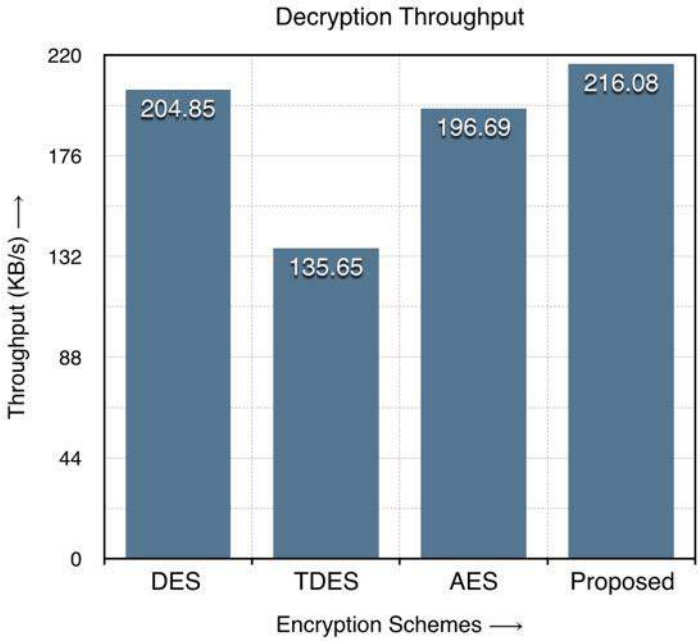


Figure 5.13: Decryption throughput comparison chart

From figure 5.13, it is concluded that the proposed approach offers maximum throughput in decryption scenario. This is followed by DES and then AES scheme while TDES lags behind performance due to its lengthy encryption process.

Hence, it has been concluded that the proposed approach is a lossless technique. The decrypted image is same as the original image. This scheme also tends to make the correlation coefficient of encrypted image towards zero (0), which means the encrypted image has no similarity with actual image. Also, the file size ratio is optimum, which means the encrypted file size is well within the limits.

Encryption time of proposed approach is comparable to AES scheme. It is more than the DES scheme but very less than the TDES. Similarly, decryption time is comparable to AES and DES schemes for small file sizes while it is less than both for large file sizes. However, decryption time of proposed scheme is far less than TDES scheme for any file size.

Throughput for encryption process of proposed scheme is less than DES and is comparable to AES scheme, while it is more than the TDES. However, decryption throughput of proposed scheme is highest among DES, TDES and AES.

Hence, all the objectives mentioned in chapter 2 have been achieved successfully.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

From the discussed results in chapter 5, it is worth mentioning that the proposed methodology delivers completely lossless results, which is one of the signifance of this approach. This also maintains the data size of image on storage. Also there is no need to send multiple share images, that clearly shows no pixel expansion is there. Finally the algorithm requires only two keys. Also the most important aspect from designer's point of view is that the encryption unit can act as decryption unit and vice-versa without any need of further modifications. This is possible due to the division algorithm described earlier.

The concept of this proposed approach is clear that whenever the user does not want to use cover images for data hiding or for image encryption, at those times this approach comes in handy. Key generation is far more easily utilized in here. For realtime scenerio like in wireless image tranfers, or online activities which takes into account the tranfer of images or any visual data.

Another important aspect of this Encryption Algorithm is that the same encoder can be used as decoder without any change in the programming. So, the need of separately designing the decoder/decryption unit is absent. Thus, same encoder/encryption unit can work as decryption unit thereby reducing the overall system complexity.

The most important aspect is that a single image is sent over the medium and all the essential information that needs to be sent can be extracted from the same without transmitting the multiple shares, hence this approach eliminates the need of multiple shares, which can save necessary bandwidth or resources for other uses.

REFERENCES

[1] S. Haykin, *Digital Communications*. 2nd ed. John Wiley and Sons, 1998.

[2] S. Benedetto and E. Biglieri, *Principles of Digital Transmission: With Wireless Applications*. 2nd ed. Springer International Publishing, 2008.

[3] J. G. Proakis, *Digital Communications*. 4th ed. McGraw-Hill Publications, 2000.

[4] O. Goldreich, *Foundations of Cryptography: Basic Techniques*. 1st ed. Cambridge University Press, 2004.

[5] D. Kahn, *The Codebreakers: The story of secret writing*. 2nd ed. Scribners, 1996.

[6] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. 3rd ed. CRC Press, 1997.

[7] D. R. Stinson, Chapman, and Hall, *Cryptography: Theory and Practice*. 2nd ed. CRC Press, 2005.

[8] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 7, pp. 656-715, Jul. 1948.

[9] J. Savard, *The ideal cipher: Kerckhoff's design goals for ciphers*. 1st ed. McGraw-Hill Publications, 1976.

[10] FIPS-46, "Data Encryption Standard," *National Institute of Standards and Technology*, Jan. 1979.

[11] FIPS-197, "Advanced Encryption Standard," *National Institute of Standards and Technology*, Nov. 2001.

[12] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, "The RC6 block cipher," *MIT Lab. for Computer Science*, Aug. 1998.

[13] R. L. Rivest, "The RC4 encryption algorithm", *RSA Security Inc.*, Mar. 1992.

[14] FIPS-186, "Digital Signature Standard," *National Institute of Standards and Technology*, Jun. 2009.

[15] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 7, pp. 644-654, May 1976.

[16] FIPS-180-4, "Secure Hash Standard," *National Institute of Standards and Technology*, Mar. 2012.

[17] W. Stallings, *Cryptography and Network Security, Principles and Practice*. 4th ed. Pearson Publications, 2014.

[18] A. Shamir, "How to share a secret", *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[19] M. Naor and A. Shamir, "Visual cryptography, advances in cryptography: Eurpocrypt '94," *Lecture Notes in Computer Science*, vol. 950, Springer International Publishing, 1994.

[20] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Transactions on Fundamentals*, vol. 82, no. 10, pp. 2172-2177, Oct. 1999.

[21] T. Hofmeister, M. Krause, and H. Simon, "Contrast-optimal k out of n secret sharing schemes in visual cryptography," *Theoretical Computer Science of ACM*, vol. 240, no. 2, pp. 471-485, Jun. 2000.

[22] J. Weir and W. Yan, *Visual cryptography and its applications*. 1st ed. Jonathan Weir and WeiQi Yan and Ventus Publications, 2012.

[23] C. Yang and T. Chen, "Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation," *Elsevier Journal on Pattern Recognition*, vol. 39, no. 7, pp. 1300-1314, Nov. 2006.

[24] J. Erickson, *Hacking: The Art of Exploitation*. 2nd ed. No Starch Press, Feb. 2008.

[25] ECRYPT, "Yearly report on algorithms and keysizes," *EuroCrypt Publications*, Jan. 2007.

[26] N. Koblitz, "Elliptic curve cryptosystems," *American Mathematical Society Journal of Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, Aug. 1987.

[27] M. J. Wiener, "Cryptanalysis of short RSA secret exponents," *IEEE Transactions on Information Theory*, vol. 36, no. 3, pp. 553-558, May 1990.

[28] L. Ham and S. Yang, "ID-Based cryptographic schemes for user identification, digital signature, and key distribution," *IEEE Journal on selected areas in Communications*, vol. 11, no. 5, pp. 757-760, Jun. 1993.

[29] H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, "Dual RSA and its security analysis," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2922-2933, Aug. 2007.

[30] T. S. Halkidis, N. Tsantalis, A. Chatzigeorgiou, and G. Stephanides, “Architectural risk analysis of software systems based on security patterns,” *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 3, pp. 129-142, Jan. 2008.

[31] Q. Gong-bin, J. Qing-feng, and Q. Shui-sheng, “A new image encryption scheme based on DES algorithm and Chua’s circuit,” *IEEE International Workshop on Imaging Systems and Techniques*, pp. 168-172, May 2009.

[32] Z. Yun-peng, Z. Zheng-jun, L. Wei, N. Xuan, C. Shui-ping, and D. Wei-di, “Digital image encryption algorithm based on Chaos and improved DES,” *IEEE International Conference on Systems, Man, and Cybernetics*, pp. 474-479, Oct. 2009.

[33] S. Zhou, Q. Zhang, and X. Wei, “Image encryption algorithm based on DNA sequences for the big image,” *IEEE Conference on Multimedia Information Networking and Security*, pp. 884-888, Nov. 2010.

[34] S. F. Mare, M. Vladutiu, and L. Prodan, “Secret data communication system using Steganography, AES, and RSA,” *IEEE 17th International Symposium for Design and Technology in Electronic Packaging*, pp. 339-344, Jun. 2011.

[35] X. Li, W. Zhang, X. Wang, and M. Li, “Novel convertible authenticated encryption schemes without using Hash functions,” *International Conference on Advanced Communication Control and Computing Technologies*, pp. 504-508, Apr. 2012.

[36] K. Sakiyama, Y. Li, K. Ohta, and M. Iwamoto, “Information theoretic approach to optimal differential fault analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 2, no.8, pp. 109-120, Jul. 2012.

[37] N. Pavan, G. A. Nagarjun, N. Nihaar, G. S. Gaonkar, and P. Sharma, “Image steganography based on Hill cipher with key hiding technique,” *IOSR Journal of Computer Engineering*, vol. 11, no.8, pp. 47-50, Jun. 2013.

[38] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, “(n, k, p)-Gray code for image systems,” *IEEE Transactions on Cybernetics*, vol. 43, no. 2, pp. 515-529, Apr. 2013.

[39] H. Jo, S. Hong, J. Chang, and D. Choi, “Data encryption on GPU for high performance database systems,” *Elsevier Journal on Procedia Computer Science*, vol. 19, no. 9, pp. 147-154, Jun. 2013.

[40] H. Jo, S. Hong, J. Chang, and D. Choi, “Data encryption on GPU for high performance database systems,” *Elsevier Journal on Procedia Computer Science*, vol. 19, no. 9, pp. 147-154, Jun. 2013.

[41] A. Anees, A. M. Siddiqui, and F. Ahmed, “Chaotic substitution for highly autocorrelated data in encryption algorithm,” *Elsevier Journal on Communications in Non-linear Science and Numerical Simulation*, vol. 19, no. 10, pp. 3106-3118, Feb. 2014.

[42] M. Zanin and A. N. Pisarchik, “Gray-code permutation algorithm for high dimensional data encryption,” *Elsevier Journal on Information Sciences*, vol. 270, no. 131, Mar. 2014.

[43] S. Nagaraj, G. S. V. P. Raju, and V. Srinadth, “Data encryption and authentication using public key approach,” *Elsevier Journal on Procedia Computer Science*, vol. 48, no. 4, pp. 126-132, Apr. 2015.

[44] C. Chang and T. X. Yu, “Sharing a secret gray image in multiple images,” *IEEE International Symposium on Cyber Worlds*, pp. 230-237, Nov. 2002.

[45] S. Cimato, R. Prisco, and A. Santis, “Contrast optimal colored visual cryptography schemes,” *IEEE Information Theory Workshop*, pp. 139-142, Apr. 2003.

[46] R. Youmaran, A. Adler, and A. Miri, “An improved visual cryptography scheme for secret hiding,” *IEEE Biennial Symposium on Communications*, vol. 1, no. 2, pp. 340-343, Jun. 2006.

[47] Z. Zhou, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography,” *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2441-2453, Aug. 2006.

[48] Z. Wang and G. R. Arce, “Halftone visual cryptography through Error diffusion,” *IEEE Conference on Image Processing*, pp. 109-112, Oct. 2006.

[49] H. Wu, H. Wang, and R. Yu, “Color visual cryptography scheme using meaningful shares,” *IEEE Conference on Intelligent Systems Design and Applications*, pp. 173-178, Nov. 2008.

[50] Z. Wang, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography via Error diffusion,” *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 383-396, Sep. 2009.

[51] F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 27-38, Mar. 2010.

[52] I. Kang, G. R. Arce and H. Lee, “Color extended visual cryptography using Error diffusion,” *IEEE Transactions on Image Processing*, vol. 20, no. 1, pp. 132-145, Jan. 2011.

[53] S. Katta, “Visual secret sharing scheme using grayscale images,” *Cornell University Cryptology and Security ePrint Archive*, vol. 1, no. 6, pp.1-12, Jan. 2011.

[54] N. S. Alex and L. J. Anbarasi, “Enhanced image secret sharing via Error diffusion in halftone visual cryptography,” *IEEE Conference on Electronics and Computer Technology*, pp. 393-397, Apr. 2011.

[55] D. Wang, L. Dong, and X. Li, “Towards shift tolerant visual secret sharing schemes,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 323-337, Jun. 2011.

[56] F. Liu and C. Wu, “Embedded extended visual cryptography schemes,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 307-322, Jun. 2011.

[57] P. Chiu and K. Lee, “A simulated annealing algorithm for general threshold visual cryptography schemes,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 992-1001, Sep. 2011.

[58] Y. Hou and Z. Quan, “Progressive visual cryptography with unexpanded shares,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 11, pp. 1760-1764, Nov. 2011.

[59] T. Chen and K. Tsao, “User-friendly random grid based visual secret sharing,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 11, pp. 1693-1703, Nov. 2011.

[60] R. Wang and S. Hsu, “Tagged visual cryptography,” *IEEE Signal Processing Letters*, vol. 18, no. 11, pp. 627-630, Nov. 2011.

[61] S. Lin and W. Chung, “A probabilistic model of (t, n) visual cryptography scheme with dynamic group,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 197-207, Feb. 2012.

[62] M. Iwamoto, “A weak security notion for visual secret sharing schemes,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 372-382, Apr. 2012.

[63] S. J. Shyu and H. Jiang, “Efficient construction for region incrementing visual cryptography,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 22, no. 5, pp. 769-777, May 2012.

[64] S. J. Shyu, “Visual cryptograms of random grids for general access structures,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 3, pp. 414-424, Mar. 2013.

[65] K. Lee and P. Chiu, “Image size invariant visual cryptography for general access structures subject to display quality constraints,” *IEEE Transactions on Image Processing*, vol. 22, no. 10, pp. 3830-3841, Oct. 2013.

[66] D. Wang, T. Song, L. Dong, and C. Yang, “Optimal contrast grayscale visual cryptography schemes with reversing,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2059-2072, Dec. 2013.

[67] R. D. Prisco and A. D. Santis, “On the relation of random grid and deterministic visual cryptography,” *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 653-665, Apr. 2014.

[68] N. Askari, H. M. Heys, and Cecilia R. Moloney, “Novel visual cryptography schemes without pixel expansion for halftone images“, *Canadian Journal of Electrical and Computer Engineering*, vol. 37, no. 3, pp. 168-177, Jul. 2014.

[69] X. Wang, Q. Pei, and H. Li, “A lossless tagged visual cryptography scheme,” *IEEE Signal Processing Letters*, vol. 21, no. 7, pp. 853-856, Jul. 2014.

[70] D. Ou, W. Sun, X. Wu, “Non-expansible XOR-based visual cryptography scheme with meaningful shares,” *Elsevier Journal on Signal Processing*, vol. 108, no. 11, pp. 604-621, Oct. 2014.

[71] P. Chiu and K. Lee, “User-friendly threshold visual cryptography with complementary cover images,” *Elsevier Journal on Signal Processing*, vol. 108, no. 32, pp. 476-488, Oct. 2014.

[72] X. Yan, S. Wang, X. Niu, and C. Yang, “Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality,” *Elsevier Journal on Digital Signal Processing*, vol. 38, no. 2, pp. 53-65, Dec. 2014.

[73] C. Yang, C. Chen, S. Cai, “Enhanced Boolean-based multi secret image sharing scheme,” *Elsevier Journal on Systems and Software*, vol. 1, no. 13, pp. 89-101, Feb. 2015.

[74] C. Yang and C. Lin, “Almost aspect ratio invariant visual cryptography without adding extra sub-pixels,” *Elsevier Journal on Information Sciences*, vol. 312, no. 24, pp. 131-151, Mar. 2015.

[75] R. A. Ulichney, *Digital Halftoning*. MIT Press, Cambridge, 1987.

[76] M. Naor and B. Pinkas, “Visual authentication and identification,” *CRYPTO Journal on Cybernetics*, vol. 3, no. 1, pp. 322-336, Mar. 1997.

[77] G. Horng, T. Chen, and D. Tsai, “Cheating in visual cryptography,” *Design Codes Cryptography*, vol. 38, no. 2, pp. 219-236, Oct. 2006.

[78] C.N. Yang and C.S. Laih, “Some new types of visual secret sharing schemes,” *IEEE Journal on cybernetics*, vol. 31, no. 25, pp. 260-268, Dec. 1999.

[79] C.C. Wu and L.H. Chen, “A study on visual cryptography,” *M.S. thesis, Institute of Computer and Information Science*, National Chiao Tung University, Taiwan, 1998.

[80] T. Katoh and H. Imai, “An extended construction method for visual secret sharing schemes,” *IEICE Transactions on Data Security*, vol. 79, no. 8, pp. 1344-1351, May 1996.

[81] H. Wu and C. Chang, “Sharing visual multi-secrets using circle shares,” *Elsevier Jounal on Computer Standards and Interfaces*, vol. 28, pp. 123-135, July 2005.

[82] O. Benedens, “Geometry-based watermarking of 3D models,” *IEEE Transactions on Computer Graphics and Applications*, vol. 19, no. 1, pp. 46-55, June 1999.

[83] L. Euler, “A curious question with solution submitted,” *Academy Memoirs*, 1849.

[84] S. Dally, *User Book of Computer Puzzles*. 1st ed. Century Publications, Oct. 1984

[85] A. J. Schwenk, “Which rectangular chessboards have a knight’s tour?,” *Mathematics Association of America*, vol. 64, no. 5, pp. 325-332, Dec. 1991.