A Survey on Image Encryption using Chaos-based Techniques

Veena G[1], Dr. Ramakrishna M[2]
Dept. of CSE, Vemana Institute of Technology
Bengaluru, India

***Abstract*—Encryption methods such as AES (Advanced Encryption Standard), DES (Data Encryption Standard), etc. cannot be used for image encryption as images contain a huge amount of redundant data, a high correlation between neighboring pixels and size of the image is very large. Chaos-based techniques have suitable properties that are required for image encryption. The properties include sensitivity to initial conditions, pseudorandom number, ergodicity, and density of periodic orbits. In this paper, a survey of image encryption using chaos-maps such as a logistic map, piecewise linear chaotic map (PWLCM), tent map, etc. is done in order to choose best map for image encryption. Comparison of image encryption using different chaotic maps is done by considering parameters such as key-space and correlation analysis.**

***Keywords*—Chaos theory; image encryption; logistic map; PWLCM; tent map**

I. Introduction

To secure information present in the image from unauthorized user access during transmission and storage, image encryption is used. Image encryption [1][12] can be achieved by changing pixel positions as well as changing contents of pixels as a result the true content of the image is completely changed. Different techniques such as cryptography [28], steganography, compression, and digital watermarking can be used to encrypt the image. Images can be encrypted using chaos-based techniques which are referred to as chaotic cryptography. Chaotic cryptography [1-4] [19-29] is the use of mathematical chaos theory to the cryptography. Chaotic cryptography involves the use of chaotic maps for generating confusion and diffusion. The chaos-based technique has properties that are suitable for image encryption. Sensitivity to initial condition is one property of chaos-based technique in which a minute variation in initial conditions will result in a large variation in behavior of the system, i.e., to decrypt the image, exact initial conditions are very much essential. Numerous chaotic maps are used in encryption. A chaotic map is a function that shows chaotic structure. Chaotic maps are used to generate random numbers. Logistic map, Baker’s Map, Tent map, Renyi map [1-4] are a few of the important chaotic maps. Chaotic systems are used to generate the sequence of numbers which can be used as a key in image encryption. Chaotic systems exhibit certain properties required for image encryption and decryption, one such property is sensitivity to initial conditions [5], Fig. 1(a) shows the plot of logistic function for two different initial conditions plotted against time versus the value obtained from logistic function, the red line shows the plot of the logistic map when x0 = 0.2, the green line shows the plot of the logistic map when x0 = 0.200001. Fig. 1(b) shows the plot of the difference between logistic map values for 2 initial conditions x0 = 0.2 and x0 = 0.200001, it can be seen that the difference between the 2 initial conditions is very small but the difference in values generated by the logistic map is very large this property is known as sensitivity to initial conditions. The sensitivity to initial conditions property of chaotic systems can be used in image encryption. Chaotic systems are used to generate pseudorandom numbers, the numbers generated by the chaotic system exhibit all the properties of random numbers but they are not random since passing the exact initial conditions the numbers can be regenerated. Chaotic systems [18] exhibit a property called ergodicity [10]; a system is said to be ergodic if it shows irreducibility. All the above properties of chaotic systems can be used in effective image encryption and decryption. There exist many techniques to encrypt images using the chaotic maps. This paper surveys different techniques to identify the best chaotic map for image encryption.

The rest of this paper is organized as follows: Section II gives the literature review of image encryption using chaotic maps. Section III gives a comparative analysis of the image encryption using chaotic maps. Finally, Section IV concludes this paper.

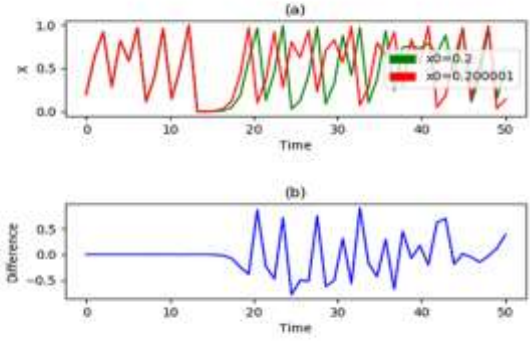

Fig. 1. Logistic Map Plot (a) Logistic Map for 2 Initial Conditions (b) Difference between Logistic Map Values for 2 Initial Conditions.

II. Literature Review

A. DNA Encoding

A combination of DNA encoding and chaos-based logistic map [1] was used to encrypt a color image. In DNA encoding, data encoding will be performed based on DNA sequence.

Bases that are present in single-stranded DNA are Thymine (T), Guanine (G), Cytosine (C), and Adenine (A). T and A are complemented to each other similarly G and C are also complemented to each other. To encode binary data using four bases (T,G,C and A), binary numbers 11, 10, 01, and 00 can be used. Eight coding rules can be used that are shown in Table I.

TABLE I. EIGHT CODING RULES

A	B	C	D	E	F	G	H
00 T 01 C 10 G 11 A	00 A 01 C 10 G 11 T	00 T 01 G 10 C 11 A	00 A 01 G 10 C 11 T	00 C 01 A 10 T 11 G	00 G 01 A 10 T 11 C	00 C 01 T 10 A 11 G	00 G 01 T 10 A 11 C

The logistic map as shown in equation (1) is a simple single-dimensional map that shows the unexpected degree of complexity. Mathematically it is defined as follows.

$$y_{n+1} = \mu x_n(1 - y_n) \tag{1}$$

If the initial values of y_0 and μ is ($0 <= y_0 <= 1$) and ($0 < \mu < 4$) respectively then the logistic map produces a sequence of values $y_0, y_1, y_2, \ldots$. The important behavior of logistic map is when μ is ($0 < \mu < 3$) the sequence approaches a fixed value quickly. A different behavior is observed when μ is ($3.56995 < \mu < 4$) the generated sequences are not periodic; they are not convergent and they have sensitivity to initial value.

A Color image [13-15] is split into Red, Green, and Blue components that are transformed into three binary matrixes R, G, and B respectively. DNA encoding is used on each of the matrices using key1 ε [1,8] after DNA encoding further matrices are added using mod 2 for increasing the strength of encoding. A chaotic sequence (seq1) is generated by using logistic chaotic map with initial values y_0 and μ_0. DNA encoded matrices are complemented using seq1, the complemented result is decoded through DNA decoding using key2 ε [1,8]. A chaotic sequence (seq2) is generated using a logistic chaotic map with initial values y_1 and μ_1. The exclusive-or operation is performed DNA decoded matrix and seq2 and RGB image is recovered. Totally six key parameters used in [1], if the precision used is 10^{-14} the total keys' space will be approximately 10^{56} i.e. ($10^{14} * 10^{14} * 10^{14} * 10^{14}$). The key space is large so it will not be vulnerable to exhaustive attacks. The system is sensitive to initial parameters, with slight variation in initial parameters the decrypted image will be very much different from the original image (avalanche effect). The limitation in the above algorithm is that the speed is not effective, to improve the speed there is a need for DNA chip technology.

B. Tent Map

A chaotic tent map was used to encrypt and decrypt images [2]. Tent map [3] is mathematically defined as in equation 2:

$$x_{j+1} = f(x_j, \alpha) = \begin{cases} f_L(x_j, \alpha) = \alpha x_j, x_j < 0.5 \\ f_R(x_j, \alpha) = \alpha(1 - x_j), otherwise \end{cases} \tag{2}$$

The tent map function [16-17] evaluates to real numbers [0, 1]. α is the control parameter which takes a positive real number and x_0 is the initial condition of equation (2). The behavior of the tent map can be easily studied by the plot of the bifurcation diagram, which is a plot of the sequence generated by the tent map with the control parameter (α) used for generating the sequence. The following details can be observed from the bifurcation diagram. For $\alpha \epsilon [0,1)$ tent map has one fixed point x = 0, i.e., the equation converges to x = 0. For α = 1 all values of $x \leq 0.5$ are fixed points of the system. For α between 1 and 2, the sequence generated by the system is chaotic which is unstable. Tent map exhibits fixed point-behavior when $\alpha < 1$ and chaotic behavior when $\alpha > 1$. To encrypt the image [2] following procedure is used:

- Read the plane image of size N, initial condition (x_0) as encryption key, and control parameter (α).
- Obtain the sequence of size N using a chaotic tent map as given in equation (2) as array x(n).
- Encrypt image using x(n) to obtain the ciphered image.

To decrypt the image same values of x_0 and α which were used in encryption should be used. Totally two key parameters used in [2] x, α if the precision used is 10^{-16} the total keys' space will be approximately 10^{32} i.e., ($10^{16} * 10^{16}$). The key space is large so it will not be vulnerable to brute-force attacks. The encrypted image showed a correlation coefficient of two adjacent pixels in diagonal, vertical, and horizontal directions as 0.00003, 0.0025, and 0.0016 respectively. The entropy of the encrypted image is 7.999876.

C. 3D cat Map

Equation (3) gives Arnold-cat map, where x and y are representing pixel positions.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ 1 \tag{3}$$

In equation (3) mod 1 takes care of the fractional part, the linear transform shears unit square, and mod operation folds it back to the unit square. The 3D cat map is given by equation (4) where B is a matrix.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = B \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod\ 1 \tag{4}$$

In [4] following steps are followed to encrypt the image:

1) Key generation: 128-bit sequence number is split into $k_{px,}$ $k_{py,}$ $k_{pz,}$ $k_{qx,}$ $k_{qy,}$ k_{qz} that are used in 3D cat map and $k_{l,}$ k_s are used in logistic map.

2) Conversion of the 2D image into 3D: The image is split to form several three-dimensional cubes.

3) Apply 3D cat map on the result of step b.

4) Apply diffusion process on the result of step c using the logistic map.

5) Transform three dimensional cubes to two-dimensional image.

The total key space is 2^{128} [4]. The key space is large so it will not be vulnerable to brute-force attacks. The encrypted image showed a correlation coefficient of two adjacent pixels in diagonal, vertical and horizontal directions as 0.01480, 0.00016, and 0.01183, respectively.

D. Spatiotemporal Chaotic System

In [5] image encryption consists of confusion and diffusion stages. A spatiotemporal chaotic system is used. The chaotic system consists of logistic map and piecewise linear chaotic map (PWLCM). The pseudorandom numbers are produced by the chaotic system which consists of a two-dimensional dynamic map. The two-dimensional dynamic map is as defined in equation (5).

$$\begin{cases} x_{i+1} = (1-\beta)f_1(x_i) + \beta f_2(y_i) \\ y_{i+1} = (1-\beta)f_1(y_i) + \beta f_2(x_i) \end{cases} \tag{5}$$

Where f_1 is the logistic map and f_2 is PWLCM. Both f_1 and f_2 are chaotic maps. f_1 and f_2 are defined as in equation (6a, 6b).

$$f_1(x) = \alpha x(1-x) \tag{6a}$$

$$f_2(x) = \begin{cases} \frac{x}{\gamma}, 0 \le x < \gamma \\ \frac{(x-\gamma)}{(0.5-\gamma)}, \gamma \le x < 0.5 \\ f_2(1-x). 0.5 \le x < 1 \end{cases} \tag{6b}$$

The image encryption consists of a substitution process followed by a diffusion process. In the substitution process S-box is generated and the pixels of the image to be encrypted will be substituted by the contents of the S-box based on the key, substitution process creates confusion i.e., a small change in the key will result in large changes in the ciphered image. The circular S-box is used for the substitution process. Equation (7) is used in the substitution process.

$$\begin{cases} p_i' = S[(header + p_i) mod\ 256] \\ \quad header = p_i' \oplus m \end{cases} \tag{7}$$

Where p_i is pixel in the plane image, p_i' is the cipher pixel corresponding to the original pixel p_i. Usage of circular S-box has an added advantage in which the substitution for a pixel depends on not only on the pixel value itself but also on the value of the previous cipher pixel. The substitution operation is followed by diffusion operation. In the diffusion process a small change in the plane image, will result in large changes in the ciphered image. Key stream buffer is used for the diffusion process. The keys generated by the cypher are stored in key stream buffer. Equation (8) is used in the diffusion process.

$$c_i = [(p_i' \oplus c_{i-1}) + Get(c_{i-1})]\ mod\ 256 \tag{8}$$

E. Linear Diophantine Equation

In [6] the image encryption is performed based on a chaotic system called piece-wise linear chaotic map (PWLCM) to generate two numbers. The generated numbers are used as co-efficient of the Linear Diophantine Equation (LDE) [7]. The set of solutions to LDE is used in the permutation of the image. The image is divided into sub-images of size N = m x n. The solution to LDE is found out only for the first sub-image, for the rest of sub-images the key is altered by replacing d number of values of the key with newly generated d number of values from the chaotic system, since the solution to LDE is not found for each sub-image the encryption is faster. Once all the sub-image is permuted each permuted sub image is diffused. The New initial conditions for the chaotic system are generated that depends on the total encrypted image. The above steps are repeated again to generate the permutation key and the total encrypted image is permuted again to obtain the cypher image that completes round 1. Depending on the number of rounds the above steps are repeated.

Equation (9) is piece wise linear chaotic map (PWLCM) equation.

$$x(n) = F[x(n-1)] = \begin{cases} \frac{x(n-1)}{r}, if\ 0 \le x(n-1) < r \\ \frac{[x(n-1)-r]}{(0.5-r)}, if\ r \le x(n-1) < 0.5 \\ F[1-x(n-1)], if\ 0.5 \le x(n-1) < 1 \end{cases} \tag{9}$$

The system using PWLCM will behave chaotically when r i.e., the control parameter is within $]0,0.5[$, the initial condition is within $]0,1[$. Equation (10) is LDE equation.

$$ag + bh = c \tag{10}$$

Where a, b and c are constants of natural integers, a and b are generated from PWLCM. The equation (10) can be solved using the equation (11).

$$\begin{cases} g(t) = g_0 + \frac{b}{\wedge} t \\ h(t) = h_0 - \frac{a}{\wedge} t \end{cases} \tag{11}$$

Where ^ is the GCD of a and b, t ϵ {0,1, 2, …., L-1} where L is the permutation length same as the length of sub-image. Once the solutions of LDE are determined as a set of G and H, here G is {g(1), g(2),, ….., g(L)} and H is {h(1),h(2),,……,h(L)}. The elements of G and H are sorted either in ascending or descending order. If I_G and I_H are index vectors of G and H then the permutation key I_Z is obtained by equation (12). Using $I_{Z,}$ image is shuffled.

$$I_Z = I_G(I_H) \tag{12}$$

In the above scheme [6] total key space is 2^{256}, which is large for resisting brute force attacks. The entropy using the above scheme [6] is equal to its highest value (H – 8). The encryption scheme satisfies zero correlation property.

F. Bidirectional Diffusion

In [8] image encryption is performed using the permutation and diffusion process. Chaos technique is used to generate the key, skew tent map and logistic maps are used in key generation. In the permutation process, the pixel position of the plane image is shuffled as a result the permuted image will be totally different from the plain image. The permutation process is carried out using multiplication operation and insertion operation. In multiplication operation, if P represents a permutation of length l and Q represents a permutation of length m then the multiplication operation produces a permutation of length lm. In insertion operation, if P represents a permutation of length l and let ins(P, s) denote inserting the element l at the position s in P. If S is a sequence of insertion positions of length m, then the INS(P, S) can be computed using the equation (13).

$$INS(P,S) = \begin{cases} P, S = \emptyset \\ INS(ins(P,s_0), S - \{s_0\}, S \neq \emptyset \end{cases} \tag{13}$$

Smaller permutations are combined using multiplication and insertion to generate larger permutations. The entropy using the above scheme [8] is greater than 7.99. Diffusion is a process in which a small change in the plain image should result in large changes in the ciphered image. If a first pixel is altered in the plain image, then because of diffusion all the pixels in the ciphered image will be altered, but if the last pixel is altered in the plain image then only the last pixel in the ciphered image will be altered, hence in [8] the diffusion is carried out in both forward and backward directions. In the above scheme total key space is 2^{312}, that is large for resisting brute force attacks. The entropy using the above scheme [8] is equal to its highest value.

G. Bülban Chaotic Map

In [9] fast image encryption algorithm is implemented using the Bülban chaotic map. A very high chaotic behavior with larger range of parameter values is exhibited by Bülban chaotic map which increases the security level and key space. Bülban chaotic map is a real one-dimensional, simple and discrete chaotic map. Equation (14) defines Bülban chaotic map.

$$x_{n+1} = x_n \times \sqrt{\frac{a}{x_n - b}} \tag{14}$$

The encryption is performed in T rounds, each round consists of confusion and diffusion stages to change the position and values of the pixels. Two sequences (PR, PC) of real numbers are generated using Bülban chaotic map which is converted to unsigned integers. The pixel values of each row are circularly shifted to the right by the number of times as provided by sequence PR. The pixel values of each column are circular shifted down by the number of times as provided by sequence PC. Four real sequences (DR+, DR-, DC+, DC-) are generated using Bülban chaotic map as given in equation (15).

$$DR^{+} = \{\, DR_j^{+} \mid DR_j^{+} = DR_j^{+} \times 10^5 \, mod \, 256 \,\}$$

$$DR^{-} = \{\, DR_j^{-} \mid DR_j^{-} = DR_j^{-} \times 10^5 \, mod \, 256 \,\}$$

$$DC^{+} = \{\, DC_i^{+} \mid DC_i^{+} = DC_i^{+} \times 10^5 \, mod \, 256 \,\}$$

$$DC^{-} = \{\, DC_i^{-} \mid DC_i^{-} = DC_i^{-} \times 10^5 \, mod \, 256 \,\} \tag{15}$$

The real sequences are converted to unsigned integers. Equation (16) is used in substitution.

$$P_i = (P_i + (DR^{+} \oplus pred(P_i)))mod\, 256$$

$$P_{M-i+1} = (P_{M-i+1} + (DR^{-} \oplus succ(P_{M-i+1})))mod\, 256$$

$$P_j = (P_j + (DC^{+} \oplus pred(P_j)))mod\, 256$$

$$P_{N-j+1} = (P_{N-j+1} + (DC^{-} \oplus succ(P_{N-j+1})))mod\, 256 \tag{16}$$

Using equation (16) diffusion of pixels is carried out row wise as well as column wise to change the pixel values. Where ⊕ operator is bitwise exclusive-or, pred(P_i), and succ(P_i) these functions return the row Pi predecessor and successor respectively. In pred(P_i), if P_i is the first row then the last row will be returned else Pi_{-1} row will be returned. In succ (P_i) if P_i is the last row then the first row will be returned else Pi_{+1} row will be returned. The above process is repeated for T different rounds. In the above scheme total key space is 2^{360}, which is large for resisting brute force attacks. The entropy using the above scheme is almost equal to 7.999.

H. Hybrid Chaotic Map

In [10] hybrid chaotic map is used to generate keys required for image encryption. First, the image is subjected to DWT (Discrete Wavelet Transforms). DWT decomposes a digital image into various subbands so that lower frequency subbands have finer frequency resolution and higher frequency subbands have a coarser resolution. DWT here decomposes the image into four subbands LL, LH, HL, and HH. Four different chaotic equations (17-20) are used to generate random sequences.

$$\begin{cases} y_{n+1} = b^2 x_n, \\ x_{n+1} = (x_n)^2 + (y_n)^2 - a.r \end{cases} \tag{17}$$

$$\begin{cases} y_{n+1} = y_n - r.\tan(x_n) \\ x_{n+1} = \sin(x_n) + \sin(y_{n+1}) \end{cases} \tag{18}$$

$$\begin{cases} y_{n+1} = y_n - r.\tanh(x_n) \\ x_{n+1} = \tanh(x_n) + \sin(y_{n+1}) \end{cases} \tag{19}$$

$$\begin{cases} y_{n+1} = y_n + a.r\cos(x_n) \\ x_{n+1} = \cos(x_n) + \sin(y_{n+1}) \end{cases} \tag{20}$$

The 4 subbands obtained from DWT are subjected to a permutation process. The keys required for permutation is generated using a chaotic system. Different bands use different chaotic equations (H1 to H4). The permuted image is subjected to diffusion. The key required for the diffusion process is generated using one of the four chaotic equations. In the above scheme [10] total key space is 2^{58}, which is large for resisting brute force attacks. The entropy using the above scheme is almost equal to 7.999.

I. Lorenz Chaotic Map

In [11] the pseudorandom numbers required for image encryption are generated by Lorenz chaotic map, the permutation of image rows and columns is carried out by random switch control mechanism. Equation (21) represents Lorenz chaotic map.

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = cx - y - xz, \\ \dot{z} = xy - bz \end{cases} \tag{21}$$

From Lorenz chaotic equation sample sequences {xi}, {yi} and {zi} are generated. The generated sequences are used to generate random sequences S1 and S2 as given in equation (22).

$$S1_i = mod(round((x_i + y_i) * 10^{12}),2)$$

$$S2_i = mod(round(z_i * 10^{12}), 256) \tag{22}$$

To permute pixels of the image of size M x N, two random sequences R and L are generated using Lorenz chaotic equation, the sequences are represented by the equation (23).

$$R = \{R_1, R_2, \ldots\ldots, R_M\}$$

$$L = \{L, L_2, \ldots\ldots, L_M\} \tag{23}$$

The sequences R and L are sorted into SR and SL sequences. The positions of each point in the sequences SR and SL in the sequences R and L are marked to get sequences TR and TL. The row and column transformation of the image is performed using the equation (24).

$$\bar{I} = \begin{cases} f_1(I) = \ if\ S1_i = 0, \\ f_2(I) = \ if\ S1_i = 1 \end{cases} \tag{24}$$

I and $\bar{I}$ represents a plane image and scrambled image respectively. f_1 is a row transformation if $S1_i = 0$ then TR$_i$ row is moved to the ith row. If $S1_i = 1$ then TL$_i$ column is moved to the ith column. After permutation of the image, the pixels of the image will be scrambled and image diffusion will be performed using the equation (25).

$$\overline{I_\iota} = mod(C_i \oplus S_2 - C_{i-1} - \overline{I_{\iota-1}}, 256) \tag{25}$$

Where C_i is the ciphered value of the ith pixel. In the above scheme total key space is 2^{128}, which is large for resisting brute force attacks. The entropy using the above scheme is almost equal to 7.99.

III. Comparision Analysis and Discussion

Table II shows different chaotic maps used to encrypt an image. The features like correlation analysis, key spaces are compared. In [1] the algorithm used removes pixel correlation of the RGB image in the spatial domain by using DNA addition, the security of image encryption in [1] depends both on the chaotic systems as well as DNA operation providing the dual security, the speed performance of the proposed algorithm is not ideal compared to other algorithms. In [2] the pixel values are changed only in one direction hence it is susceptible to entropy attacks. In [4] three-dimensional chaotic map called 3D cat map is used to encrypt the image, the algorithm used in [4] is suitable for real-time Internet image and video encryption. [4] provides very high resistance to statistical attacks as well as differential attacks. In [5] to provide high security the circular S-box is introduced that provides high resistance to common attacks, brute-force attacks, differential attacks, and statistical attacks. In [6] chaotic map is combined with LDE to generate a high speed and more secure image encryption system that is best suited for low-end microprocessors. In [8] image encryption is done using chaotic map with total shuffling and bidirectional diffusion. The key stream used in diffusion depends on both the sequence generated by the chaotic map as well as pixels of the plain image that increases the plaintext security. In [9] Bülban chaotic map is used for image encryption, to provide high security an XOR operation is combined with modulo function, the circular shift is used to shuffle the pixel positions, the proposed algorithm in [9] has very high speed hence can be used in real-time application encryption of images. In [10] DWT and double chaotic function is used to encrypt the image which shows higher NPCR and UACI values 99.6472% and 33.6248% respectively, this method of image encryption is well suited for wireless communications. In [11] pseudorandom sequences are generated using Lorenz chaotic system which shows high entropy.

TABLE II. Chaotic Map Comparison Analysis, H – Horizontal Correlation, V – Vertical Correlation and D – Diagonal Correlation

Ref.	**Chaotic map and Technique used**	**Correlation Analysis**				**Key space**	**Special feature**
		Image	**H**	**V**	**D**		
[1]	Logistic map and DNA encoding	Plain	0.9099	0.0059	0.9856	2^{186}	Reduced pixel correlation due to DNA encoding.
		Ciphered	0.0059	-0.0042	0.0180		
[2]	Tent map	Plain	0.9576	0.9362	0.9157	2^{106}	Time taken for encryption and decryption is less. 256 x 256 image with 24 bits takes 0.9-0.95 s for encryption
		Ciphered	0.0016	0.0025	0.0003		
[4]	3D cat map	Plain	0.91765	0.95415	0.90205	2^{128}	Suitable for real rime image encryption and transmission applications.
		Ciphered	0.01183	0.0025	0.0003		
[5]	Logistic map, PWLCM and Spatiotemporal	Plain	0.93348	0.95922	0.91299	2^{280}	Circular S-box is used for substitution operation.
		Ciphered	0.00292	-0.0012	-0.00045		
[6]	PWLCM and LDE	Plain	0.9721	0.9851	0.9595	2^{256}	It can be implemented using low end microprocessors.
		Ciphered	0.0026	0.0034	-0.0019		
[8]	Skew tent map, Logistic maps and Bidirectional diffusion	Plain	0.98498	0.9781	0.96847	2^{312}	The key stream buffer is used in diffusion.
		Ciphered	0.00032	-0.00274	-0.00147		
[9]	Bülban chaotic map	Plain	0.9618	0.9854	0.9618	2^{360}	Circular shift is used to shuffle the pixel positions.
		Ciphered	0.00039	0.0059	-0.0050		
[10]	Hybrid chaotic map and DWT	Plain	0.98453	0.95271	0.97553	2^{58}	The encryption is best suited for applications like wireless communications.
		Ciphered	0.00047	-0.03911	0.00305		
[11]	Lorenz chaotic map and switch control mechanism	Plain	0.9728	0.9281	0.9050	2^{128}	Switch control law is used to realize the pixel permutation of the image.
		Ciphered	-0.0011	0.0014	0.0005		

IV. Conclusion and Future Work

In this paper nine different techniques are discussed for encrypting the image with the chaotic maps. Chaotic maps are best suited for the image encryption since image has huge amount of redundant data, a high correlation between neighboring pixels and large size. In chaotic maps higher dimensional maps provide higher security compared to lower dimensions. The image encryption system will be highly secure when the key used in substitution and permutation of the image pixels, are both random as well as the key depend on the plain image. Lot of research need to be done in the areas of multimedia encryption and decryption.

References

[1] Lili Liu, Qiang Zhang, Xiaopeng Wei "A RGB image encryption algorithm based on DNA encoding and chaos maps", Computers & Electrical Engineering, vol. 38, issue 5, pp. 1240–1248, 2012.

[2] Chunhu Li, Guangchun Luo, Ke Qin, Chunbao Li "An image encryption scheme based on chaotic tent map", Nonlinear Dynamics, vol. 87, no. 1, pp. 127–133, 2017.

[3] Kanso, A "Self-shrinking chaotic stream ciphers", Communications in Nonlinear Science and Numerical Simulation volume 16 issue 2, pp. 822–836, 2011.

[4] Guanrong Chen, Yaobin Mao, Charles K. Chui "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons & Fractals, vol. 21, issue 7, pp. 49–61, 2004.

[5] Xuanping Zhang, Zhongmeng Zhao, Jiayin Wang "Chaotic image encryption based on circular substitution box and key stream buffer", Signal Processing: Image Communication, vol. 29, issue 8, pp. 902–913, 2014.

[6] J.S. Armand Eyebe Foudaa, J. Yves Effa, Samrat L. Sabat, Maaruf Ali "A fast chaotic block cipher for image encryption", Communications in Nonlinear Science and Numerical Simulation, vol. 19, issue 3, pp. 578-588, 2014.

[7] B. Sroysang, "More on the diophantine equation 8x + 19y = z2," International Journal of Pure and Applied Mathematics, vol. 81, no. 4, pp. 601–604, 2012.

[8] Xuanping Zhangas, Zhongmeng Zhao "Chaos-based image encryption with total shuffling and bidirectional diffusion", Springer Science, pp. 319-330, 2013.

[9] Mohamed Zakariya Talhaoui, Xingyuan Wang, Mohamed Amine Midoun "Fast image encryption algorithm with high security level using the Bülban chaotic map", Journal of Real-Time Image Processing, 2020.

[10] Ibrahim Yasser, Fahmi Khalifa, Mohamed A. Mohamed, Ahmed S. Samrah "A New Image Encryption Scheme Based on Hybrid Chaotic Maps", Hindawi Complexity, 2020.

[11] Shenyong Xiao, ZhiJun Yu, and YaShuang Deng "Design and Analysis of a Novel Chaos-Based Image Encryption Algorithm via Switch Control Mechanism", Hindawi Security and Communication Networks, 2020.

[12] P. R. Sankpal and P. A. Vijaya, "Image Encryption Using Chaotic Maps: A Survey", 2014 Fifth International Conference on Signal and Image Processing, Jeju Island, pp. 102-107, 2014.

[13] Yunpeng Zhang, Fei Zuo, Zhengjun Zhai, Cai Xiaobin, "A New Image Encryption Algorithm Based on Multiple Chaos System", International Symposium on Electronic Commerce and Security, pp. 347–350, 2008.

[14] Shujun L, Xuan Z. "Cryptanalysis of a chaotic image encryption method", Proceedings of IEEE, International Symposium on Circuits and Systems, OmniPress. Phoenix-Scottsdale, pp. 87–91, 2002.

[15] Hongjun L, Xingyuan W. "Color Image encryption based on one-time keys and robust chaotic maps", Computers and Mathematics with Applications, pp. 3320–3327, 2010.

[16] Ye G.D, Huang X.L, "An efficient symmetric image encryption algorithm based on an intertwining logistic map", Neurocomputing, pp. 45–53, 2017.

[17] Lian, S., Sun, J., Wang, Z. "A block cipher based on a suitable use of the chaotic standard map", Chaos Solitons Fractals, pp. 117–129, 2005.

[18] Kurian AP, Puthusserypady S, "Secure digital communication using chaotic symbolic dynamics", Turk J Elect Eng, pp. 195–207, 2006.

[19] Arroyo D, Alvarez G, Li S, Li C, Fernandez V, "Cryptanalysis of a new chaotic cryptosystem based on ergodicity", Int J Mod Phys B, pp. 651–659, 2009.

[20] Alvarez G, Li S, "Some basic cryptographic requirements for chaos-based cryptosystems", Int J Bifurcations Chaos, 2129–2151, 2006.

[21] Kocarev, "Chaos-based cryptography: a brief overview". IEEE Circ Syst Mag, pp. 6–21, 2001.

[22] Yen JC, Guo JI, "A new chaotic key-based design for image encryption and decryption", In: Proc IEEE Int Conference Circuits and Systems, vol. 4, pp. 49–52, 2000.

[23] S. Ahadpour, Y. Sadra, "A chaos-based image encryption scheme using chaotic coupled map lattices", Int. J. Comput. Appl, pp.15–18, 2012.

[24] Mao Yaobin, Chen Guanrong, Lian Shiguo, "A novel fast image encryption scheme based on 3d chaotic baker maps", Int J Bif Chaos , pp. 3613–3624, 2004.

[25] Gao, T., Chen, Z, "Image encryption based on a new total shuffling algorithm", Chaos Solitons Fractals, pp. 213–220, 2008.

[26] Wang X, He G, "Cryptanalysis on a novel image encryption method based on total shuffling scheme", Optics Communications", pp. 5804–5807, 2011.

[27] Musanna F, Kumar S, "A novel fractional order chaos-based image encryption using Fisher Yates algorithm and 3-D cat map", Multimedia Tools Appl., 2018.

[28] Stallings W, "Cryptography and network security principles and practice", Int. J. Eng. Comput. Sci., pp. 121–136, 2012.

[29] Wang X, Feng L, Li R, Zhang F, "A fast image encryption algorithm based on non-adjacent dynamically coupled map lattice model", Nonlinear Dyn, pp. 1–28, 2019.