# CHAPTER 1

# INTRODUCTION

## 1.1 ENCRYPTION

In present times, the protection of multimedia data is becoming very important. With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. There are so many different techniques that can be used to protect confidential data from unauthorized access. In this section, we provide a brief about the different techniques for image encryption and we also give a general introduction about cryptography.

Encryption can be defined as the conversion of plain message into a form called a cipher text that cannot be read by anyone without decrypting the encrypted text. In other words, it is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not prevent interception, but denies the message content to the interceptor. Encryption has long been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems.

Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be read.

Cryptography and encryption are two closely related terminologies that find use in modern technologies everywhere. There are two main types of cryptography:

1. Secret key cryptography
2. Public key cryptography.

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key. Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys. Cryptography technique is used when secret message are transferred from one party to another over a communication line. Cryptography technique needs some algorithm for encryption of data. Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety. Image is also an important part of our information. Therefore it’s very important to protect our images from unauthorized access.

## 1.2 IMAGE ENCRYPTION

Digital images, accounting for 70% of the information transmission on the internet, is an important parts of network exchanges. However, the image information, which is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels. Traditional encryption algorithms such as DES, IDES, are against the text messages to be proposed, which are not suitable for digital image encryption, therefore, a reliable digital image with characteristics is in urgent need of the encryption scheme.

Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other words, it is essential that nobody could get to know the content without a key for decryption. Furthermore, special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfil such a task, many image encryption methods have been proposed. The image encryption algorithms can be classified into three major groups: (i) position permutation based algorithm (ii) value transformation based algorithm and (iii) visual transformation based algorithm.

## 1.3 LITERATURE SURVEY

**Massimiliano Zanin et al**, 2014 talks about a novel permutation algorithm for fast encryption of a large amount of data, such as 3D images and real-time videos are proposed. The proposed P-Box algorithm takes advantage of Gray code properties and allows fast encryption with high information diffusion. The algorithm is optimized for integer q-bit operations (q= 8; 16; 32; . . .), allowing a direct implementation in almost any hardware platform, while avoiding rounding errors of floating-point operations. By combining the P-Box with chaotic S-Box based on the logistic map, we design a complete, highly secure and fast cryptosystem. The main function of the designed P-Box is the fast permutation of very extensive information data. The speed of the Gray number algorithm is almost independent of the image size nor of the dimension of the permuted data.

**Xiao-Jun Tong et al**, 2014 deals with nodes of Wireless Sensor Network (WSN) having limited calculation and communication ability. Traditional encryption algorithms need large amounts of resources, so they cannot be applied to the wireless sensor network. To solve this problem, this paper proposes a block cipher algorithm for wireless sensor network based on compound chaotic map. The algorithm adopts Feistel network and constructs a Cubic function including discretized chaotic map, and its key is generated by the compound chaotic sequence. Due to the limited storage space of wireless sensors, the storage space of the algorithm is one of the important indicators to measure its effect. Speed is an important index to examine the encryption algorithm. To some extent, faster speed means that the energy-limited wireless sensors can save more energy.

**Hongjun Liua et al**, 2014 discusses chaos-based colour image encryption scheme using bijection. The whole image is diffused by exclusive or (XOR) operation for random rounds, each color component is separated into blocks with the same size. A bijective function f: B → S between block set B and S-box set S, is built. The corresponding 8 × 8 S-box is dynamically generated by the Chen system with variable conditions. The ciphered image can be obtained after substituting each block with the paired S-box. Each component of the color image is divided into blocks with the same size. To ensure the bijection between block set B and S-box set S, the initial values and parameter for Chen system are designed to dynamically change with the component number and the block number.

**Yushu Zhang et al**, 2013 proposes a novel image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Firstly, divide plain image into non-overlapping 8 X 8 pixels blocks with a random matrix, then transform each block into an 8 X 8 X 8 three dimensional (3-D) binary matrix, which has six directions just as a cube. Permutation is performed by multiplying the 3-D matrix by the rotation matrix that relies on plain image according to different direction. Secondly, use block diffusion to further change the statistical characteristics of the image after confusion. This algorithm is particularly suitable for running in a parallel and noisy environment. This algorithm takes into account the need for robustness of ciphered image against external noise and disturbances and so the proposed block diffusion is adopted for secure transmission on noisy channels.

**Liu Quan et al**, 2014 explain that in order to construct high complexity, secure and low cost image encryption algorithm, a class of chaos with Markov properties was researched and this algorithm was proposed. The kind of chaos has higher complexity than the Logistic map and Tent map, which keeps the uniformity and low autocorrelation. An improved couple map lattice based on the chaos with Markov properties is also employed to cover the phase space of the chaos and enlarge the key space, which has better performance than the original one. A true random number is used to disturb the key which can dynamically change the permutation matrix and the key stream. The algorithm is sensitive to the initial key and can change the distribution the pixel values of the image.

**Jun-xin Chen et al**, 2014 presents a fast chaos-based image encryption scheme with a dynamic state variables selection mechanism is proposed to enhance the security and promote the efficiency of chaos-based image cryptosystems. By using this mechanism, the state variables generated from the three-dimensional or hyper chaotic systems are dynamically and pixel-related distributed to each pixel in both permutation and diffusion procedures. A tiny change in the plain image will bring about totally different key stream sequences even though the same secret key is used. In conjunction with pixel-swapping based confusion strategy and snake-like mode diffusion, the difference produced in state variables distribution will be transferred to the encrypting process and then spread out to the whole cipher image within the first encryption round.

**Murillo-Escobar et al**, 2014 expresses that color image encryption is important to ensure its confidentiality during its transmission on insecure networks or its storage. The fact that chaotic properties are related with cryptography properties in confusion, diffusion, pseudorandom, etc., researchers around the world have presented several image (gray and color) encryption algorithms based on chaos, but almost all them with serious security problems have been broken with the powerful chosen/known plain image attack. The security analysis confirms that the RGB image encryption is fast and secure against several known attacks; therefore, it can be implemented in real-time applications where a high security is required. A good encryption algorithm must be robust but it needs to be fast for real-time applications in telemedicine, military, personal image, video conference, biometric systems, and etcetera. The encryption speed of a 256 x 256 color image size (1.572MB) using the proposed algorithm in this paper could reach 24MB/s.

**Xing-YuanWang et al**, 2014 discusses the cycle shift in bits of pixels and employs the chaotic system for the encryption of the proposed scheme. For cycle shift operations, random integers with the same size of the original image are produced to scramble the plaintext image. Moreover, the scrambled image effects the initial values of the chaotic system for the further encryption process, which increases the sensitivity of plaintext images of the scheme. The scrambled image is encrypted into the ciphered image by the keys which are produced by the chaotic system. The computational complexity of proposed scheme is very low because it involves cyclic shift operation and the number of shifts is decided by the chaotic maps.

**Zhongyun Hua et al**, 2014 introduces a new two-dimensional Sine Logistic modulation map (2D-SLMM) which is derived from the Logistic and Sine maps. Compared with existing chaotic maps, it has the wider chaotic range, better ergodicity, hyper chaotic property and relatively low implementation cost. To investigate its applications, a chaotic magic transform (CMT) is proposed to efficiently change the image pixel positions. Combining 2D-SLMM with CMT a new encryption algorithm is proposed in this paper. Performance analysis is provided to show that 2D-SLMM has the wider chaotic range, better ergodicity and hyper chaotic properties than existing chaotic map.

**Xingyuan Wang et al**, 2014 proposes a new block image encryption scheme based on hybrid chaotic maps and dynamic random growth technique. In the diffusion process, an intermediate parameter is calculated according to the image block. The intermediate parameter is used as the initial parameter of chaotic map to generate random data stream. In this way, the generated key streams are dependent on the plaintext image, which can resist the chosen plaintext attack. The experiment results prove that the proposed encryption algorithm is secure enough to be used in image transmission systems.

## 1.4 ORGANISATION OF THE REPORT

**Current chapter** deals with a need for encryption, cryptographic techniques and brief introduction about image encryption. It also provides a literature survey about various image encryption techniques and currently used methods for it.

**Chapter 2** discusses about the image encryption algorithms and performance parameters to substantiate efficiency of the algorithm.

**Chapter 3** present a gray code permutation based algorithm for encrypting high dimensional data and it is also validated with various performance metrics.

**Chapter 4** talks about fractal based image encryption where image is hidden under the complex details of the fractal image and the performance analysis is carried out.

**Chapter 5** explains the image encryption by making use of dynamic random growth technique and its efficiency is justified by the various performance metrics.

**Chapter 6** gives the conclusion of the project and the avenues for the future work in encrypting high dimensional data like 3D images and videos.

# CHAPTER 2

# IMAGE ENCRYPTION

## 2.1 IMAGE ENCRYPTION

This project work deals with the study and implementation of three different algorithms for Image encryption followed by a detailed performance analysis of these algorithms to determine their encryption efficiency and quality.

Several applications today require images to be transmitted securely over communication lines. Digital images are subject to a wide variety of distortions during acquisition, processing, compression, storage, transmission and reproduction, any of which may result in a degradation of visual quality. Hence, encryption algorithms must be suitable such that encrypted outputs cannot be tampered in any way. To quantify and validate the efficiency of an encryption scheme, several performance metrics are used as described in the following sub-section.

## 2.2 PERFORMANCE METRICS

### 2.2.1 Histogram analysis

The histogram, also called a gray value distribution chart image, reflects the pixels distribution of an image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance. The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone. If the histogram of an encrypted image is uniform, i.e., each gray level has equal probability, then the encryption scheme is more robust against statistical attack and differential attack.

### 2.2.2 Correlation analysis

Plain image has strong correlations among adjacent pixels, which makes fast data-diffusion quite difficult and statistical attack possible. To investigate the diffusion effect of our scheme, we test the correlation between two horizontally adjacent pixels, two vertically adjacent pixels, and two diagonally adjacent pixels in the plain image and the encrypted image, respectively.

To quantify and compare the correlations of adjacent pixels in the plain image and the encrypted image more precisely, we also calculate the correlation coefficient $r_{xy}$ of adjacent pixels of the plain image and the encrypted image by Eqn (2.1),

$$r_{xy} = \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x) * D(y)}} \qquad (2.1)$$

where *E(x)* and *D(x)* are the expectation and variance of variable *x*, respectively.

### 2.2.3 Information entropy analysis

The concept of information entropy was created by Shannon. It has applications in many areas, such as, lossless data compression, statistical inference, cryptography. Recently it is used in other disciplines, such as, biology, physics, and machine learning. Information entropy is a measure of the uncertainty associated with a random event and it is used to tell how much information there is in an event. In general, the more uncertain or random the event is, the more information entropy it will contain. Therefore, it is very useful for analysing the randomness of an encryption scheme. Here we use *H(X)* to represent the information entropy of an information source $X=(x_0, x_1, \ldots, x_{L-1})$ with length *L* as in Eqn (2.2),

$$H(X) = -\sum_{i=0}^{L-1} p(x_i)\log_2 p(x_i) \tag{2.2}$$

where $p(x_i)$ represents the probability of symbol $x_i$.

For a true random information source *X* emits $2^8$ symbols with equal probability. After computing the information entropy by Equation (2.2), we get *H(X)* =8. Actually, given that a practical information source seldom generates random messages, we know that its information entropy value is smaller than 8 in general. However, when the messages are encrypted, their information entropy should ideally be 8. Particularly, if an image encryption algorithm creates symbols with information entropy less than 8, there is a possibility of predictability, which is a threat to the cryptosystem security.

### 2.2.4 Key sensitivity analysis

Key sensitivity includes encrypted key sensitivity and decrypted key sensitivity. It basically shows the change in the level of encryption with the trivial change of encrypted key and decrypted key, respectively. When an algorithm involves specific parameters in the encryption process, the behaviour of the algorithm and eventually the result is determined by the value of the parameters/keys chosen. Hence, the outputs are studied for different values of the keys involved in the encryption and decryption stages. It is also used as a metric to test the ability of an encryption scheme to withstand differential attacks.

### 2.2.5 NPCR and UACI

The Number of Pixels Changing Rate (NPCR) and the Unified Averaged Changed Intensity (UACI) are two most common quantities used to evaluate the strength of image encryption algorithms/ciphers with respect to differential attacks. Conventionally, a high NPCR/UACI score is usually interpreted as a high resistance to differential attacks. However, it is not clear how high NPCR/UACI is such that the image cipher indeed has a high security level.

The NPCR and UACI are designed to test the number of changing pixels and the number of averaged changed intensity between ciphertext images, respectively, when the difference between plaintext images is subtle (usually a single pixel).

Suppose ciphertext images before and after one pixel change in a plaintext image are $C^1$ and $C^2$, respectively; the pixel value at grid (i, j) in $C^1$ and $C^2$ are denoted as $C^1$ (i, j) and $C^2$ (i, j); and a bipolar array is defined $D$ in eqn (2.3). Then the NPCR and UACI can be mathematically defined by eqn (2.4) and (2.5), respectively, where symbol $T$ denotes the total number pixels in the ciphertext and symbol $F$ denotes the largest supported pixel value compatible with the ciphertext image format.

$$D(i,j)=\begin{cases}0, if\ C^1(i,j)=C^2(i,j)\\ 1, if\ C^1(i,j)\neq C^2(i,j)\end{cases} \tag{2.3}$$

$$NPCR: N(C^1,C^2)=\sum_{i,j}\frac{D(i,j)}{T}\times 100\% \tag{2.4}$$

$$UACI: U(C^1,C^2)=\sum_{i,j}\frac{|C^1(i,j)-C^2(i,j)|}{F\bullet T}\times 100\% \tag{2.5}$$

NPCR concentrates on the absolute number of pixels which changes value in differential attacks, while the UACI focuses on the averaged difference between two paired ciphertext images. The range of NPCR is [0, 1]. When $N(C^1,C^2)$=0, it implies that all pixels in $C^2$ remain the same values as in $C^1$.

When $N(C^1,C^2)=1$, it implies that all pixel values in $C^2$ are changed compared to those in $C^1$. In other words, it is very difficult to establish relationships between this pair of cipher text images. However, $N(C^1,C^2)=1$ rarely happens, because even two independently generated true random images fail to achieve this NPCR maximum with a high possibility, especially when the image size is fairly large compared to $F$.

The range of UACI is clearly [0, 1] as well, but it is not obvious that what a desired UACI for two ideally encrypted images is.

### 2.2.6 Randomness analysis

The NIST SP800-22 tests is a statistical package consisting of 16 tests that are developed to test the randomness of binary sequences produced by either hardware or software based on cryptographic random or pseudorandom number generators. These tests focus on a variety of different types of non-randomness that may exist in a sequence. In NIST SP800-22 tests, each test produces a P-value which is a real number in [0, 1]. If the P-value is greater than a predefined threshold a called significant level, the encrypted image passes the test successfully. If the algorithms pass the NIST Test suite, then we can claim that the encrypted image in our system is stochastic.

### 2.2.7 Mean Square Error Analysis (MSE)

The MSE test measures how much the wrong decrypted image is distorted from the original image and it is calculated as given by eqn (2.6),

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{H} \sum_{j=1}^{W} [P(i, j) - D(i, j)]^2 \qquad (2.6)$$

where *W* and *H* are the width and height of the image respectively, *P(i, j)* is original image pixel value and *D(i, j)* is the corresponding wrong decrypted image pixel value.

### 2.2.8 Peak Signal-to-Noise Ratio (PSNR) Analysis

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is most commonly used to measure the quality of reconstruction of lossy codes in image processing and is commonly calculated using the eqn (2.7). The signal in this case is the original data, and the noise is the error introduced by compression/encryption. A higher PSNR generally indicates that the reconstruction is of higher quality.

$$PSNR = 10 \log_{10} ({MAX_I}^2 / MSE) \qquad (2.7)$$

where $MAX_I$ is the maximum possible pixel value of the image(Here, it is 255 for 8 bit representation of pixels) and *MSE* represents the Mean Square Error.

# CHAPTER 3

# GRAY CODE PERMUTATION ALGORITHM FOR HIGH-DIMENSIONAL DATA ENCRYPTION

## 3.1 INTRODUCTION

In recent years, the volume of information that needs to be transmitted through any communication media has gone up very rapidly; and while security still remains a serious problem, speed is becoming another important issue. There is an evident relationship between the Encryption/Decryption Time (EDT) and the quantity of information to be transmitted; the larger the data size, the longer the EDT. It is well known that a strong cryptosystem must include two main steps: P-Box or permutation step, where the information position is changed in the data sequence, and S-Box or substitution step, where every single piece of information (symbol or group of symbols, e.g. each byte) is substituted by another symbol. These two steps reflect two basic properties of a good cryptosystem, confusion and diffusion. The purpose of this work is to design a rapid P-Box algorithm which would allow a fast permutation of a very large amount of data inside a multi-dimensional memory structure. It is clear that a cryptosystem based on permutation only, cannot guarantee much security because of their vulnerability to plaintext attacks; to ensure high security, a complete cryptosystem needs a secure S-Box.

## 3.2 ALGORITHM DESCRIPTION

### 3.2.1 Proposed Encryption Scheme

Step 1: Read the input image and using the keys k1 and k2 (k1=18921 and k2=601) generate the permutation vector Of(1).

Step2: Input image is converted into 1-D vector and by utilizing Of(1) the positions of pixels in the original image is shuffled.

Step3: Now the individual pixels of permuted image is subjected to gray code conversion.

Step4: The image obtained after gray code conversion is diffused sequentially by XOR operation with an initial seed value of ‘s’(s=45).

Diffusion operation is represented by eqn (3.1),

$$C_n = P_n \oplus C_{n-1} \qquad (3.1)$$

where $C_n$ , $C_{n-1}$ are ciphered pixels at position n and n-1, $P_n$ is pixel value at position n.

Step 5: The image after diffusion process is XORed with compound chaotic sequence to obtain the final encrypted image.

#### 3.2.1.1 Compound chaotic sequence generation:

Step1: First by using linear congruential random number generator Y1(k) is generated. The LCG sequence is generated using the eqn (3.2),

$$L(n+1) = (d \times L(n) + f)\,\mathrm{mod}(m) \qquad (3.2)$$

Step 2: Using Y1(k) as initial value generated Y2(k) by using discretized cubic map.

Step 3: X(k) is obtained from discretized logistic map and it is XORed with Y2(k) to get C1(k).

Step 4: Another sequence Z(k) is generated from LCRG with different initial conditions.

Step 5: Finally, C1(k) is XORed with Z(k) to produce C2(k), the compound chaotic sequence and this process is shown in Fig 3.1 and encryption system is depicted in Fig 3.2,

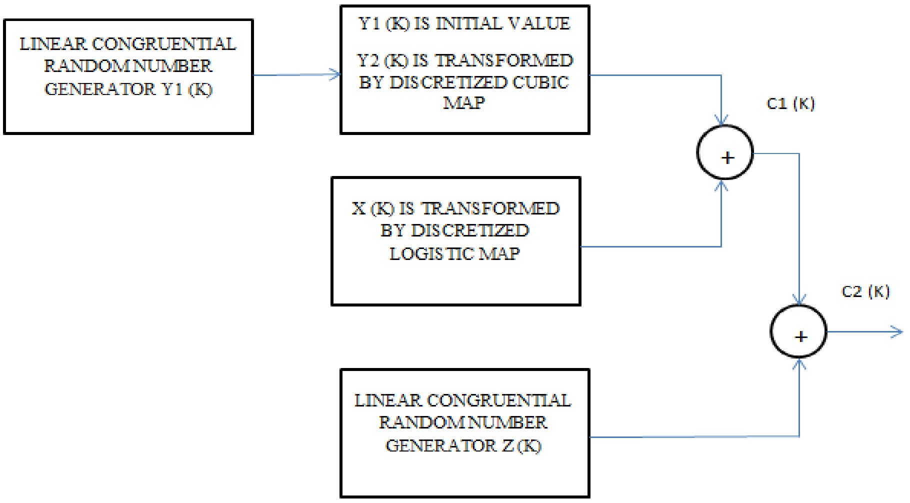

LINEAR CONGRUENTIAL RANDOM NUMBER GENERATOR Y1 (K)
Y1 (K) IS INITIAL VALUE
Y2 (K) IS TRANSFORMED BY DISCRETIZED CUBIC MAP
C1 (K)
+
X (K) IS TRANSFORMED BY DISCRETIZED LOGISTIC MAP
C2 (K)
+
LINEAR CONGRUENTIAL RANDOM NUMBER GENERATOR Z (K)

Fig. 3.1 Generation of compound chaotic sequence

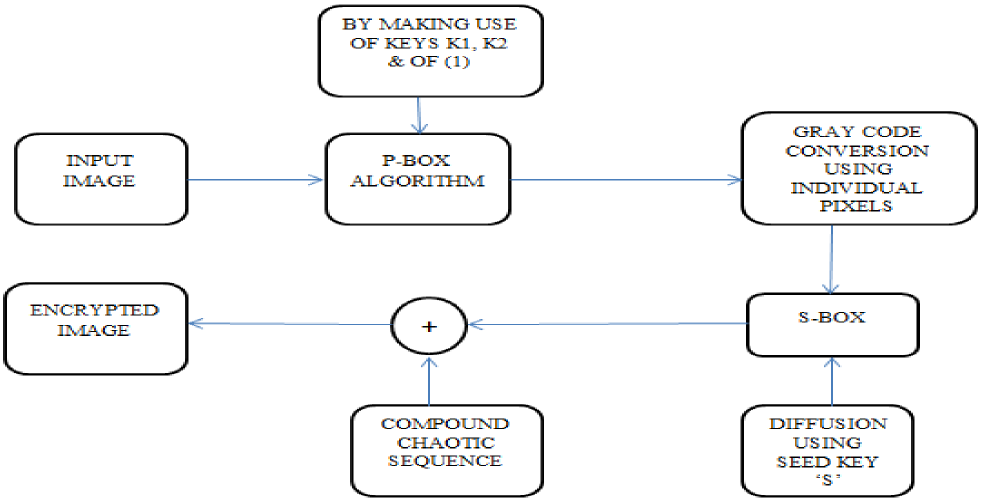

BY MAKING USE OF KEYS K1, K2 & OF (1)
INPUT IMAGE
P-BOX ALGORITHM
GRAY CODE CONVERSION USING INDIVIDUAL PIXELS
ENCRYPTED IMAGE
+
S-BOX
COMPOUND CHAOTIC SEQUENCE
DIFFUSION USING SEED KEY 'S'

Fig. 3.2 Encryption System

### 3.2.2 Decryption Process

The decryption process involves the exact reverse of steps performed in encryption.

Step1: The encrypted image is XORed with compound chaotic sequence and it is then subjected to inverse S-Box operation.

Step2: Then the pixels of the image obtained after inverse S-BOX operation is converted back from gray code to binary.

Step3: The image obtained after step 2 is again shuffled back to original pixel values using Of(1).

## 3.3 Performance analysis and results

The proposed encryption algorithm is applied on the source image and the resultant encrypted and decrypted images are shown below in Fig. 3.3,

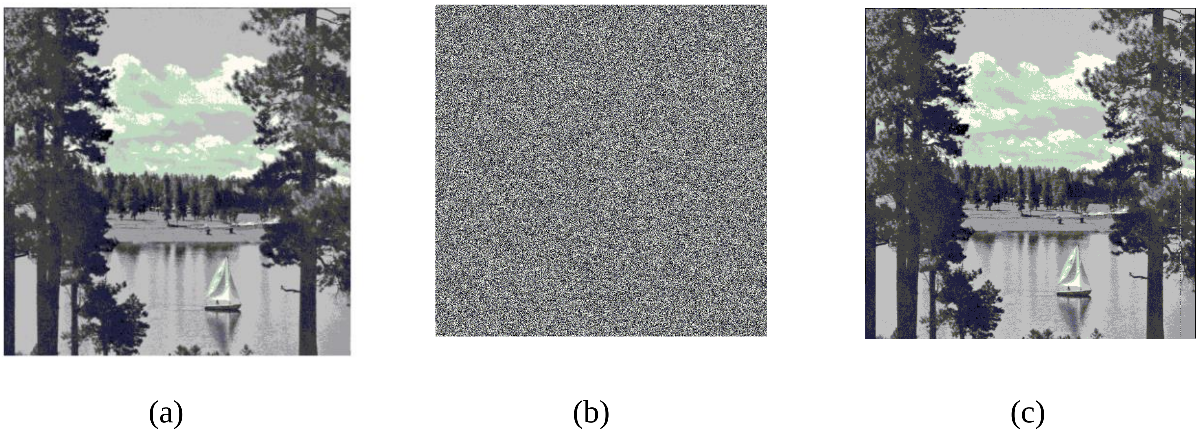
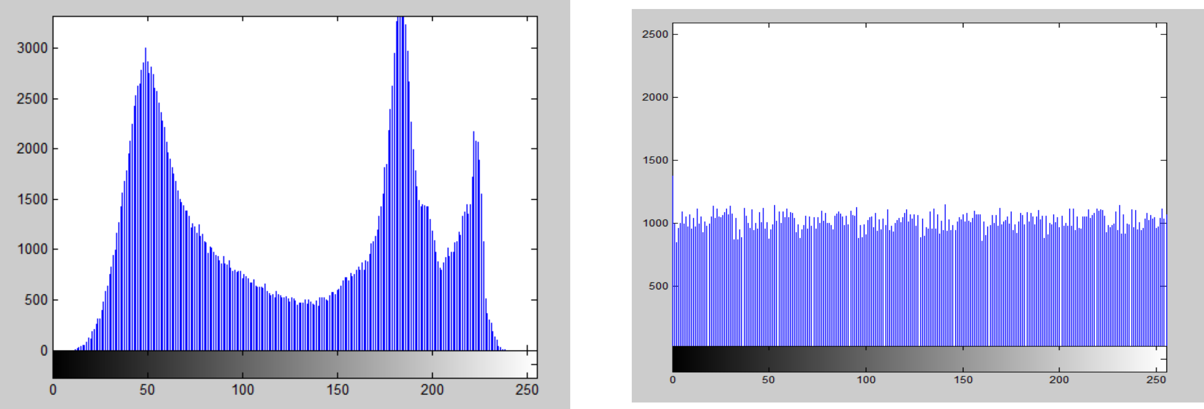


Fig 3.3 (a) Original Image (b) Cipher image (c) Decrypted image

The histogram plots of the source and cipher images are taken to show the tonal distribution of pixels in original and encrypted image.

A uniform histogram plot (Fig. 3.4 (b)) of the encrypted images shows that the probability of occurrence of each gray level is uniform thereby making the encryption scheme more robust against statistical attack and differential attack.



(a) (b)

Fig. 3.4 Histogram plots of (a) Source image (b) Cipher image

The correlation plot of horizontally, vertically and diagonally adjacent pixels in the encrypted image shown in Fig. 3.5, indicate that reconstruction of the image is difficult due to high degree of randomness between any pair of pixels taken

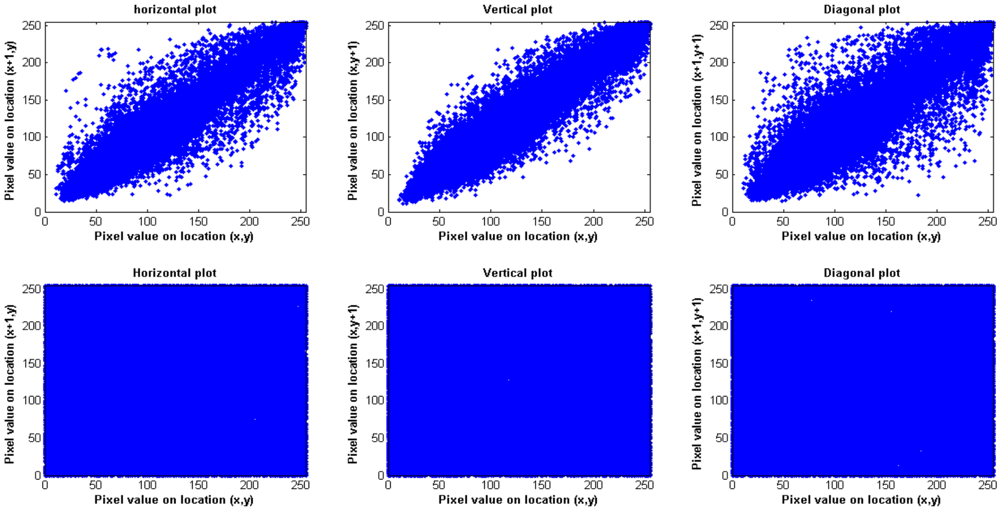


Fig. 3.5 Correlation of adjacent pixels in [Top] Source image & [Bottom] Cipher image

The performance analysis parameters are computed for different encrypted images obtained by employing above mentioned algorithm and the results are shown in Table 3.1.

Table 3.1- Performance Analysis Results

| **Input image** | **Cross Correlation coefficient** | **NPCR %** | **UACI %** | **Entropy** | **PSNR (dB)** |
|---|---|---|---|---|---|
| | 0.0053 | 99.58 | 12.49 | 7.9994 | 31.7824 |
| | 0.0031 | 99.58 | 12.49 | 7.9993 | 31.5897 |
| | 0.0014 | 81.54 | 20.45 | 7.9993 | 34.2920 |
| | 0.0019 | 63.73 | 15.99 | 7.9994 | 33.118 |

From the NIST Test suite report shown in Table 3.2, it is evident that the randomness test performed on the encrypted output from the proposed algorithm has passed the significant threshold level.

Table 3.2- NIST Statistical Test Suite Report

| TEST | PV | PP |
|---|---|---|
| Block frequency | 0.350485 | 10/10 |
| Cumulative sums | 0.350485 | 10/10 |
| Runs | 0.002043 | 10/10 |
| Longest run | 0.739918 | 10/10 |
| Rank | 0.122325 | 10/10 |
| FFT | 0.739918 | 10/10 |
| Serial | 0.122325 | 10/10 |
| Universal | 0.47568 | 9/10 |
| Approximate entropy | 0.000199 | 7/10 |
| Random excursion | ---------- | --- |
| Non-overlapping template | 0.739918 | 10/10 |
| Overlapping template | 0.534146 | 10/10 |
| Random excursion variant | ---------- | --- |
| Linear complexity | 0.350485 | 10/10 |
| Final result | SUCCESS | |

## 3.4 CONCLUSION

For real-time secure communication with a large amount of information, the proposed algorithm introduces a P-Box as the first stage followed by sequential column-wise diffusion and an XOR operation with the chaotic sequence. The algorithm was optimized for integer n-bit operations that avoids rounding errors of floating-point operations. The encryption speed of the proposed algorithm is independent of the data size that allows encryption of extremely large amounts of information in real time. The proposed encryption system has relatively low complexity as it takes advantage of the Gray code properties and hence can be implemented for sensor networks where nodes cannot handle heavy floating point arithmetic.

# CHAPTER 4

# FRACTAL BASED IMAGE ENCRYPTION SYSTEM

## 4.1 INTRODUCTION

Today large sets of data are being transferred over the internet and also through portable handheld devices. Cryptography and Steganography are two important approaches for achieving a secure transmission of the images. Cryptography, basically codes the original data into unreadable texts called the ciphered text before transmission. Steganography, on the other hand hides the original data under a mask such that only the intended user knows how the data is hidden and will be able to retrieve the original data. If the mask used is an image, it is called as a cover image.

Any digital crypto system is divided into two based on the key distribution namely symmetric key and asymmetric key. The proposed algorithm utilizes the concepts of symmetric key cryptography as well as steganography. The mask used for encrypting the image and hiding the data is a fractal image. A fractal image is the representation of a mathematical equation or function that is iterated for a finite number of times. So, fractals can be self-similar at different scales of magnification, also possess high variations in its details, color, local and global irregularity that cannot be easily described using traditional Euclidian geometry.

The fractal image that we have utilized in our proposed algorithm is the spiral fractal. To enhance the encryption process, in addition to the diffusion and confusion process a delay function has also been introduced which will be discussed in detail in the sections to follow.

## 4.2 ALGORITHM DESCRIPTION

The proposed encryption algorithm utilizes the fractal image to encrypt the information image. The pixels of the source image shown are first subjected to an XOR operation with the Fractal image shown in Fig. 4.1.

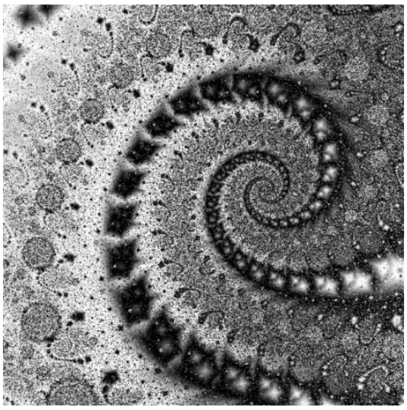


Fig. 4.1 Spiral Fractal Image used in the proposed cryptosystem

The image obtained after XOR operation is then delayed by one pixel position to make the output more random.

The delay function is given below in eqn (4.1):

$$Y1_{i,j} = \begin{cases} Y_{i,j-1} & j \neq 1 \\ Y_{i-1,2^M} & j = 1 \quad , i \neq 1 \\ 0 & i,j = 1 \end{cases} \tag{4.1}$$

The delayed set of pixels is consecutively subjected to confusion and diffusion processes. The confusion process is initiated with the help of a Linear Congruential Random Generator (LCRG). By using the sequence generated from LCRG the delayed set of pixels are permuted and also LCRG is highly sensitive to the initial seed value, and the seed value used here is 17. To enhance the encryption level of the output, a subsequent diffusion scheme is implemented by means of a S-Box algorithm. The confusion operation followed by substitution ensure high level of security and the substitution operation has to be done with care so as to ensure high entropy obtained by utilizing fractal image is not reduced. The entire encryption system is represented as shown in Fig. 4.2.

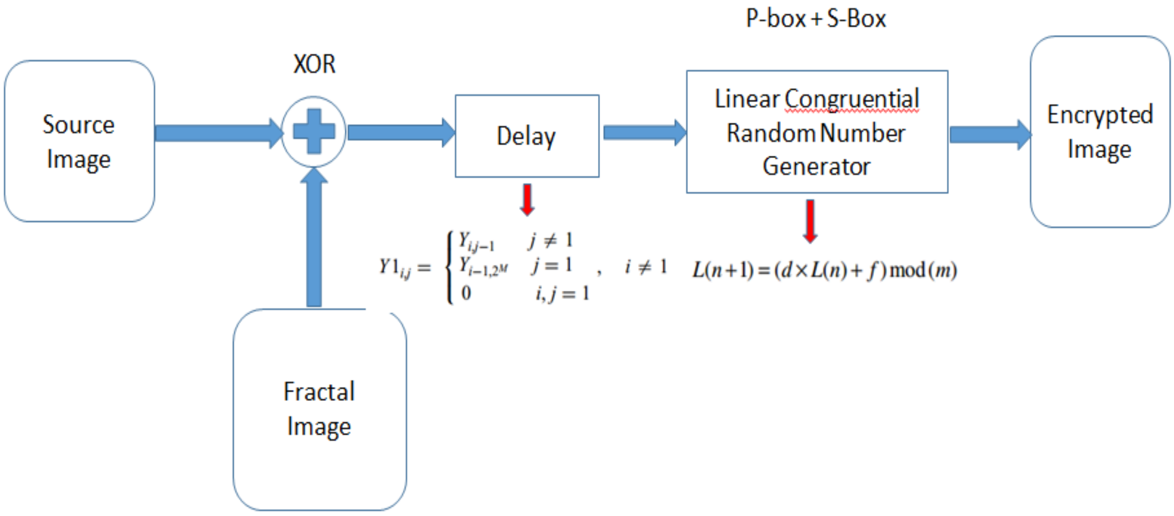
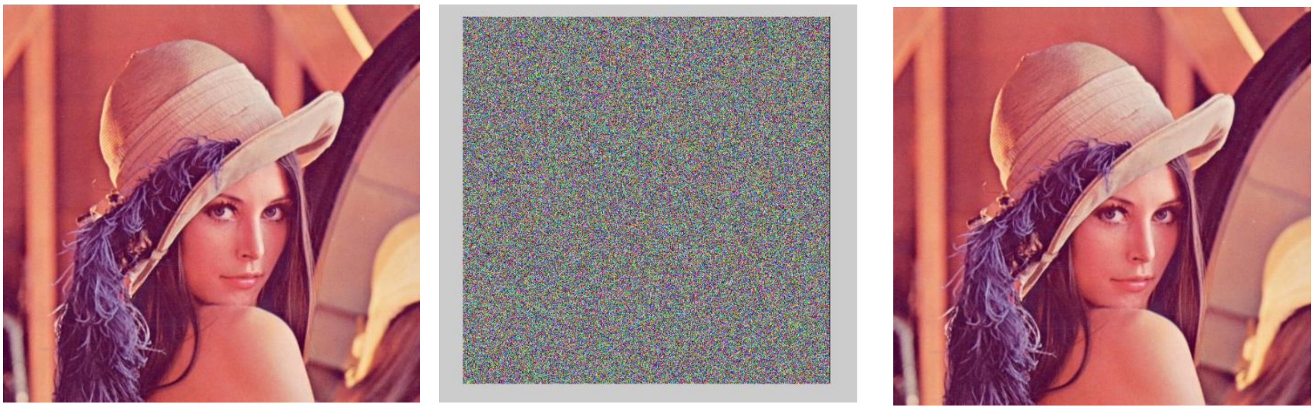

P-box + S-Box
XOR
Source Image
Delay
Linear Congruential Random Number Generator
Encrypted Image
Fractal Image
$Y1_{i,j} = \begin{cases} Y_{i,j-1} & j \neq 1 \\ Y_{i-1,2^M} & j = 1 \quad , \quad i \neq 1 \\ 0 & i,j = 1 \end{cases}$
$L(n+1) = (d \times L(n) + f) \bmod (m)$

Fig. 4.2 Proposed Encryption system

The proposed encryption algorithm is implemented for color image components as well. The encryption algorithm is applied on the source image and the encrypted image obtained is shown in Fig. 4.3. The various performance analysis of the algorithm is discussed in detail in Section 4.3.

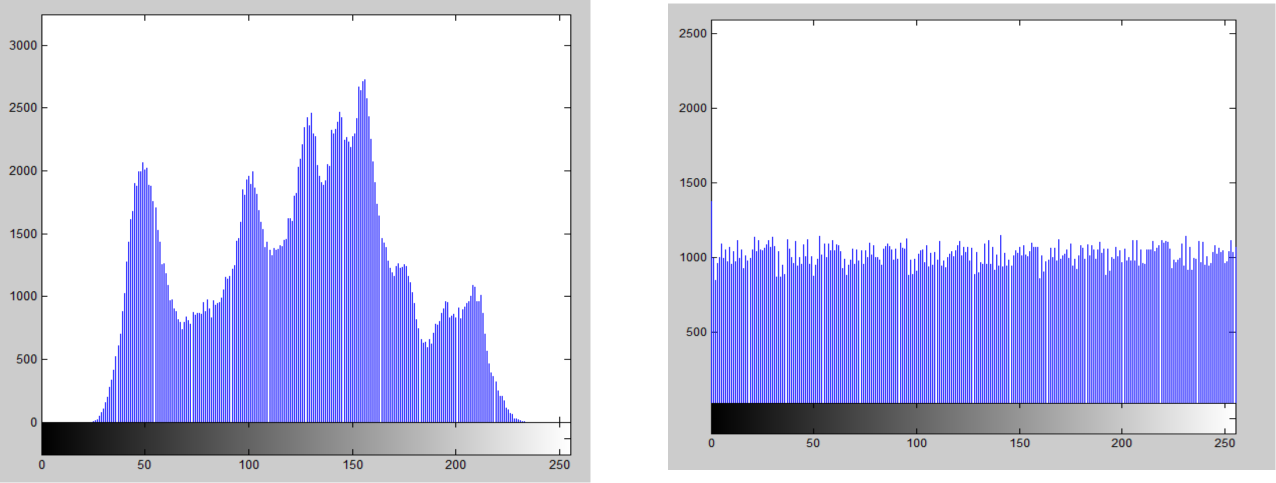


(a) (b) (c)

Fig. 4.3(a) Source Image (b) Encrypted Image (c) Decrypted output

## 4.3 PERFORMANCE ANALYSIS & RESULTS

When the histogram of an encrypted image is uniform then we can say that the encryption scheme is more robust against statistical attacks. When the histogram is uniform the reconstruction of the source image from the encrypted image is difficult. The histogram of the source and ciphered images are shown in Fig. 4.4.



(a) (b)

Fig. 4.4 Histograms of (a) Source image (b) Cipher image

The correlation of adjacent pixels in original image is very high and it indicates that the neighbouring pixels correspond to a particular region, but in the encrypted image the pixels are randomly distributed and hence the correlation of adjacent pixels is very low so that the image is protected against statistical attacks.

The correlation of horizontally, vertically and diagonally adjacent pixels is calculated for the plain and encrypted image. It can be seen that though there is high correlation between pixels in the plain image, the correlation among adjacent pixels in the encrypted image is negligible as is evident from the correlation plot shown in Fig 4.5. Thus we can say that the encryption system provides good security against statistical attacks.

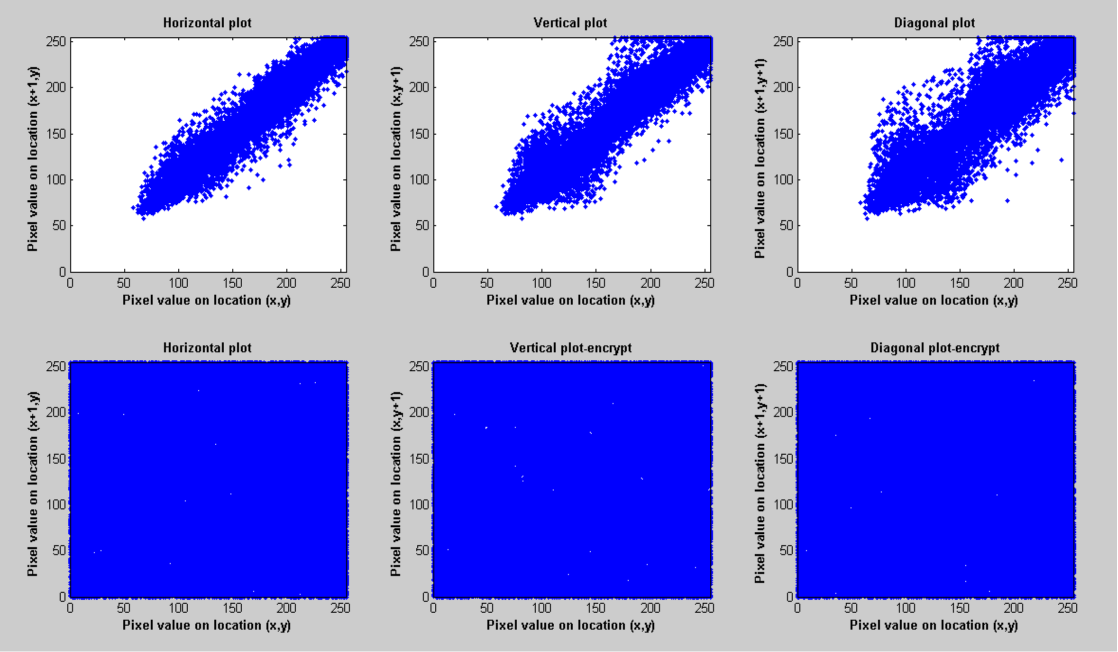


Fig.4.5 Correlation of adjacent pixels in [Top] Source image & [Bottom] Cipher image

The proposed encryption-decryption process is carried out for four different colour images and various performance analysis parameters are calculated. From the simulation results it can be seen that correlation coefficient between original and encrypted image is very low. Also, the entropy measured over different image sets is a high value (~7.99), thus indicating the efficiency of the encryption scheme. The PSNR values indicate that the loss of information in the decrypted image is minimal. The cross correlation coefficient indicates the relationship between the original image and encrypted image is less. In all the different set of color images it can be seen that the encryption scheme is highly efficient.

The performance metrics for different color images is listed in Table 4.1.

Table 4.1- Performance Analysis Results

| Images | Cross Correlation coefficient | Entropy | PSNR(dB) | MSE |
|---|---|---|---|---|
| | R: 0.0014<br>G: -0.0014<br>B: -0.0013 | 7.9968<br>7.9983<br>7.9972 | 51.7564 | 0.6925<br>0.4132<br>0.4340 |
| | R: 0.0034<br>G: -0.00082<br>B: 0.00073 | 7.9984<br>7.9980<br>7.9948 | 54.2482 | 0.2977<br>0.2844<br>0.1453 |
| | R: 0.00052<br>G: 0.0022<br>B: 0.0011 | 7.9965<br>7.9978<br>7.9966 | 51.3211 | 0.6351<br>0.4797<br>0.2839 |
| | R: 0.0015<br>G: -0.0014<br>B: 0.0014 | 7.9936<br>7.9935<br>7.9952 | 51.5877 | 0.4608<br>0.4731<br>0.4195 |

The NIST test is used to check the randomness of sequence generator and to determine how closer it is towards the true random generator sequence. The PP-value indicates the passing proportions of set of sequences that has successfully passed the test.

If the PV-value obtained in the NIST Report is greater than a predefined threshold α called significant level, the encrypted image passes the test successfully. As can be seen from Table 4.2, the encrypted image resulting from the proposed algorithm has passed the test and hence can be considered stochastic.

Table 4.2- NIST Statistical test suite Report

| TEST | PV | PP |
|---|---|---|
| Block frequency | 0.350485 | 10/10 |
| Cumulative sums | 0.534146 | 10/10 |
| Runs | 0.350485 | 10/10 |
| Longest run | 0.739918 | 9/10 |
| Rank | 0.991468 | 10/10 |
| FFT | 0.739918 | 10/10 |
| Serial | 0.739918 | 10/10 |
| Universal | 0.00199 | 8/10 |
| Approximate entropy | 0.27311 | 8/10 |
| Random excursion | ---------- | --- |
| Non-overlapping template | 0.911413 | 10/10 |
| Overlapping template | 0.74235 | 9/10 |
| Random excursion variant | 0.350485 | 10/10 |
| Linear complexity | 0.213309 | 8/10 |
| Final result | SUCCESS | |

## 4.4 CONCLUSION

The proposed algorithm for the image encryption of high dimensional color images using fractal images shows a great level of security achieved. The scope of this work can be extended from a single fractal image to multi-fractal images to improve the encryption quality. The performance analysis clearly demonstrates the quality of the encryption scheme and its security against statistical attacks. Entropy and correlation analysis further reiterates the efficiency of the proposed scheme.

# CHAPTER 5

# CHAOTIC BLOCK IMAGE ENCRYPTION BASED ON DYNAMIC RANDOM GROWTH TECHNIQUE

## 5.1 INTRODUCTION

Today more and more images and videos are being transmitted over the internet. As a result these images are prone to be attacked, tampered or stolen. For secure transmission of the information we go for various encryption schemes. We send bulk amount of data in the form of images and videos and encrypting such large volumes of data using traditional encryption systems like RSA, DES and IDEA has become a huge overhead and rather difficult. The chaos based encryption scheme has the characteristics of non-periodicity, ergodicity, non-convergence and sensitivity to initial conditions, which drew more and more attention to this scheme. The classic encryption schemes include a permutation and a diffusion process. For the permutation process there are many options like cat map permutation, XOR scrambling, sometimes even double images are used, some others propose generic methods and DNA sequences. In the diffusion process different maps are used to further improve the encryption like logistic map, Tent map, cubic map, ring shifts, XOR operations and the like. The proposed algorithm uses an Arnold map with a slight modification in the permutation process and a combination of logistic map and a tent map with a ring shift operation for the encryption stage. In the permutation process the Arnold map is slightly modified because the Arnold map is periodic making the information insecure and thereby the encryption scheme very poor. It can be seen that after five rounds of permutation, we get the plaintext again. So the cat map cannot be used in image transmission system, since the attacker can get the plaintext image of any cipher image just by iterating cat map to the cipher image. Despite these problems the encryption process is very fast which is very important in the real-time data transmission. The importance of the faster encryption is that the attacker will be unable to know if the transmitted information is the ciphered text or the plain text, thus making the transmission all the more secure.

## 5.2 ALGORITHM DESCRIPTION

### 5.2.1 Encryption

The encryption algorithm is based on hybrid chaotic maps and dynamic random growth technique. Like any other cryptosystem, the proposed encryption algorithm has a permutation and a diffusion process.

#### 5.2.1.1 Permutation Process

For the permutation process we make use of the Arnold cat map but in a modified manner. For a N×N image P we use the logistic map function given by eqn (5.1),

$$f : x_{n+1} = \mu x_n (1 - x_n) \tag{5.1}$$

where $x_n$ is an independent variable and $\mu$ is the control parameter of the logistic map whose value must be in the range 3.56 < $\mu \leq 4$ for the logistic map to be chaotic. Our assumption for the initial value of $\mu$ was 3.9.

(1) The chaotic sequence $x_n$ is generated from the equation (5.1). The initial values $x_{0,}$ $\mu_0$ are the secret keys for n=1, 2,..., 204. We drop the first 200 values to avoid any transient effects in the resulting output.

(2) Let,

$$low_i = floor(x_{200+i} \times 10^{14}) \bmod \frac{N}{8} + \frac{N}{2} + (i-1)\frac{N}{8}, \; i = 1, 2, 3, 4 \quad (5.2)$$

(3) Apply the shuffle process to the lower size of $low_i \times low_i$ of the image using the Arnold cat map function which is given by the eqn (5.3),

$$A= \begin{bmatrix} 1 & p \\ q & 1+pq \end{bmatrix} mod\ N \quad (5.3)$$

In the Arnold cat map we choose p=4 and q=8 and $N$ denotes the image dimensions (Here, N = 512 for a 512 x 512 image).

This step is repeated for all the four values of i=1, 2, 3, 4. This process is called the dynamic random growth technique since the lower part of the image permuted by the cat map function is random.

(4) Then shuffle the entire image using the cat map twice. By doing the shuffle operation twice we are able to overcome the periodicity problem.

### 5.2.1.2 Diffusion Process

In the diffusion process we include another logistic map and a tent map which are given by eqn (5.4) and (5.5),

Logistic Map:

$$h : x'_{n+1} = \mu' x'_n (1 - x'_n) \tag{5.4}$$

Tent map:

$$T(u,\alpha) = \begin{cases} \frac{u}{\alpha}, & 0 \le u \le \alpha \\ \frac{1-u}{1-\alpha}, & \alpha < u \le 1 \end{cases} \tag{5.5}$$

Here u is an independent variable; α is the control parameter of the Tent chaotic map; when $0 < \alpha < 1$, the Tent map is chaotic.

In the diffusion process we first divide the permuted image into four sub-images of the same size. We then perform the following steps:

(1) We first generate the chaotic sequence from the eqn (5.6),

$$h : x'_{n+1} = \mu' x'_n (1 - x'_n) \tag{5.6}$$

The initial values $x'_0$ and $\mu'_0$ are taken as the secret keys, n=1,2,3,..,104. We then drop the first 100 values to avoid the transient effects.

(2) Iterate the equation to get $r_i$ for i=1,2,3,4 until they are in one permutation of {1,2,3,4}, using the eqn (5.7),

$$r_i = floor(x_n^{'} \times 10^{13}) \bmod 4 + 1 \tag{5.7}$$

(3) Now concatenate the four sub images in the order obtained from $r_i$. This diffused image is then ring shifted by 5 pixel positions to obtain the final encrypted image that has a greater degree of randomness.

### 5.2.2 Decryption

The decryption process is typically the reverse process. First we ring shift the pixel values in the reverse order. The scrambled image is then subdivided into four equal sized sub-images. This is then rearranged to get back the permuted image using the secret keys. Reversing the Arnold and Tent map functions, we perform the inverse of the permutation process to get the final decrypted image.

## 5.3 PERFORMANCE ANALYSIS AND RESULTS

The proposed encryption algorithm is applied on the source image and the resultant encrypted and decrypted images are shown below in Fig. 5.1,

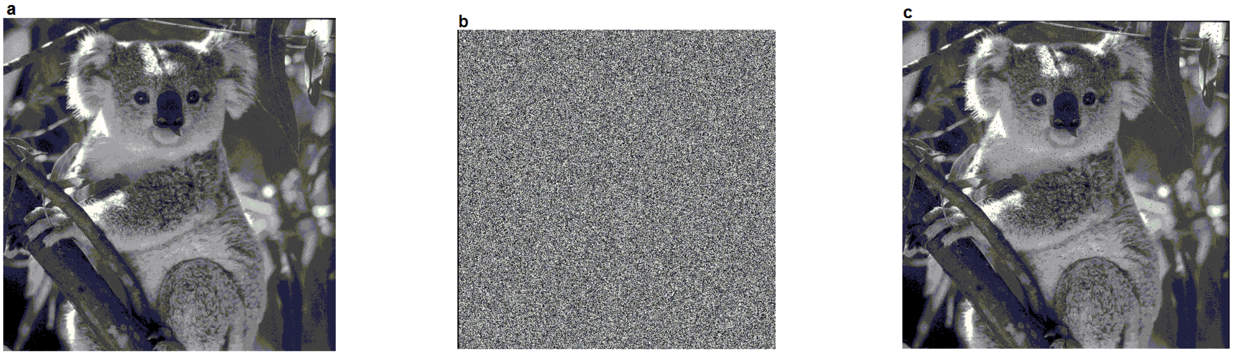


Fig. 5.1 (a) Original image (b) Cipher image (c) Decrypted image

Fig. 5.1 shows the encryption and decryption results of the Dynamic Random Growth algorithm applied on an input image as shown. The encryption quality has been tested by carrying out the following performance analysis as shown in Table 5.1

Table 5.1- Performance Analysis Results

| Images | Cross Correlation coefficient | NPCR | UACI | Entropy | PSNR(dB) | MSE |
|---|---|---|---|---|---|---|
| | 0.00059 | 99.30 | 31.21 | 7.9972 | 32.0252 | 40.79 |
| | 0.0048 | 96.16 | 24.15 | 7.9971 | 27.6545 | 111.591 |
| | 0.0103 | 99.32 | 37.48 | 7.9972 | 26.46 | 146.58 |
| | 0.0045 | 99.32 | 28.30 | 7.9972 | 29.2085 | 78.0245 |

The values of the performance metrics indicate that the algorithm is resistant to statistical and differential attacks and is also characterized by high entropy thus rendering intermediate attackers' effort useless.

Additionally, the auto correlation plots (Fig. 5.2) of the original and cipher images reveal that any two adjacent pixels taken along any direction, are not correlated thus providing evidence of the degree of pixel randomness in the encrypted image.

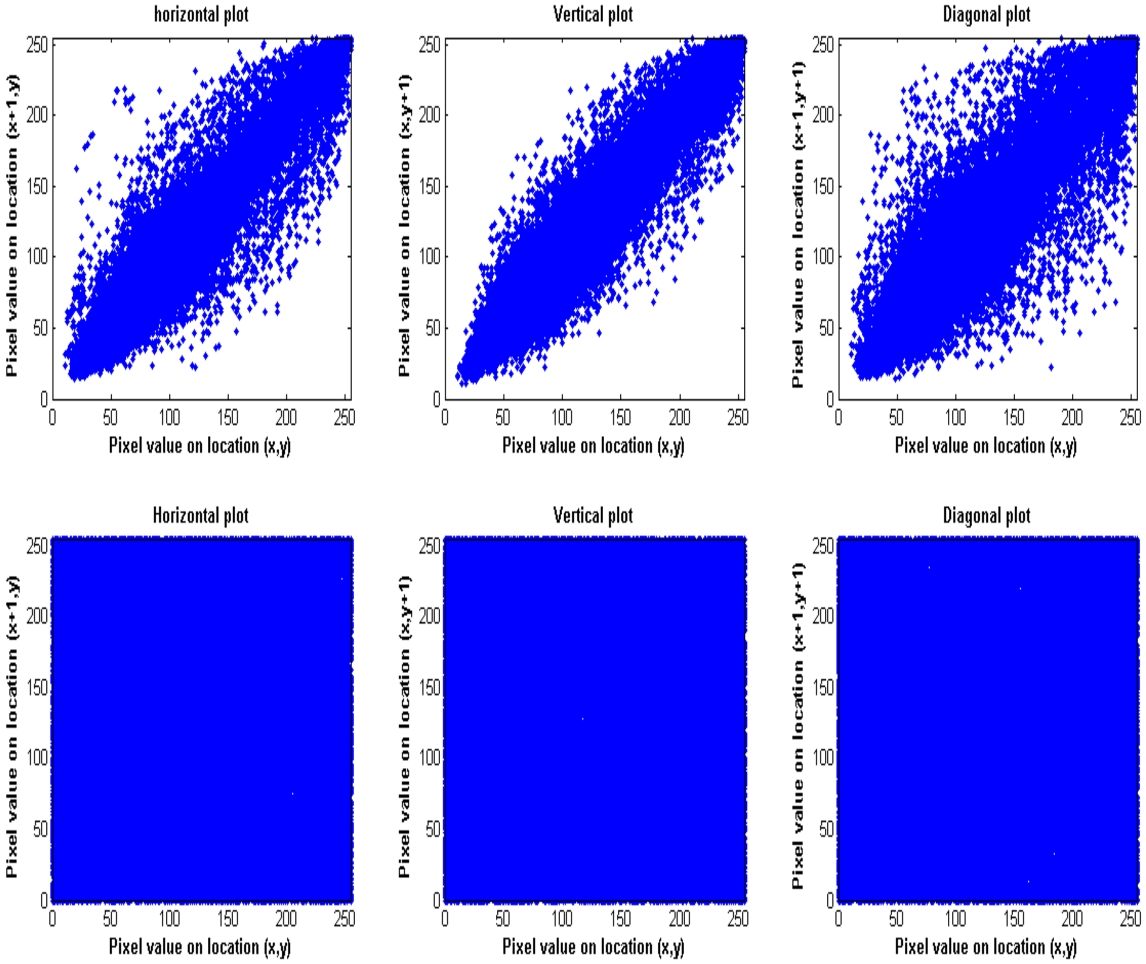
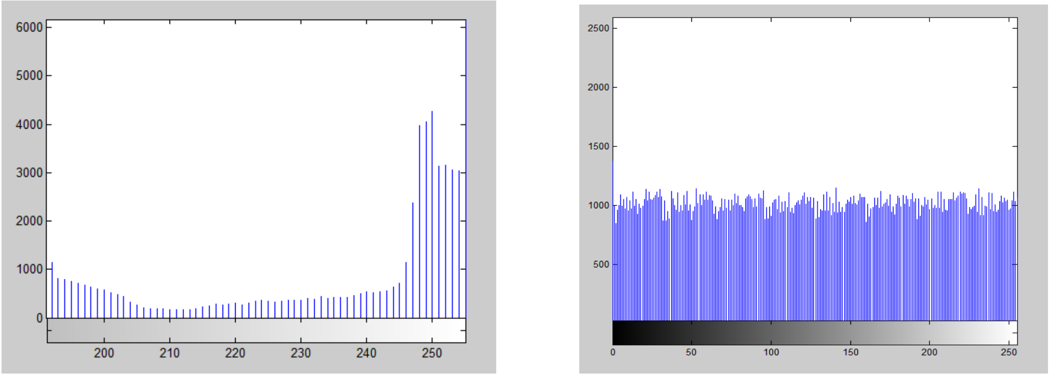


Fig. 5.2 Correlation of adjacent pixels of Original [Top] and Cipher images [Bottom]

For the source image the histogram is concentrated around particular gray level intensity range. The histogram of the source and encrypted images shown in Fig. 5.3 substantiates the fact that the proposed algorithm is robust against statistical attack. Each gray level in the encrypted image has equal probability of occurrence thus making reconstruction of the source image difficult.



(a) (b)

Fig. 5.3 Histogram of (a) Original Image (b) Cipher Image

The NIST statistical test suite results are shown in Table 5.2.

Table 5.2- NIST Statistical Test Suite Report

| TEST | PV | PP |
|---|---|---|
| Block frequency | 0.122325 | 9/10 |
| Cumulative sums | 0.350485 | 9/10 |
| Runs | 0.122325 | 10/10 |
| Longest run | 0.739918 | 10/10 |
| Rank | 0.213309 | 10/10 |
| FFT | 0.122325 | 9/10 |
| Serial | 0.017912 | 10/10 |
| Universal | 0.122325 | 9/10 |
| Approximate entropy | 0.28431 | 8/10 |
| Random excursion | ---------- | --- |
| Non-overlapping template | 0.534146 | 10/10 |
| Overlapping template | 0.74435 | 9/10 |
| Random excursion variant | 0.350485 | 10/10 |
| Linear complexity | 0.017912 | 9/10 |
| Final result | SUCCESS | |

## 5.4 CONCLUSION

In this section, a new block image encryption scheme based on Cat map with permutation–diffusion architecture is proposed. In the permutation process, we use Arnold cat map and dynamic random growth technique to confuse the original image to keep the advantages of fast encryption of cat map, but to eliminate its drawback of periodicity. In the diffusion section, we scramble the subimages followed by a ring shift operation of the image pixels. Since cat map is periodic and can be easily cracked by chosen plaintext attack, we use cat map in another securer way, which can completely eliminate the cyclical phenomenon and resist chosen plaintext attack. The performance analysis results show that the proposed image encryption scheme can resist brute-force attack, statistical attack and differential attack. So it can be used in image transmission on the Internet.

# CHAPTER 6

# CONCLUSION & FUTURE WORK

## 6.1 CONCLUSION

The project work involved the implementation and analysis of three novel encryption cryptosystems to address the issue of secure image transmission in real time systems. Chaos based logistic sequences were used because of their non-periodic nature to enhance the encryption quality of the algorithms. Each algorithm devised is suitable for encryption of large and high dimensional images and data sets. Performance analysis results show that the encrypted images are resistant to brute force attack, statistical and differential attacks. Hence, these cipher outputs are suitable for use in image transmission systems and other secure multimedia applications.

## 6.2 FUTURE WORK

Future work involves extending the algorithms to video data and also focussing on the effect of multi-fractal images on the entropy and encryption quality. We are also looking to explore the scope of the algorithm for data sets characterized by multiple measurements and higher dimensions such as biomedical images etc.

## REFERENCES

1. Aloha Sinha, Kehar Singh (2010), “A technique for image encryption using digital signature”, Optics Communications, Vol-2 I 8 (2203), pp.229-234.

2. Chen, T.-H., Wu, C.-S (2010), “Compression-unimpaired batch-image encryption combining vector quantization and index compression”, Inform. Sci. 180, pp.1690–1701.

3. Ephin M, Judy Ann Joy and N. A. Vasanthi (2013), “Survey of Chaos based Image Encryption and Decryption Techniques”, Amrita International Conference of Women in Computing (AICWIC’13) Proceedings published by International Journal of Computer Applications (IJCA).

4. Hegui Zhu, Cheng Zhao, Xiangde Zhang (2013), “A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem” , Signal Processing: Image Communication 28, pp.670–680.

5. Hoffstein, J., Pipher, J., Silverman, J.H (2008), “An introduction to mathematical cryptography” (Springer).

6. Hongjun Liua, Abdurahman Kadirb, Yujun Niud (2014), “Chaos-based color image block encryption scheme using S-box”,International journal of electronics and communicationsInt. J. Electron. Commun. (AEÜ) 68, pp.676–686.

7. Jiun-In Guo, Jui-Cheng Yen (2000), “A new mirror-like image Encryption algorithm and its VLSI architecture”, Pattern Recognition and Image Analysis, Vol.2, pp.236-247.

8. John Justin M, Manimurugan S (2012), “A Survey on Various Encryption Techniques”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1.

9. Juneja, M., Sandhu (2009), “Designing of robust image steganography technique based on LSB insertion and encryption”. Proc. Int. Conf. Advances in Recent Technologies in Communication and Computing, Kottayam, Kerala, India, pp. 302–305.

10. Jun-xin Chen, Zhi-liang Zhu, Chong Fu, Hai Yu, and Li-bo Zhang (2008), “A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism”, Communication Nonlinear Sci Numer Simulation.

11. Li HJ, Wang YR, Yan HT, Li LB, Li QZ, Zhao XY (2013), “Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform”, Opt Lasers Eng 2013; 51(12):pp.1327–1331.

12. Maniccam, S.S., Bourbakis, N.G. (2001), “Lossless image compression and encryption using SCAN”, Pattern Recognition 34, pp.1229- 1245.

13. Radwan, A.G., Abd-El-Hafiz, S.K., Abdel-Haleem, S.H (October 2012), “Image encryption in the fractional-order domain”, Proc. Int. Conf. on Engineering and Technology, New Cairo City, Egypt, pp. 1–6.

14. Ranjan B (2005), “Novel Public Key Encryption Technique Based on Multiple Chaotic Systems”, Physical Review Letters, 2005(26):098702.

15. Rhouma, R., Belghith, S. (2008), “Cryptanalysis of a new image encryption algorithm based on hyper-chaos”, Phys. Lett. A 372 (38), pp.5973–5978.

16. Srividya G, Nandakumar P (Feb 2011), “A triple-key chaotic image encryption method”. In: International conference on communications and signal processing (ICCSP), Kerala, India; 10–12, pp. 266–270.

17. Wang, X., Wang, X., Zhao, J., Zhang, Z (2011), “Chaotic encryption algorithm based on alternant of stream cipher and block cipher”, Nonlinear Dyn., 63, (4), pp. 587–597.

18. Zhang, L., Liao, X., Wang, X. (2005), “An image encryption approach based on chaotic maps”, Chaos Solitons Fractals 26, pp.759–765.

19. Zhang YQ, Wang XY (2014), “A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice”, Inf Sci 2014; 273(20):pp.329–51.