Design Of Superior Colour Image Cryptosystem Using Chaotic Maps and Mathematical Transforms

[1] Renuka Patel, [2] Ankit Temurnikar, [3] Dr. Teerath Prasad Patel,
[4] Rohit Singh Thakur

[1]Computer Science Department, Madhyanchal Professional University, Ratibad, Bhopal (M.P.) India
[2] Assistant Professor, Computer Science Department
Madhyanchal Professional University, Ratibad, Bhopal (M.P.) India
[3] Department Of Computer Science Govt. College Narela Bhopal (Mp)
[4] Ravindra Nath Taigore University, Bhopal (Mp)

E-Mail:[1] renukapatelmca@gmail.com;[2].ankit.temurnikar@gmail.com; [3] teerath.patel@gmail.com
[4]rohitthakur_2006@rediffmail.com

Abstract: This paper presents an improved encryption algorithm for colour images based on chaotic system. First, the chaotic sequences generated by chaotic system, using encryption system randomly generated a set of keys, and then using the keys to scramble the image pixel position and pixel values, which is a good way to avoid the key sequence unchanged of the HIE encryption. To against attack, the algorithm encrypted in a way of one time one keys. In addition, the paper diffused encrypted three colour components RGB of a picture to avoid the drawbacks of breaking one of the components can know the all plaintext messages. Experimental results show that the proposed algorithm has good encryption and anti-jamming performance. Data transfer has become an integral part of our lives in the digital age and is increasing at an enormous pace. However, over public network like internet is susceptible to various online threats, including identity theft, infections, or attacks. So, it is extremely important to ensure the security and integrity of our data, whether it is in the form of a simple text, colour image file. Research paper on cryptosystems for colour image encryption, compression models using mathematical transforms use of chaotic colour image. The proposed cryptosystems use affine and Arnold transforms as scrambling techniques to introduce chaos in the images, whereas random decomposition and decomposition are used for matrix factorization. Decomposition are proposed in the subsequent paper these schemes are the generalizations of the colour image encryption schemes to encrypt colour image files. To analyse the efficacy, strength and robustness of the proposed systems, key sensitivity, histogram and colour image analysis, noise, occlusion and special attack analysis have been performed"

Keywords: Mathematic, Mathematics Interdisciplinary Application, chaotic system, Physical Science.

Introduction

This paper focuses on a new image scrambling algorithm which introduces a new chaotic system. Image scrambling wing chaotic properties is an application for providing security to the images from getting into the hands of unauthorized user. The proposed image scrambling scheme generates the permuting address codes by sorting the chaotic sequence directly. This paper analysed that the scrambling performance of the new algorithm is statistic. The conclusion of this paper indicates that the new algorithm can provide a high level security. The paper results in good performance of the proposed algorithm that can also be applied in the real-time applications and digital communications as it is a straightforward mechanism and easy to implement. The rest of the paper is organized as follows: proposed chaotic system in method, image scrambling algorithm based on chaos theory in colour image in chaotic system, experimental details and results are analysed in matrix of row and column combination. The paper is observed by a conclusion in result and summary.

Recently, security of multimedia data is receiving more and men attention due to the transmission over vicious communication networks. In order to protect personal information, many image encryption algorithms are designed and proposed such as two-dimensional cellular automata based method [21, Henon chaotic map [4].Cher's hyperchaotic system [12].Arnold transform [3, 4]. Chaotic functions are blessed with properties like sensitivity to the initial conditions, and ergodicity which make them very desirable for encryption [1] Image scrambling is one of the methods for securing the image by scrambling it into a disordered one beyond cognition, making it hard for those who get the image in unauthorized manner to extract information of the original image from the scrambled images. Further, image scrambling technology depends on data hiding technology which provides non-password security algorithm for information hiding. Now, the mainly used three kind of image scrambling types are scrambling in the space domain, scrambling in the frequency domain, and scrambling in the colour or domain, a great quantity of all kind of image scrambling algorithms, the Image scrambling algorithms based on chaos have attracted more and more attention since they can provide a.

The advent of digital technologies has provided a handy and user-friendly platform to individuals as any information needed to be shared is just a click away. The digital information or data comprises various types of files, whether text or images. However, data sharing over a public network is not always secure as the attacker may modify or destroy data partially or completely. Thus, it is needed to protect our data from unauthorized users. Data security includes protecting files containing text, image etc. by adopting techniques depending on the importance of datasets, their sensitivity, and regulatory compliance requirements and then applying appropriate protection to secure those resources. The core elements of data colour image security are confidentiality, integrity, authentication and non-repudiation.

Objectives of the Research

The main objectives of the present research work Sensitivity to initial conditions of chaotic system means that each point in a chaotic system is arbitrarily closely approximated by other points with significantly different future paths, or trajectories That, an arbitrarily small change, or perturbation, of the current trajectory may lead to significantly different future behaviour. The next figure compares the time series for two lately different initial conditions. The two time series stay close together for about 2 iterations. But after that, they are pretty much on their own.

Pertaining colour image colour encryption systems using mathematical transforms and matrix decomposition techniques. Compression models are also presented to enhance the integrity and easy transfer of the data. The major objectives of the current research work are to design: A cryptosystem for binary and colour digital images using pixel scrambling technique and canonical transforms. Colour image enciphering scheme using the random modulus decomposition. A scheme for double colour image encryption and compression using matrix decomposition technique. A cryptosystem for encryption is using digital image techniques.

These elements should be kept in mind while designing a cryptosystem to keep our sensitive data protected from unauthorized access and data exfiltration. Encrypting data before transmission and storage is an efficient way of handling data. Various encryption schemes have been developed over decades, and they are broadly classified into two categories: symmetric and asymmetric encryption schemes [1]. The name derives from whether or not the same keys are used for encryption and decryption. are the same as decryption keys. It is therefore critical that a secure method is adopted to transfer the keys between the sender and the recipient.

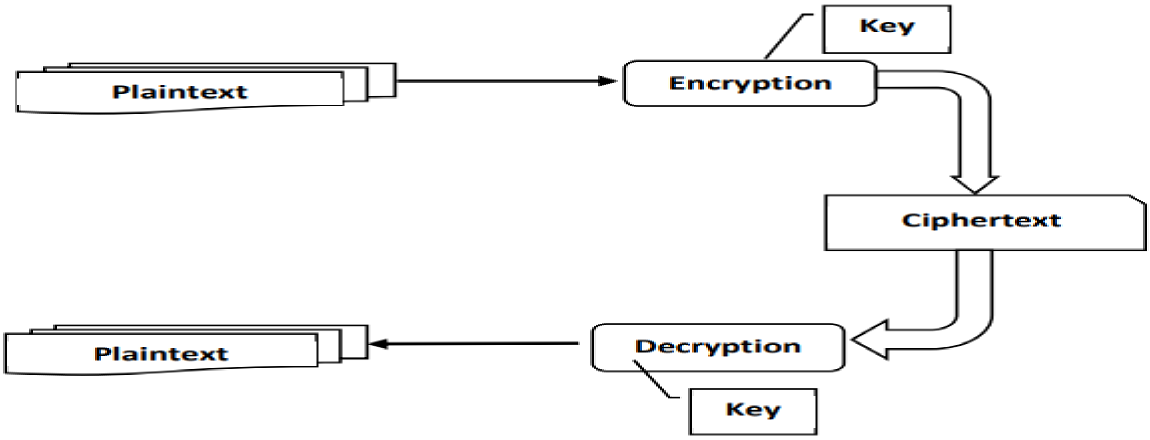


Figure 1.1: Symmetric cryptosystem

Asymmetric encryption uses the concept of a key pair: a different key is used for the encryption and decryption process. One of the keys is the private key, and the other is the public key. The private key, as the name suggests, is kept secret by the owner and the public key is made available to the public at large method. be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorized or unlawful access to the data.

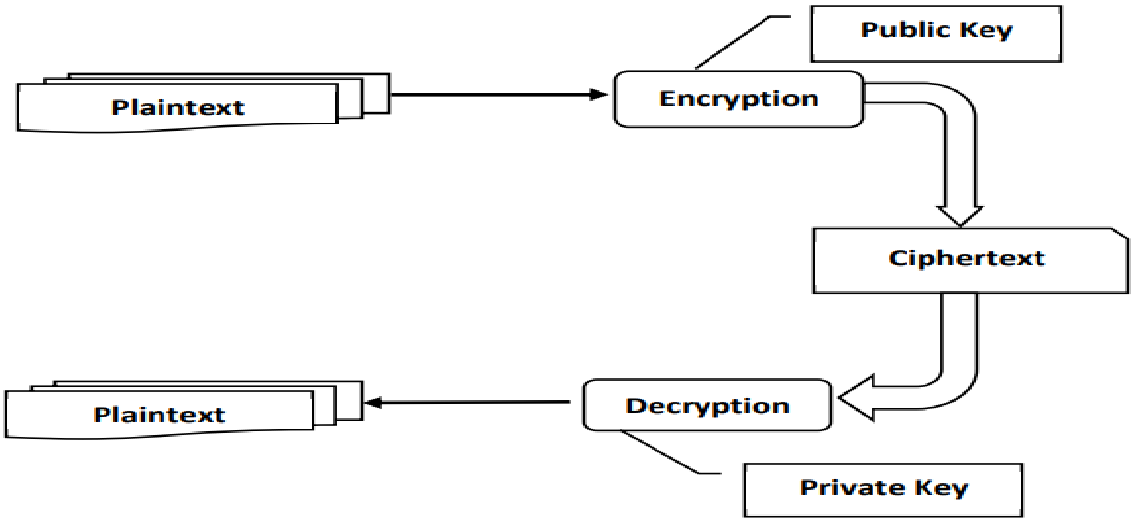


Figure 1.2: Asymmetric cryptosystem

Researchers have introduced various encryption schemes based on these two types of methods. These encryption schemes need to be analysed against various cryptographic attacks to better understand the cryptosystems and to improve the system by finding any Dutch cryptographer Auguste Kerkhof's at the end of the nineteenth century. The different types of cryptographic attacks mentioned in the literature are explained below:

Ciphertext only attack access only to a set of ciphertext(s) but does not have access to the corresponding plaintext(s). is said to be successful when the corresponding plaintexts can be determined from a given set of ciphertexts. Occasionally, the encryption key can be determined from this attack.

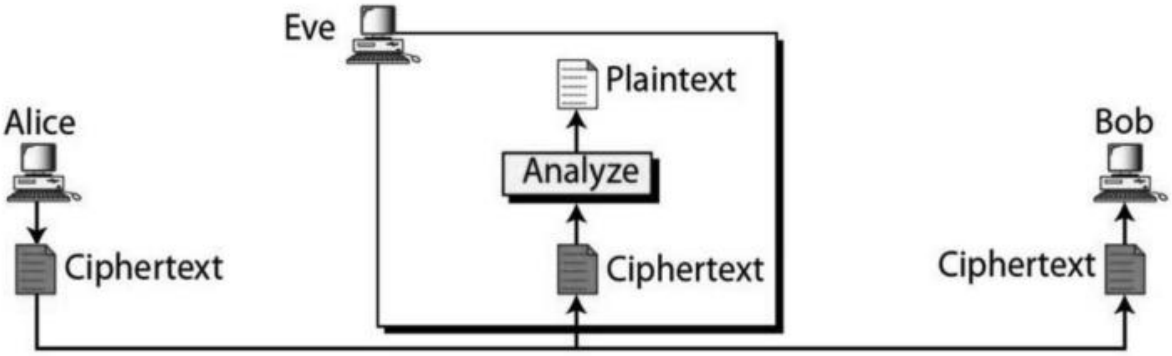


Figure 1.3: Ciphertext only attack

Known-plaintext attack, the encryption key is obtained from one or more known plaintext-ciphertext pairs, and then this key is used to decrypt other ciphertexts encrypted with the same key. In colour image cryptosystems, the phase retrieval algorithms are implemented to formulate .He double random phase encoding is vulnerable to this attack using phase retrieval algorithms. Apart from the phase retrieval technique, Simulated Annealing heuristic algorithm can also be implemented to obtain the keys, given that the plaintext and corresponding ciphertext pair are known.

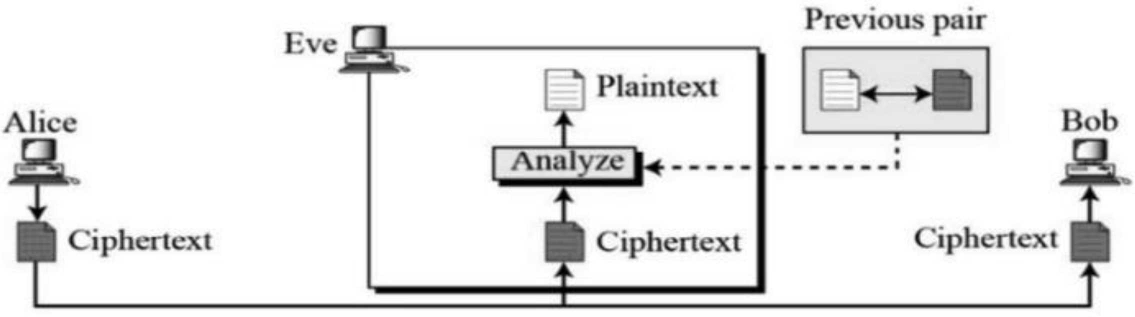


Figure 1.4: Known-plaintext attack

chosen plaintext attack. In this attack (Figure 1.4), the attacker has access to the encryption system. He can choose the plaintexts of his/her choice and get the corresponding ciphertexts. This is an active model where the attacker actually gets to choose the plaintext and do the encryption. Being able to choose any plaintext and observing the ciphertext gives the attacker a strong foothold into the inner working of the algorithm and secret key. An example of this attack is differential cryptanalysis applied against block ciphers as well as hash functions. A well-known public-key cryptosystem, is also vulnerable to chosen-plaintext attacks. In colour image cryptosystems, is applied by choosing impulse functions as plaintexts and then obtaining the corresponding ciphertexts to further retrieve the keys.

New chaotic system: Recently, introduced a new chaotic system, which is described by the following nonlinear differential equation:

$$x_1 = \mathrm{a}x_1 - x_2x_3$$
$$x_2 = \text{-b}x_1 + x_1x_3$$
$$x_3 = \text{-c}x_3 + \frac{1}{3}x_1x_2 \quad . \quad . \quad . \quad . \quad . \quad (1)$$
$$W = cx$$

Where: $x_1, x_2 \; and \; x_3$ are the state variable and a, b and c are positive constants
C = (100)
W = is the system measured output.
When a = 5.5, b =11 and c = 4, the system (1) is chaotic.

Basic transforms:

Fourier transform :

The Fourier transform converts a function of time into a complex-valued function of frequency, whose absolute value gives the total frequency present in the original signal, and the complex argument gives the phase offset of the basic sin odd rule in that frequency. That is why the Fourier transform is called the frequency domain representation of the signal. Show the results of the Fourier transform on the image Lena. Similarly, the inverse Fourier transform is defined as the reverse of the Fourier transform. Inverse Fourier transform gives the original function back from the frequency function. Mathematically, the Fourier transform is given by the following equation:

$$\hat{f}(x) = \int_{-\infty}^{\infty} f(t)\, e^{-2\pi ixt} dt, \text{ for any real number } x. \qquad (1.1)$$

The inverse Fourier transform is given by:

$$f(t) = \int_{-\infty}^{\infty} \hat{f}(x)\, e^{2\pi ixt} dx, \text{ for any real number } t. \qquad (1.2)$$

Fractional Fourier transform:

Fractional Fourier transform [2] is from a family of linear transformations which transform a function to any intermediate domain between time and frequency. It generalizes the Fourier transform.

The $Frft$ of order α of a function $f(z)$ is defined as:

$$F^{\alpha}\{f(z)\}(u) = \int_{-\infty}^{+\infty} K_{\alpha}(z,u) f(z) dz \qquad (1.3)$$

where the kernel function K_{α} (z, u) is expressed as

$$K_{\alpha}(z,u) = \begin{cases} A \exp\left[i\pi(z^2 \cot\theta - 2zu \csc\theta + u^2 \cot\theta)\right], & \alpha \neq n\pi; \\ \delta(z-u), & \alpha = 2n\pi \\ \delta(z+u) & \alpha = (2n+1)\pi \end{cases} \qquad (1.4)$$

Here $A = \frac{\exp[-i(\pi\,\mathrm{sgn}(\theta)/4 - \theta/2)]}{\sqrt{|\sin\theta|}}$ and $\theta = \alpha\pi/2$. The kernel function is expressed

using the direct delta function if is an integer multiple. In the case of order , becomes the full Fourier transform, and it becomes the identity transform for The inverse of fractional Fourier transform of order is obtained by taking the order of shows the results of the 2-dimensional fractional Fourier transform of an image Fresnel transform Fresnel transform [3]

Linear canonical transform :

A is a class of linear integral transform with three parameters. The Fourier transform, fractional Fourier transform, and the Fresnel transform are all special cases where fractional orders in fractional Fourier transform, and the wavelength and propagation distances in Fresnel transform act as additional keys. Mathematically, it is defined by the following equation:

$$I_{\alpha,\beta,\gamma}(u,v) = LCT_{\alpha,\beta,\gamma}\{I(x,y)\}(u,v) = \exp\left\{\frac{-j\pi}{4}\right\}\sqrt{\beta}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} I(x,y)\exp\{\alpha(x^2 + y^2) - 2\beta(xu + yv) + \gamma(u^2 + v^2)\}\,dxdy \qquad (1.7)$$

Here, are the transform parameters which are real and independent and domains.

Basic decomposition techniques:

Lower-Upper decomposition (LU):

The lower-upper decomposition, also known as decomposition, is a matrix decomposition technique in which a non-singular square matrix is decomposed into two triangular matrices; one is an upper triangular matrix while the other is a lower triangular matrix. In general, the decomposition of a matrix is given by:

$$\begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} \times \begin{bmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{bmatrix} = \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ l_{n1} & \cdots & 1 \end{bmatrix} \times \begin{bmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & u_{nn} \end{bmatrix}$$

= P×M = L×U

Here, is the matrix of order which is decomposed, in permutation matrix of order is the lower triangular matrix with diagonal entries equal to 1, and is the upper triangular matrix, respectively. The product in the order where is pre-multiplied with matters as the results will be incorrect if the order of multiplication is changed. To demonstrate this decomposition, a digital colour image of Cameraman of size pixels is considered for the simulation shows the results of decomposition on the image of the Cameraman.

Decomposition with column pivoting:

Orthogonal-triangular decomposition or decomposition with column pivoting is a matrix factorization technique in which a given matrix with linearly independent columns is decomposed to give an orthogonal matrix, an upper triangular matrix and a permutation matrix. In case the matrix is a complex matrix, the decomposition gives a unitary matrix instead of the orthogonal matrix. Mathematically, it can be represented as

$$\begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} = \begin{bmatrix} q_{11} & \cdots & q_{1n} \\ \vdots & \ddots & \vdots \\ q_{n1} & \cdots & q_{nn} \end{bmatrix} \times \begin{bmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & r_{nn} \end{bmatrix} \times \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix}^{-1}$$

$$Im = Q \times R \times P^{-1}$$

To demonstrate this decomposition, a colour image of Lena of size pixels is considered for simulation. shows the corresponding results of the decomposition with column pivoting of the image Lena and it also shows the orthogonal matrix, upper triangular matrix and permutation matrix corresponding to the given colour image shows the results of decomposition on the image of the Cameraman. (a-h) are (a) input image: Lema. The product and in the order where is pre-multiplied with is shown in Figure (f). Here, the order of the multiplication matters as pre-multiplying will lead to incorrect results, as shown in shows the retrieved image by post-multiplying.

Compressed sparse row (CSR) :

CSR [8] is a compression technique used to compress sparse matrices.

Suppose $I=\begin{bmatrix} e_1 & 0 & 0 & 0 \\ 0 & e_2 & e_3 & 0 \\ 0 & 0 & e_4 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ is a sparse matrix that is to be compressed. *CSR* method gives a 3-column compression for this matrix. These three columns are obtained using the following steps.

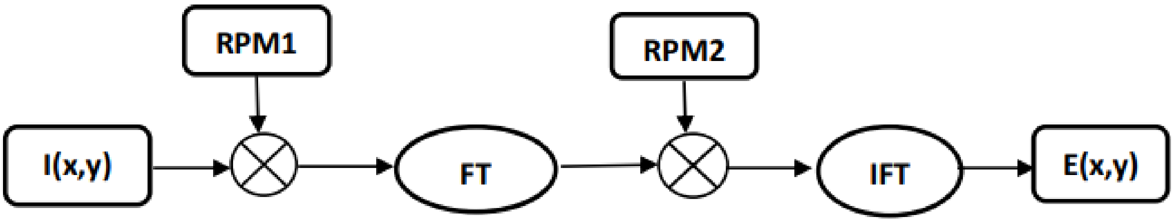
First, write all the non–zero entries of matrix '*I*' from left to right and top to bottom in a column vector, say '*V*'.

is now represented by three columns and having a total of 13 elements. V =[e_1 e_2 e_3] [1 2 3] , [0 1 4 3], [0 0 1 4] from and allocate the rows for the non-zero entries using . Since the first entry in tells the number of non-zero elements in the zeroth row (here, the row numbers are starting from zero, first, and so on). The third entry tells the number of non-zero elements in the zeroth row and first row, and so on. After that, the entries in the vector allocate the columns to the non-zero elements, and this way, the original sparse matrix is retrieved back from these three columns.

Basic encryption techniques

This section provides the basic encryption structures like double random phase encoding [9] and phase truncated Fourier transform [10], which are the basis for almost every based encryption system. In addition to these schemes, some more basic cryptosystems using eq.-1

- ✓ **Double random phase encoding:**



Here, denotes the input image, and is the corresponding encrypted image obtained using the following steps: Step-1: The input image is bonded with a random phase of colour image Here, is a random matrix of the size of the input colour image and possesses values in the interval **[0 1]**

The following steps show the complete process of encryption using symmetric. represents the Fourier transform operation. Here, and denote phase truncation and phase reservation operations, respectively. In operation, the phase part is discarded, and the magnitude part is preserved, whereas in the operation, the magnitude part is discarded, and the phase part is preserved, which yields decryption keys**.**

Entropy:

The degree of randomness in an image is measured by its entropy value [14]. As the level of randomness increases, the entropy rises, and events become less predictable. The minimum value of entropy is zero, and it indicates the constant value of pixels in any location. For an image, the maximum value of entropy depends on the number of colour image scales. Entropy is given by the following formula: where denotes the pixel values is the probability of the pixel value. Therefore, an image with 256 colour image scales has a maximum entropy value. The maximum value indicates that the pixel values are uniformly distributed in an encrypted image with a higher entropy value indicates a better quality of encryption.

Large key space:

A key space is the set of all valid, possible, distinct keys of a given cryptosystem. The security of any cryptosystem is proportional to the size of its key space. A cryptosystem with a larger key space is more resistant to attackers as a larger key space has an increased Brute force search time.

Key sensitivity:

A scheme is considered secure if it is susceptible to its encryption parameters and keys. That means a slight change in the parameter must yield completely ambiguous results. Key sensitivity analysis must be carried out for each key separately for a cryptosystem to analyse its strength.

Low time complexity:

It is again an important quality metric for any cryptosystem. A cryptosystem with high computational time is not considered good for practical applications. Therefore, a scheme must have low time complexity.

Image Encryption and Compression:

Data transmission over a public network is always prone to contamination, theft and manipulations. A safety mechanism must be followed to protect it from intruders and attackers. There are plenty of such safety mechanisms, which are reported in the literature like advanced encryption standard [29], data encryption standard [30], algorithm [31] etc. These algorithms have been investigated extensively by researchers for possible loopholes in them. Owing to the large size of colour images, it has also been found that these cryptosystems are slow for colour images. So, this limitation compelled researchers to evolve fast encryption mechanisms that can do parallel processing and design a suitable algorithm to cope up with the changing trends in cryptanalysis. The very first successful attempt to design such a cryptosystem is credited to [9]. They proposed double random phase encoding. An Optical colour image encryption technique that can be implemented digitally. It uses two random phase masks to give a stationary white noise as an encrypted image. Thus, this based cryptosystem paved the way for researchers to propose more cryptosystems. Subsequently, has been further enhanced by using fractional Fourier transform [2], Fresnel transform [3], amplitude modulation [4], fractional Mellin transform [5], Hartley transform [6], Radial Hilbert transform [7] etc. However, the scheme was soon observed to be symmetric and linear; thus, it was assailable. It is vulnerable to chosen-plaintext [8], chosen-ciphertext [7], and known-plaintext [5] attacks. This issue was resolved when Qin and Peng [10] proposed an asymmetric and non-linear scheme based on phase truncated Fourier Transform ( ), in which amplitude and phase truncation operations were implemented. In cryptography, an asymmetric cryptosystem uses the concept of public and private keys. In Qin and Peng's model, the keys used for encryption and decryption are different. Therefore, it is also termed asymmetric. This phase truncation-based asymmetric cryptosystem paved the way for researchers to introduce various based cryptosystems [14-15]. Later, it was found that this scheme is also vulnerable to specific attacks and their variants [30-31]. Thus, a new approach was needed which could preserve the non-linearity and endure the special attack. In 2015, Cai et al. [26] proposed a new scheme based on coherent superposition and equal modulus decomposition. Unlike based cryptosystems, this based cryptosystem generates two equal moduli masks: one acts as ciphertext and the other as a private key. Later on, several based cryptosystems were reported in the literature. Some of them used multiple fractional Fourier transform with different orders [26], in the gyrator domain [14], cascaded [8] etc. However, the cryptanalysis of this scheme reveals its vulnerability to iteration-based attacks [7] because the public key has the same phase as that of the mask used in encryption. Wang et al. [7] proposed a cryptosystem in 2016, an alternative to based cryptosystem. Their scheme is based on random modulus decomposition (RD), and provides better security than equal modulus decomposition. In approach, two complex-valued masks of random moduli were produced from the Fourier transform of the image. Unlike does not convey any information about the amplitude of the private key.

Researchers have also developed cryptosystems which involve implementation of pixel scrambling techniques like affine transform and Arnold transform [15-19]. Singh et al. [19] proposed a scheme for colour image encryption using the fractional Hartley and affine transform in 2017. Shah et al. [17] proposed a novel image encryption algorithm based on affine transformation combined with linear fractional transformation. Liu et al. proposed a double colour image encryption based on Arnold transform and discrete fractional angular transform. Singh et al. [19] proposed image encryption using fractional Hartley transform followed by Arnold transform and singular value decomposition in the frequency domain. These pixel scrambling techniques are used to reduce the correlation between the original image and its encrypted image. In addition, they also increase the key space by providing additional keys.

Digital colour image Encryption:

In today's world, the primary source of communication is digital communication. All sorts of data are being stored and exchanged online, e.g. names and (email) addresses, private colour images, files and bank details. Companies often place confidential files, contract information, and customer data online to make them available to only authorized employees who require access to these data. With the rapid increase in digital media transmission, privacy and identity theft issues have become important; thus, encryption plays a vital role in ensuring digital media is transmitted securely. Over the years, many image security schemes have been proposed which are secure, fast and efficient. But still, there is a lot to explore when it comes to colour image file encryption. Colour image data is widely used as evidence in courts, biometrics, secret business talks, and in other related fields, so it becomes pivotal to secure data against attackers. Researchers have proposed some colour image encryption schemes [8], [7] using scrambling operators. Since a colour image file can be saved as a 2-D array, we can apply colour image enciphering algorithms to colour image files as well. Rajput and Matoba [8] proposed such a kind of voice encryption scheme based on DRPE, which encrypts the colour image data recorded on digital holograms. Similarly,. [9] implemented the DRPE scheme in quantum scenarios to encrypt the colour image data. In addition to it, [9] proposed a speech encryption approach, which is based on the permutation of speech segments using a chaotic Baker map and substitution using masks in both time and transform domains. [1] gave an colour image encryption scheme on the basis of a virtual optics scheme whereby they apply both virtual wavelength and virtual diffraction distance in conjunction with a complex-valued random mask to design multiple locks and multiple keys. [2] proposed a mixture of chaos functions to colour image files. Lima and [3] introduced an colour image data file encryption scheme using cosine number transform. Anjana et al. [9] also proposed a colour image data encryption scheme using Arnold transform with random modulus decomposition. Therefore, Thus a single platform to encrypt colour image files and images has been attempted in the present thesis. The proposed algorithms for colour image data encryption show great adaptability and flexibility as these can also be applied to images for encryption.

Nonsubsampled contourlet transform:

Nonsubsampled contourlet transform (NSCT) is an extension of Contourlet transform (CT) that having shift-invariant feature [16].

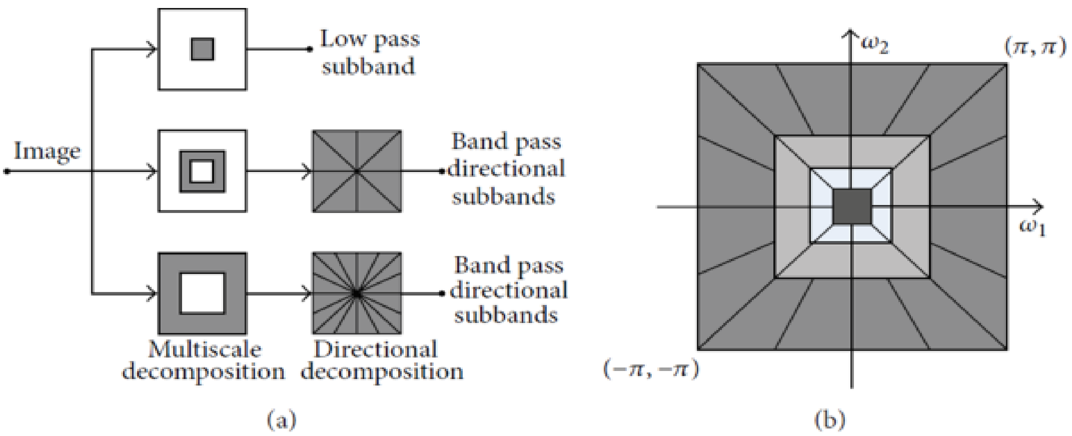
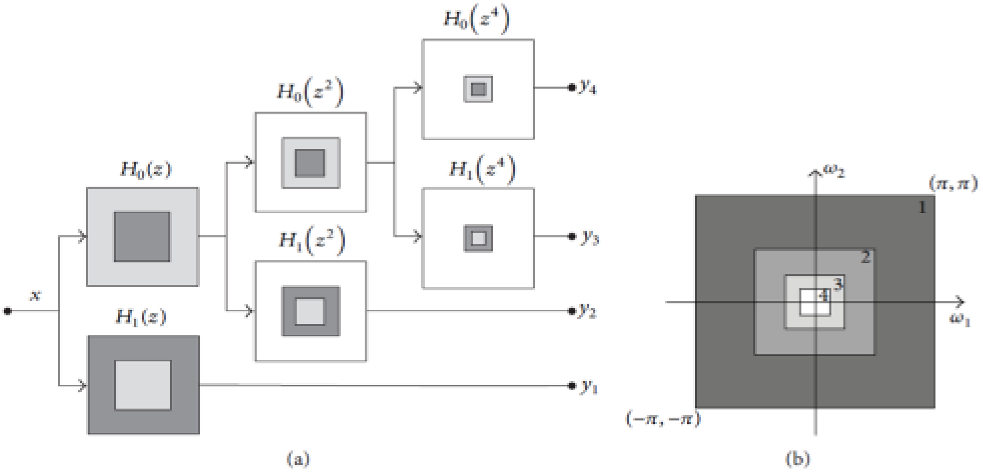


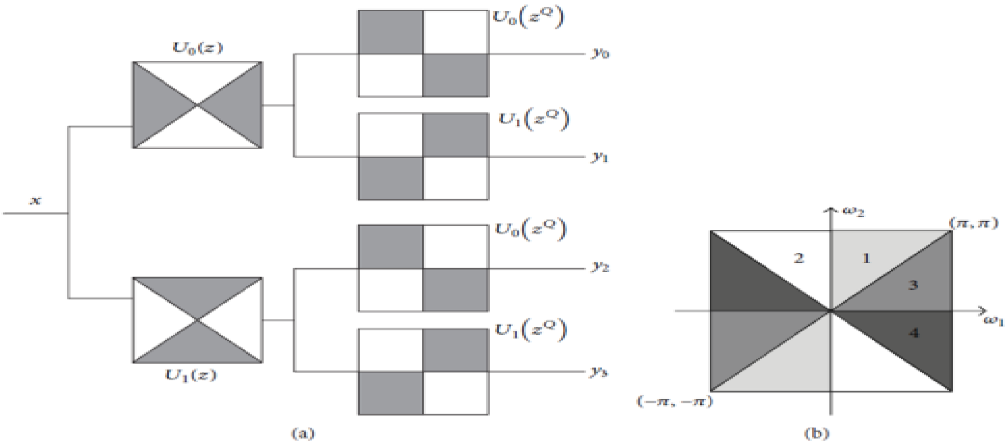
Figure 14.1 (a) shows the Nonsubsampled filter bank (NSFB) structure that implements NSCT. The idealized frequency partitioning obtained using NSFB structure is depicted in the multiscale decomposition feature of CT is achieved by using Laplacian pyramids (LPs). Directional filter banks (DFBs) is used to generate the directional decomposition of CT. LP and DFB utilize down samplers and up samplers, respectively [16]. Therefore, CT is not shift-invariant. NSCT is designed using Nonsubsampled pyramids (NSP) and nonsubsampled DFBs to achieve shift-invariant feature [16].

Here, H_0(z) and H_1(z) represent low and high pass filter at initial level, respectively. k and n represent number of decomposition levels and total number of decompositions of NSCT, respectively. Figure 3.2 (b) shows the prefect frequency of NSP .



Combining NSP and NSDFB :

NSCT is achieved by integrating NSP and NSDFB (see Figure 3.1 (a)). NSP contains multiscale decomposition and captures the point discontinuities. NSDFB has directional decomposition feature. It links point discontinuities into linear structures [26]. NSDFB can be repeated continually on low pass sub-band obtained from NSP. Hence, NSCT is appropriate for image encryption as it provides shift-invariance, multi direction.

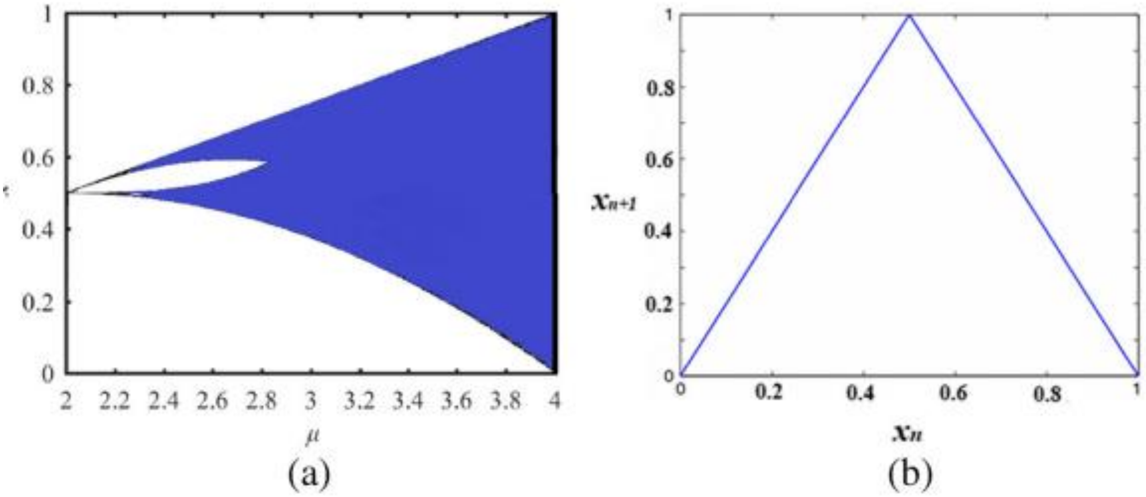


Four-channel NSDFB developed with two-channel fan filter bank (a) Filtering structure and (b) Corresponding frequency partitioning.

Logistic map:

A chaotic system shows deterministic behaviour. It is non-linear in nature. A famous example of one dimensional chaotic map is logistic map [36]. In this system, states change with iterations in a deterministic way. Logistic map is discrete time, one dimensional and non-linear map with quadratic non-linearity [38]. The logistic map colour image has the following state equation:

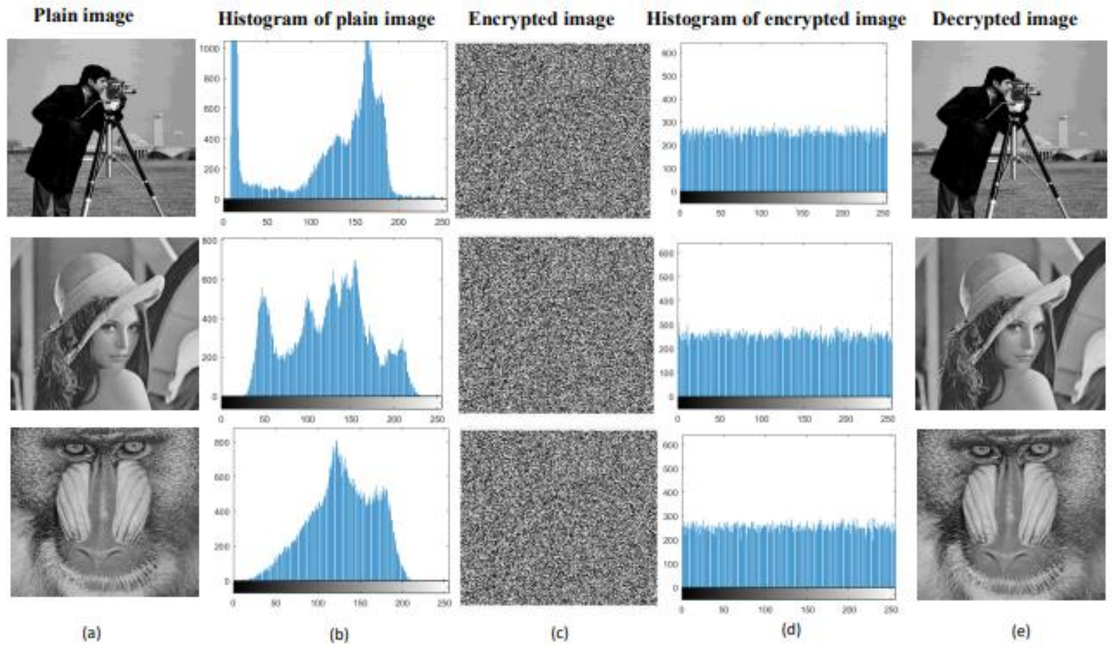
$$x_{n+1} = \begin{cases} r x_n & \text{if} \quad 0 < x_n < 0.5 \\ r(1 - x_n) & \text{if} \quad 0.5 \leq x_n < 1 \end{cases}$$



Visual analysis: show the results obtained on gray and colour images using IGN, respectively. Note that only red channel results of colour images are considered.

[36] Another essential requirement for an image encryption scheme is its highly sensitive behaviour towards its secret keys. For a good encryption system, a single bit modification in secret key gives completely different encrypted result. In this research we have used PWLCM and tent logistic maps. These chaotic maps are highly sensitive to initial conditions and control parameters. If we take a very insignificant change in key or control parameter, the resulting generated random sequence will completely change which in response gives entirely different encryption/decryption results. In Fig. 10 two test images Lena and Peppers are used for key

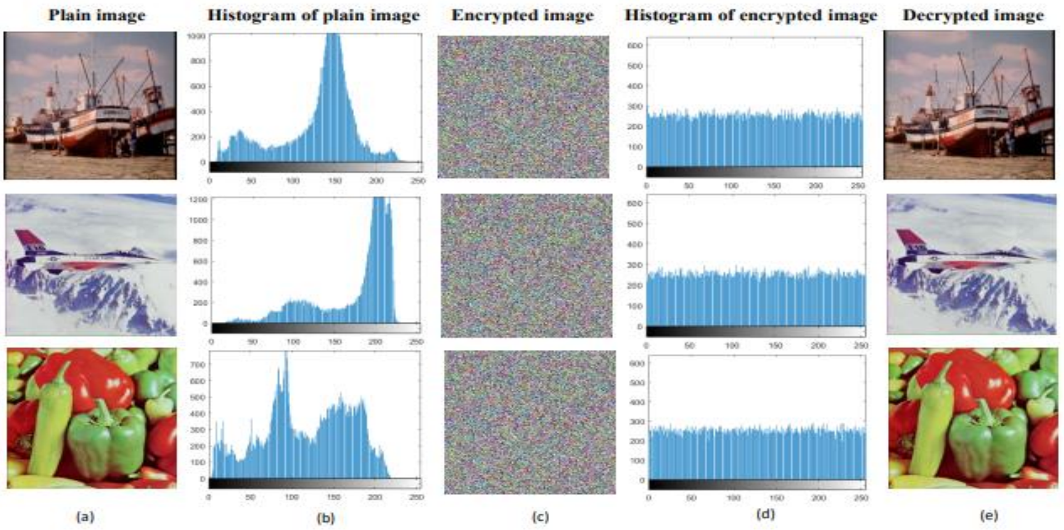
sensitivity analysis. First we encrypt them using key components x0 = 0.76 and m = 0.15 for PWLCM and x0 = 0.479, µ1 = 4.5, y0 = 0.596, µ2 = 6.2, z0 = 0.964, µ3 = 7.9 for tent logistic map. Figure 10c, g show the result of using slightly different key than original key, that is x0 is changed from 0.479 to 0.4790000000000000009.0d, h depict the difference between the encryption results and modified key based encryption results. From these results it is evident that the encryption results are significantly change by taking a minor modification in any of the key component. Distribution of pixels in cipher image histogram shows that how pixels in an image are dispersed.



Colour image and techniques involved for comparison:

IGN has been tested on ten images [7]. The first gray scale images are Cameraman, Lena, Baboon, Pirate, and Woman. The next five colour images are Boat, Airplane, Peppers, House, and Lake. The size of these colour image is 256 × 256. Five well-known meta-heuristic based image encryption techniques such as GA [47], ACO [12], WDICA [12], GDNA [26], and DHS [24] are used for comparison.

Visual analysis of IGN (a) Plain images, (b) Histogram of plain images, (c) Encrypted images, (d) Histogram of encrypted images, and (e) Decrypted images.



Security analysis:

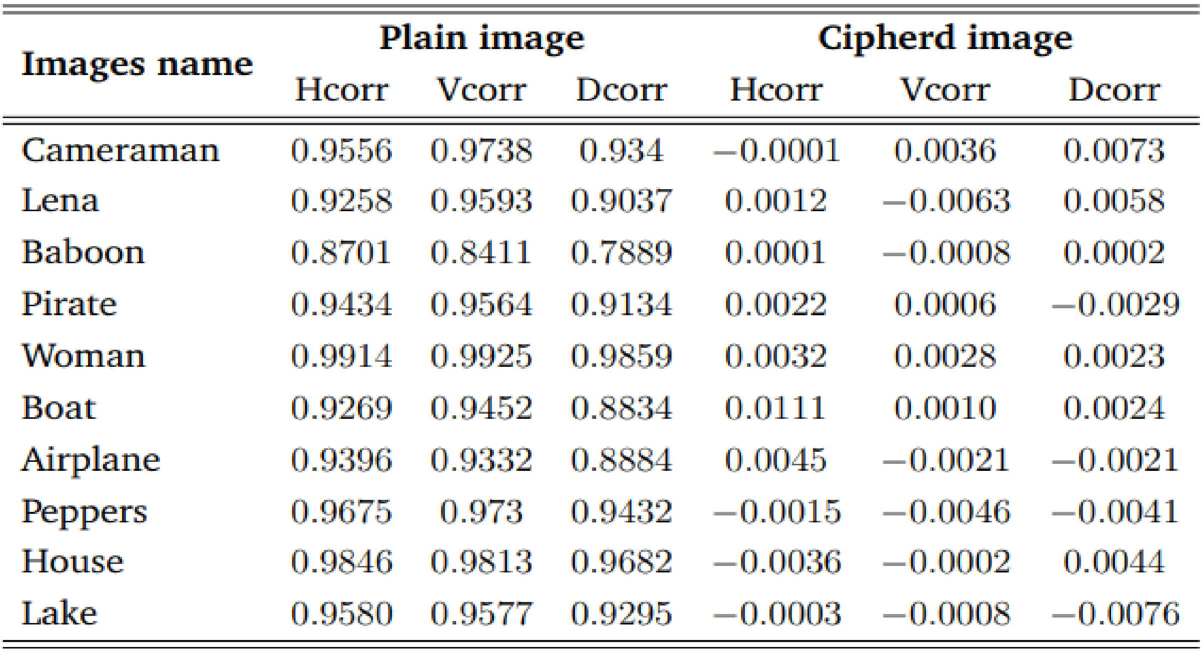
In this section, the security analysis of IGN has been done. The five well-known security analysis namely statistical attack, differential attack, secret key, occlusion attack, and noise attack analyses have been used to test the robustness of IGN.

Histogram analysis: show the histograms of gray plain images and colour image plain images, respectively. Figures 1(d) and 2(d) show the histograms of encrypted gray and colour images, respectively. From Figures 1(d) and 2(d), it is observed that the pixels of encrypted images are uniformly distributed. Thus, it is hard to find out any information from the encrypted images.

Correlation analysis:

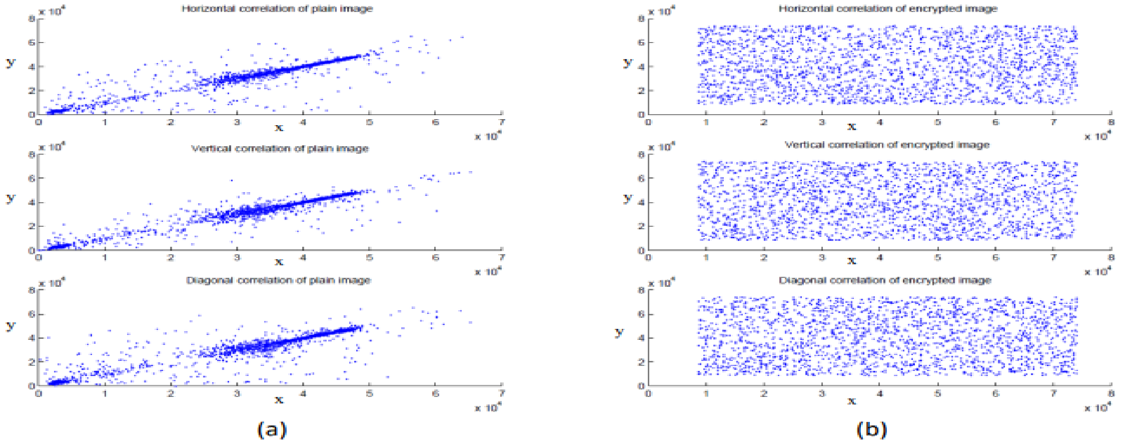
To investigate IGN, the horizontal, diagonal, and vertical correlation between adjacent pixels of input and encrypted image is computed. Depicts Horizontal, Vertical (Vcorr), and Diagonal correlation coefficients of test images and their respective encrypted colour images. It has been observed from that the attacker cannot find any relationship between adjacent pixels to break the algorithm.

Table : Correlation coefficient analysis of IGN



Images name	Plain image			Cipherd image		
	Hcorr	Vcorr	Dcorr	Hcorr	Vcorr	Dcorr
Cameraman	0.9556	0.9738	0.934	−0.0001	0.0036	0.0073
Lena	0.9258	0.9593	0.9037	0.0012	−0.0063	0.0058
Baboon	0.8701	0.8411	0.7889	0.0001	−0.0008	0.0002
Pirate	0.9434	0.9564	0.9134	0.0022	0.0006	−0.0029
Woman	0.9914	0.9925	0.9859	0.0032	0.0028	0.0023
Boat	0.9269	0.9452	0.8834	0.0111	0.0010	0.0024
Airplane	0.9396	0.9332	0.8884	0.0045	−0.0021	−0.0021
Peppers	0.9675	0.973	0.9432	−0.0015	−0.0046	−0.0041
House	0.9846	0.9813	0.9682	−0.0036	−0.0002	0.0044
Lake	0.9580	0.9577	0.9295	−0.0003	−0.0008	−0.0076

Shows horizontal, vertical, and diagonal correlation analysis of plain cameraman's image. It can be seen that the adjacent pixels of a plain colour image are highly correlated with each other. Therefore, it may reveal the statistical information of an image shows the horizontal, vertical, and diagonal correlation analysis of an encrypted cameraman's image. From figure, it can be observed that pixels are seen random [41] in the space which implies that there is no relation among the adjacent pixels. Hence, attacker cannot extract any statistical information from an encrypted colour image. [36] Image histogram shows that how pixels in an image are dispersed. From the above Example 1, Lena image, Fig. 8a is taken as original image, with size (256 × 256). Histograms of its corresponding ciphered image components are shown in Fig. 11a, b, c. From the histogram it is clear that, there does not exist any clue to mount a statistical analysis attack on the encrypted image.



Correlation analysis of IGN (a) Plain cameraman image and (b) Encrypted cameraman image.

Differential analysis:

The sensitivity of IGN towards plain image is tested using differential analysis shows the average and variance values of NPCR and UACI after 30 independent runs. It is observed that the IGN is extremely sensitive towards small change in the plain image and colour image

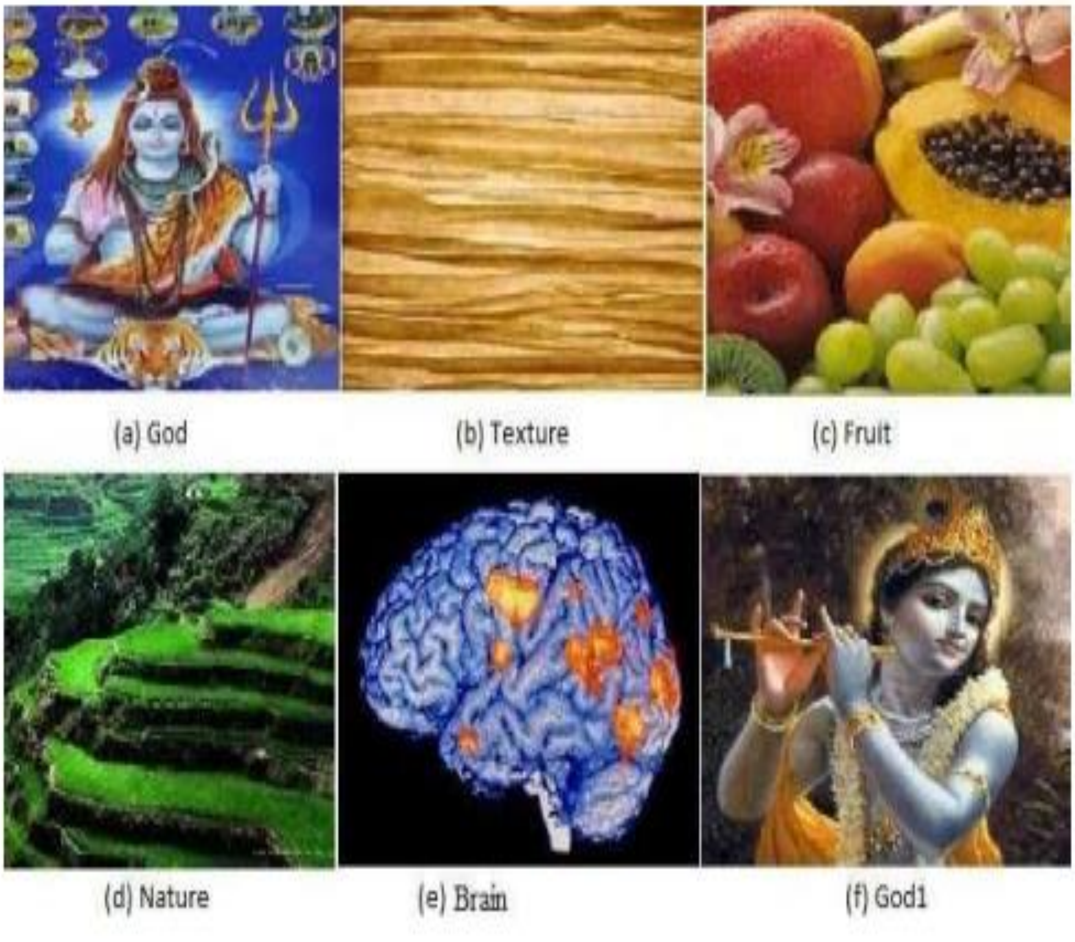
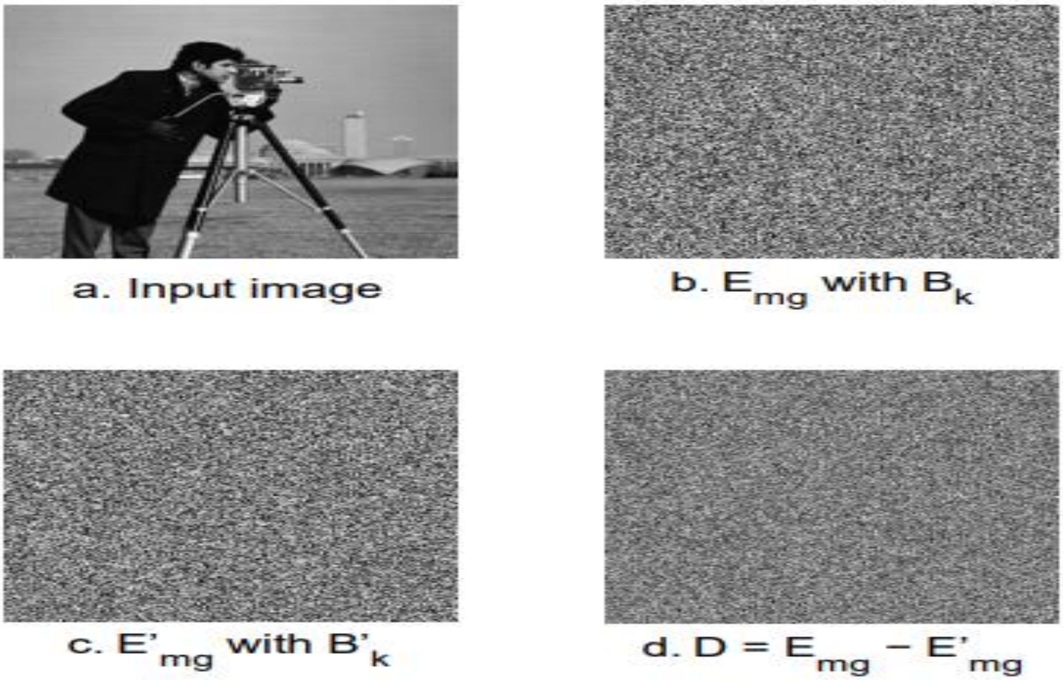


Table 3.3: NPCR and UACI analysis of IGN

Secret key sensitivity: The image encryption technique must be sensitive towards the initial values of secret key. Table demonstrates the difference between E and E_0 .



a. Input image

b. E_{mg} with B_k

c. E'_{mg} with B'_k

d. $D = E_{mg} - E'_{mg}$

To evaluate the sensitivity of secret key, select the input image and generate secret key (Bk). The second secret key (BK_0) is generated with the difference of one pixel. The two encrypted images are generated by utilizing Bk and BK_0 . Finally, the difference between these encrypted images is computed. E and E 0 are two encrypted images of same plain image are generated using different secret keys such as Bk and BK_0 with difference of a single pixel. Table 3.8 shows the difference between E and E 0 using Bk and BK_0 . It can be observed from table that the IGN is extremely sensitive towards initial conditions.

Statistical analysis

In order to resist attacks, the scrambled images should possess certain random properties. To prove the robustness of the proposed algorithm, a statistical analysis has been performed by calculating the histograms and the correlation coefficients for the original image and the scrambled image. For the two images that have been tested, it has been determined (chaotic system) that their quality is good.

CONCLUSION & RESULT

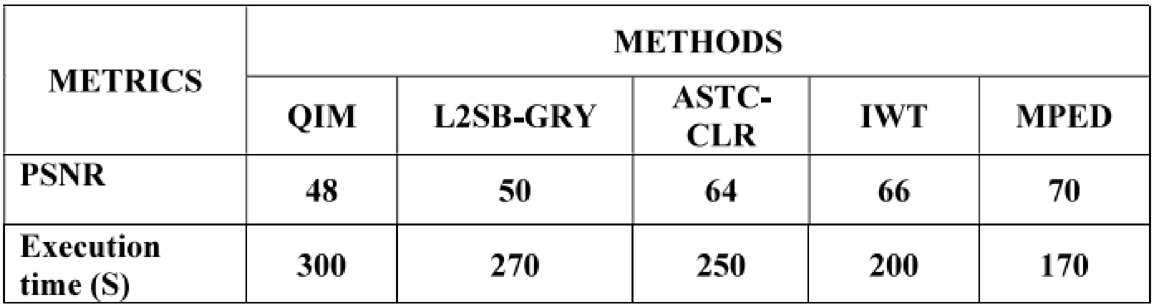
In this paper, we designed a three-dimensional chaotic system. The continuous-time chaotic system had already been transformed into discrete-time (DT) chaotic system by Euler method. The phase portrait of DT chaotic system had been implemented on an oscilloscope via Altera field programmable gate array. A cryptographic system of RGB image security for 3D chaotic system was proposed. There are three features in the encryption system. First, we use the information of plaintext image to produce the initial conditions of chaotic system. Second, the image of the permutation process shuffles the position of pixels in the plaintext image channels separately. Third, in the diffusion process, the pixels information in the shuffled image had been concealed by the XOR operation. The chaotic encryption system had been also implemented on Altera. Then, the cipher image can be obtained through the FPGA and simulated the image by MATLAB code. In the security analysis, such as histogram analysis, correlation coefficient analysis, information entropy analysis, differential attack analysis (NPCR and UACI) have been performed in this paper. Experimental results show that the proposed algorithm has better security in comparison with other algorithms.

In this chapter, IGN is proposed which has an ability to tune the required initial parameters of beta chaotic map for a secure key generation. The tuning of parameters has been done through GA using multi-objective fitness function. Moreover, the encryption has been carried out on sub-bands of an **COLOUR IMAGE** instead of a plain image, which further enhances the security. IGN is tested on ten well-known benchmark images. It also provides significant quality of decrypted colour images. To test the security of IGN, the various experiments have been carried out such as statistical attack, differential attack, secret key, noise attack, and occlusion attack analyses. The experimental results have shown that chaotic colour image has better performance as compared to the existing colour image encryption techniques.

In the paper, cryptosystems have been proposed for colour image encryption, compression, in the canonical transform domains and decomposition techniques are implemented for matrix decomposition, giving decryption keys. Affine and Arnold transform used in the schemes to increase the key space. The work contained in the thesis has been carried out as per the objectives outlined in the proposal. The paper contains the general introduction, basic transforms and techniques, colour image quality metrics, motivation for research, and the paper objectives in the paper. The relevant research gaps have been identified and presented in this paper. The cryptosystems developed to meet the specific objectives along with their implementation are explained in the four subsequent paper.

The table of result in colour image:

Performance Comparison results :



METRICS	METHODS				
	QIM	L2SB-GRY	ASTC-CLR	IWT	MPED
PSNR	48	50	64	66	70
Execution time (S)	300	270	250	200	170

While designing the cryptosystems, the pixel scrambling technique, namely affine transform, is implemented to increase the key space, and fractional Fourier transform is implemented to overcome the problem of linearity. This chapter consists of the following schemes for encryption:

- Scheme: Asymmetric cryptosystem for grayscale colour images using an affine transform in Fourier domain.
- Scheme: Asymmetric enciphering of binary and grayscale colour images using affine transform and fractional Fourier transform.

To validate and analyse the performance of the cryptosystems, key sensitivity analysis, statistical analysis and performance of the encryption schemes against various cryptographic attacks are carried out. Results obtained illustrate that all the proposed encryption schemes performed reasonably well, and successfully overcome the earlier shortcomings. It is worth noting that the schemes are sensitive to the chaotic map parameter, as a slight change in the parameter yields completely ambiguous results. Performance comparison results in this research paper for reversible data hiding. The colour image in chaotic map intriguing reversible image future embedding is reversibility is reversibility. in this work pre-processing is used for pixel colour image selection and then the improved chaotic colour image. The encrypted secret information in to the image by using which can recover original. Chaotic colour image experimental result show that the proposed method provides better performance than other techniques

SUMMARY

In this paper, a new image scrambling algorithm, by using image scrambling to encrypt the image to improve the security chaotic system of image. The new algorithm based on chaotic system and decomposition and recombination of sisal values is able to scramble pixel positions and pixel values of images. Analysis of the statistical information of stabled images in the experimental tests shows that the present algorithm provides reasonable security. Owing to the strong irregularity of the sorting transformation that improves the effect of the scrambling. The experimental results show that the algorithm is effective to scramble the image and can provide high security. It simulates scrambling under MATLAB to confirm it.

Comparison:

A deep and detailed overall comparison of the proposed scheme with other image encryption schemes is given below –

Table

Algorithms	**NPCR**	**UACI**	**Correlation**	**key space**	**Entropy**
Dhiman G, Kumar [4]	81.47	25.00	0.2564	10^{89}	6.2543
Ankush Srivastava [13]	90.08	25.35	0.4692	10^{74}	4.2165
Arooj Nissar & Mir[16]	90.70	30.28	0.25498	10^{100}	5.5482
Arroyo, D, Li [27]	99.19	28.90	0.31248	10^{69}	3.5477
Diaconu, AV [31]	74.10	35.23	0.222055	10^{43}	7.4469
phase retrieval attack[39]	74.63	35.98	0.055569	10^{55}	6.9999
Tahir Sajjad Ali & Rashid Ali [36]	85.01	37.26	0.65578	10^{89}	4.8975
Renuka Patel & Ankit Temurnikar[41]	88.21	35.41	0.98258	10^{91}	5.2314

References:

[1]. Curiac DI, Volosencu C (2012) Chaotic trajectory design for monitoring an arbitrary number of specified locations using points of interest. Mathematics Problem in Engineering, 1–18

[2]. Daemen J, Rijmen V (2001) AES Proposal, Rijndael. National institute of standards and technology, FIPS-197

[3]. Dhiman G, Kaur A, Sharma V, Kautish S, Guo S, Slowik A, Anshu S, A V (2020) Special issue on computational approaches for COVID-19 disease medical image analysis. Current medical imaging, Bentham Science

[4]. Dhiman G, Kumar V (2019) Spotted hyena optimizer for solving complex and non-linear constrained engineering problems. In: Harmony search and nature inspired optimization algorithms. Springer, pp 857–867

[5]. Diamidinos M, Chard alias K, Migita A, Koinonias P, Panagiotopoulou P, Mantas J (2016) Social and psychological effects of internet use. Acta Inform Med 24(1):66–68

[6]. Drebin H, Bailer J, Anders A, Wagner H, Gallas C (2014) Cyberstalking in a large sample of social network users: prevalence, characteristics and impact upon victims. Cyberpsychol Behave Soc Newt 17(2):61–67

[7]. -plaintext attack (2013) on optical encryption based on double random phase keys 1044 p-46, 2006.

[8]. D.f Venera c (2018) Fourier series use in the map Express, vol. 14, no. 8, pp. 3181 86, 2006.

[9]. X. Wang a on phase the colour image work in pical - Common. vol. 285, no. 6, pp. 1078 81, 2012.

[10]. V c genera cryptosystem based on phase Digital Signal Processing Digital Signal Processing - Appl. Opt., vol. 54, no. 22, pp. 6874 81, 2015.

[11]. RD ELISEAR -plaintext attack-based optical cryptosystem using phase- Appl. Opt., vol. 52, no. 4, pp. 871 78, 2013.

[12]. Hr vingal proccing of networking -plaintext attack on encryption domain Opt. Commun.vol. 309, pp. 231 35, 2013.

[13]. Ankush Srivastava & Prokash Ghosh 2019, _An Efficient Memory Zeroization Technique Under Side-Channel Attacks‘, 32nd International Conference on VLSI Design.

[14]. Aoki, K, Ichikawa, T, Kanda, M, Matsui, M, Moriai, S, Nakajima, J & Tokita, T 2000, _Camellia: A 128-bit block cipher suitable for multiple platforms - design and analysis‘, In Selected Areas in Cryptography, pp. 39–56.

[15]. Archambeau, C, Peeters, E, Standaert, FX & Quisquater, JJ, _Template Attacks in Principal Subspaces‘, In CHES, pp. 1–1.

[16]. Arooj Nissar & Mir, AH 2010, _Classification of stage analysis techniques: A study‘, Digital Signal Processing, pp.1758–1770.

[17]. Arribas, V, Bilgin, B, Petrides, G, Nikova, S & Rijmen, V 2018, _Rhythmic Keccak: SCA Security and Low Latency in HW‘, IACR Transactions on Cryptographic Hardware and Embedded Systems 2018, vol. 1, pp. 269–290.

[18]. Arribas, V, Cnudde, TD & Šijačić, D 2017, _Glitch-Resistant Masking Schemes as Countermeasure Against Fault Sensitivity Analysis‘, In FDTC IEEE Computer Society, pp. 1–8.

[19]. Aarthi, R & Kavitha, S 2017, 'Image encryption using binary bit plane and rotation method for an image security', Internationall Journal of Engineering Development and Research, vol. 5, no.

[20] Gy Anjin purohit (2011-18) pp. 2321-9939. 2. Abbas, NA 2016, 'Image encryption based on independent component analysis and Arnold's cat map', Egyptian Informatics Journal, vol. 17, no. 1, pp. 139-146.

[21]. Acharya, B , Patra, SK & Panda, G 2008, Image encryption by novel cryptosystem using matrix transformation : First International Conference on Emerging Trends in Engineering and Technology , pp. 77-81.

[22]. Adda, AP , Jadj-Said, N , M'Hamed, A & Belgoraf, A 2007, 'Lorenz's attractor applied to the stream cipher', Chaos, Solitons & Fractals, vol. 33, no. 5, pp. 1762-1766.

[23]. Al-Husainy & Uliyan, DM 2017, 'Image encryption technique based on the entropy value of a random block', International Journal of Advanced Computer Science and Applications, vol. 8, no. 7, pp. 260-266.

[24]. Al-Romema, NA , Mashat, AS & AlBidewi, I 2012, 'New chaos-based image encryption scheme for RGB components of color image', Computer Science and Engineering, vol. 2, no. 5, pp. 77-85.

[25]. Alvarez, G & Li 2006, 'Some basic cryptographic requirements for chaos-based cryptosystems', International Journal of Bifurccation and Chaos, vol. 16, no. 8, pp. 2129-2151.

[26]. Arrowsmith, DK , Cartwright, Lansbury, AN & Place, CM 1993, 'The Bogdanov map: Bifurcations, mode locking and chaos in a dissipative system', International Journal of Bifurcation and Chaos, vol. 3, no. 4, pp. 803-842.

[27]. Arroyo, D, Li, Amigo, JM, Alvarez, G & Rhouma, R 2010, 'Comments on "Image encryption with chaotically coupled chaotic maps"‘, Physica D: Nonlinear Phenomena, vol. 239, no. 12, pp. 1002-1006.

[28]. De Monte, S, d'Ovidio, F, Chate, H & Mosekilde, E 2005, 'Effects of microscopic disorder on the collective dynamics of globally coupled maps', Physics D: Nonlinear Phenomena, vol. 205, no. 1-4, pp. 25-40.

[29]. Denning 1982, Cryptography and data security, Addison-Wesley Publishing Company, Inc, USA.

[30]. Devaney, RL 1989, An Introduction to Chaotic Dynamical Systems, Addison-Wesley, California.

[31]. Diaconu, AV, Costea, A & Costea, MA 2014, 'Color image scrambling technique based on transposition of pixels between RGB channels using knight's moving rules and digital chaotic map', Mathematical Problems in Engineering, vol. 014, p. 15 pages.

[32]. Diffe, W & Hellman, ME 1976, 'New Directions in Cryptography', IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654.

[33]. Wang X, Wu X, Zhang Y (2018) Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Optics Lasers Eng 107:370–379

[34]. Wu Y, Noonan JP, Again S (2011) NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology. J Select Areas Telecommand (JSAT) 1(2):31–38

[35]. Chai X, Bi J, Gan Z, Liu X, Zhang Y, Chen Y (2020) Colour image compression and encryption scheme based on compressive sensing and double random encryption strategy. Sig Process 176:107684

[36]. Tahir Sajjad Ali & Rashid Ali, Multimedia Tools and Applications (2022) 81:20585–20609 A novel colour image encryption scheme based on a new dynamic compound chaotic map and S-box. under exclusive licence to Springer Science + Business Media, LLC, part of Springer Nature 2022.

[37]. Wang X, Zhu X, Wu X, Zhang Y (2018) Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Optics Lasers Eng 107:370–379

[38]. Wu J, Liao X, Yang B (2017) Color image encryption based on chaotic systems and elliptic curve ELGamal scheme. Sig Process 141:109–124

[39]. Kp agrahit (2013) -phase retrieval attack free cryptosystem based on direct attack to phase-truncated Fourier-transform-based encryption using a Opt. Lett., vol. 38, no. 18, pp. 3684 86, 2013.

[40]. Rn vimlesh (2012-14) optical asymmetric cryptosystem based on phase Appl. Opt., vol. 53, no. 2, pp. 208 13, 2014. Pp 5648-1584

[41]. Renuka Patel and Ankit Temurnikar (2020-23) based on colour digital image volume 23 , issue 2 , December 2023. Pp. 223-240