International Journal of Progressive Research in Science and Engineering
Volume-2, Issue-2, February-2021
www.ijprse.com

A Survey on Image Encryption Using Chaotic Maps

Marakumbi Prakash R[1]

[1]*Assistant Professor, Department of Electronics & Communication, Tontadarya College of Engineering, Gadag, Karnataka, India.*

Corresponding Author: pmarakumbi@gmail.com

Abstract: - Authentication plays an important role in protecting image against unauthorized access. Digital images are transmitted over insecure channels such as the internet. Images must be protected against attempts to manipulate them; such manipulation could tamper the decisions based on these images. To protect the authenticity of images several methods have been proposed. Image authentication methods have gained attention due to their significance in the areas of multimedia communications and multimedia networking applications. The traditional encryption techniques exhibits a low level of security and significantly low level of resistance to the attacks. This problem can be overcome by chaotic image encryption techniques as they have a high level of randomness in key generation. This paper attempts to study various chaos-based image encryption algorithms and techniques and to compare their performance in various environments.

Key Words: — ***Cryptography, Chaos, Chaotic Maps, Encryption Techniques, Image Encryption, Security, Secure Communication.***

I. INTRODUCTION

Authentication methods provide a means of ensuring the integrity of an image. Therefore, there is need to protect these images against various attempts to manipulate them and it is important to make an effective method to solve image authentication problem that is ensuring the integrity of an image. Due to increase in the multimedia applications, image authentication techniques have gained attention. To handle these problems, various methods of cryptography were proposed. Cryptography is the study of techniques for secure communications, in the pressure of unauthorized users. The various aspects of cryptography includes confidentiality, data integrity and authentication. The idea of using chaos in cryptography is highly appreciated and researched because it is highly sensitive to initial condition and control parameters, ergodicity and pseudo- randomness and therefore it enhances the requirements of the secure algorithm. The image encryption techniques can be classified into two groups based in the encryption approach; they are chaos-based methods and non-chaos. The term chaos is defined as "when the present determines the future, but approximate present does not approximately predict the future. I.e. any small change in the initial conditions causes a drastic change in the output.

II. IMAGE ENCRYPTION TECHNIQUES

The image encryption techniques can be classified into two groups based in the encryption approach; they are chaos-based methods and non-chaos. Image encryption can also be divided into full encryption and partial encryption schemes [1] according to the percentage of the data that is encrypted. Encryption schemes can also be classified as either combined-compression methods or noncompression methods.

III. CHAOS THEORY IN CRYPTOGRAPHY

A chaotic dynamical system is any deterministic system that is both highly random and sensitive to initial conditions [2]. Chaotic systems are similar to noisy systems because both are highly unpredictable. Chaotic systems have uses in cryptography because they are pseudorandom, unpredictable and sensitive to initial condition and control parameters [3]. Chaotic systems are useful for encryption because they appear to be random data and their sensitivity to initial conditions allows this randomness to be unpredicted, allowing a basis for decryption [4]. The main difference between chaos maps and chaos cryptography is that chaos cryptography is defined by finite sets, while chaos maps are defined by real numbers. The dynamic systems are said to be chaotic when they satisfy three conditions.

A. Sensitivity to Initial Conditions:

The primary requirement of the dynamic systems to be considered a chaotic is, it must be sensitive to initial conditions that is the start values of the control parameters. When the dynamic systems are iterated with a set, of initial values, it results in a trajectory and when any small changes in a trajectory and when any small changes in the initial values if the same dynamic systems should produce a trajectory that is entirely different from the first set of values. This phenomenon is technically referred to as "Butterfly Effect". The most prominent method to study the sensitivity of the systems us through the usage of "Lyapnov-Exponent", which depicts the numerical quantity to represent the long-term

divergence of trajectories given to arbitrarily close initial values.

$$|\delta z(t)| \approx e\lambda t|\delta Zo|$$

Where λ is the Lyapnov exponent.

With this property, obtaining the correct output is highly dependent on the key (initial values) and even a single bit change will result in entirely different trajectory.

B. Topological Mixing:

The term mixing in mathematics refers to the process that is irreversible, where topologically mixing means that nay given open subset of the domain will eventually, intersect with any given open subset of the range of the function

$$B \cap fn\ (A) \neq \emptyset$$

A, B—> open subsets of domain and range

fn —>n iteration of the chaotic function 'f'

This property is significantly desirable for cryptography which means that given any initial values, eventually be mapped to every possible output which resist the probabilistic attacks against cipher.

C. Density of Periodic Orbits:

The final requirement for a dynamic system to be considered on a chaotic system is, it must have dense periodic orbits is defined on the orbit obtained due to the oscillations of the dynamic system between a finite set of values.

Thus, in order for a dynamical system to have dense periodic orbits at any point in the range of the function must be approached arbitrary close to periodic orbits.

A chaotic dynamical system is a deterministic system that exhibits significant random behavior as it is highly sensitive to initial conditions. The above-mentioned properties make the chaotic systems unpredictable and thereby resembles noise. This close relationship between chaos and cryptography have a significant application in secure communication. Chaos in cryptography makes the encryption process easier to execute, high speed and are immune to most of the attacks [5].

The encryption process on image using chaos is performed by using chaotic maps. The chaotic maps resemble and will have all the properties and requirements of the system to be chaotic such as sensitivity to initial conditions, randomness, unpredictable, etc., this makes the chaotic maps the best alternative for cryptographic algorithms. The key principle behind encryption of images are we need a system that generates a true random number and image pixels are encrypted based on those random numbers[6].

The key difference between the chaotic maps and cryptographic algorithm to be noted is that the transformation obtained through the process of encryption are defined as finite sets whereas the chaotic maps are valid only for real numbers. There are two basic ways to use a chaotic map in crypto system. Either chaotic maps can be used to generate the pseudo random key stream which can be used for the encryption process which resembles the characteristics of stream cipher. Any plain text or a secret key can be used as the initial conditions or control parameters such that any small change in the key at receiver side may result in a noise like output where this approach resembles the characteristics of block ciphers.

There are few similarities between the chaotic systems and cryptographic algorithms as mentioned in the table 1.

Table.1. Cryptography Algorithm

Chaotic System	Cryptography Algorithm
Parameters(Real)	Key(Boolean)
Sensitive to the initial conditions and control parameters	Diffusion
Iterations	Rounds
Set of real numbers	Finite set of integer numbers
Structure Complexity	Algorithm Complexity

IV. CHAOS BASED GENERAL IMAGE ENCRYPTION SCHEME

The basic approach to chaos based crypto systems consists of two phases, they are confusion and diffusion. The functioning of basic chaos-based image encryption process can be explained with the block diagram shown in fig,1.

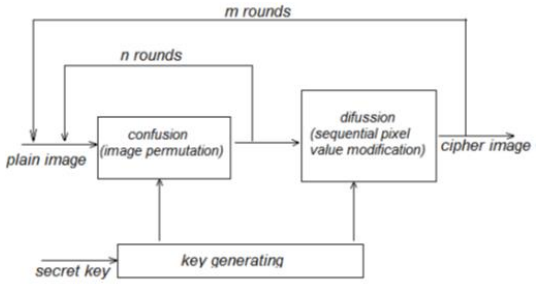

Fig. 1. Chaos Based Image encryption Idea.

The straightforward approach to the chaos-based image encryption has two phases of operations. They are phase 1 is

termed as the confusion phase or pixel permutation phase. In this phase, the pixel positions are changed over the entire image such that the image becomes unrecognizable. This process is sometimes referred to as pixel scrambling. Scrambling is done by the setting the initial conditions and control parameters to the chaotic map which serves as the key and it is iterated for several times to increase the scrambling. However, the image becomes unrecognizable. It is not secure to have only the confusion phase, as they are prone to most of the attacks. Furthermore, the scrambled image is further passed over the second phase known as the diffusion phase. This process aims to change the value of pixels in the entire image. The change in the pixel value is achieved by using a chaotic map by using initial conditions and control parameters as the key and this process is fed back to the phase 1 and iterated for several rounds to achieve the satisfactory level of security. The randomness property of the chaotic maps makes it more suitable for image encryption [7].

V. Parameters For Security Analysis

Any encryption process is done to secure the data from unauthorized users. It is not only important to develop the encryption algorithm to secure the data but also it is equally important to check for the vulnerabilities of the encryption process at all levels ensuring the robustness of the securing algorithm. In this aspect, there are several parameters to be analyzed especially for image encryption algorithms. Some of the most common attacks to encrypted images are discussed in [8,9].

A. Key Space Analysis

Key space in cryptography refers to the set of all possible combinations of key. One way an adversary could do the decrypt the data is to try all possible combinations of key. Thus, size of keys defines the time taken to try all possible keys. The time taken will exponentially increase the size of the key. Hence, the key space should be large enough so that the time taken to try all possible keys will take years together. In addition, analysis males the cryptosystem more robust against brute force attack.

B. Key Sensitivity Analysis

This analysis defines the level of sensitivity of the encryption/decryption process to the key applied. Even a single bit change in the key should result in an entirely different encrypted/ decrypted image. This analysis shows the impact of the key with the actual message. This analysis is more crucial to determine the robustness of the cryptosystems again known plain text attacks.

C. Histogram Analysis

This analysis is essential to check the strength of cryptosystem against the statistical attack. Statistical attack is performed by trying to exploit any characteristics of the encrypted image. In case of image encryption, the correlation between the two pixels or adjacent pixels may reveal any clue about the characteristics of original image. Similarly, the histogram of the image is the measure of distribution of pixels at various intensity levels. A good encryption should result in a flat histogram so that it contains equal number of pixels at all intensity levels, which does not reveal any clue or characteristics of the image. The randomness of the chaotic system makes the encrypted image to look like noise so that there will be not any resemblance to the plain image.

D. Correlation Coefficient Analysis

The resemblance between the two pixels either in horizontally, or vertically or diagonally or adjacent duration could reveal the characteristics of the cipher image which intern paves way for statistical analysis attack. It is significant to consider the correlation among the pixels in the same image as well as plain image and cipher image. If the correlation coefficient is higher, then that implies there are more similarities between the plain and cipher image, which in turn makes the crypto system more vulnerable or statistical attack. This can be minimized by proper solution of confusion and diffusion stages.

E. Entropy Analysis

The term entropy defines the level of uncertainty in the cipher image in other words the predictability of the cipher image using the probability of occurrences of pixel in cipher image when the entropy is higher; the outcomes are all have the equal probability lesser the entropy the probability of outcome is less so becomes predictable. Entropy in other words is defined as the measure of surprise.

F. Differential Analysis

Differential crypto analysis is the process of exploiting the similarities or finding the relation between the plain image and cipher image. This attack has introduced in the year 1980's. This is almost similar to known plain text attack. The adversary uses a pair of plain text related by a constant difference. This difference is defined in several methods. Then the adversary computes the differences of the cipher texts. Then exploits the statistical pattern in this distribution usually these statistical patterns depend upon the key or map used in the encryption. This analysis is essential to find the sensitivity of encryption process to any slightest change in the key. A good encryption algorithm should have a significant change in the output even if there is a bit change in the key. This measure of differential cryptanalysis is estimated in two

ways, such as NPCR that is number of pixel change rate which defines the percentage of various pixel numbers between two cipher images, whereas whose plain images differ from only one pixel.

VI. Study Of Various Chaotic Maps

As discussed in previous section the chaos-based encryption scheme undergoes two stages such as confusion and diffusion phases. These phases are done by employing various chaotic maps to achieve proper confusion and diffusion for robust encryption. This section summarizes the various chaotic maps employed in image encryption.

The chaotic maps will be chosen such that it has a robust nature, good mixing property and wider control parameters [10]. The following figure shows the classification of chaotic maps.

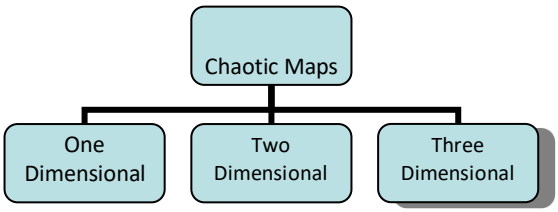

Fig. 2. Classification of Chaotic Maps

One Dimensional Chaotic Map:

A. Logistic Maps

Logistic maps are polynomial maps which has a degree of 2, this map was proposed by Robert May in the year 1976. Logistic maps are expressed as

$$rn{+}1= \alpha rn\ (1-rn)$$

Where, rn takes any value from 0 to 1.

n is the number of iteration;

α is the control parameter with the interval [1,4].

In logistic maps r0, α act as the initial conditions and is expressed as (r0 , ∞) where r0 takes any value between [0,1] initially. These maps are used to shuffle the coordinates of rows and columns to disperse the original image [R8]. This logistic map may be repeated any number of times to get the better dispersion of the plain image.

Logistic maps comes with certain drawbacks such as the key space is very small and the chaotic behavior is expressed within the range (3.57,4) for α. For the values greater than 4 (i.e. $\alpha > 4$). The maps return negative values.

B. Tent Maps

Tent maps are expressed as

$$rn{+}1= f(rn,\beta)= \beta rn, \quad rn<0.5$$
$$(1-rn), \quad rn\geq 0.5$$

Where $\beta \in (0,2)$; β and rn are the control parameters and is expressed as (β ,rn).

The behavior of the tent map is almost similar to the logistic map and they share the limitations i.e. range. When β exceeds beyond to the maps results in negative values. The limitations lead to that the encryption algorithm with pure tent map becomes vulnerable for statistical attacks. In order to overcome this problem, the tent maps are used jointly with other maps such as sine maps, which considerably increase the key space and wider control parameters. The sine map is expressed as

$$rn{+}1= \beta s Si(\pi rn)$$

When βs is the control parameter and it takes any value between 0 and 1;

r0 is the initial condition. Pure sine maps also exhibits certain drawbacks for the value $\beta s=0.941$.

The system is not chaotic and it produces periodic signals at the output, which makes it not suitable for encryption algorithms.

C. Skew Maps

The asymmetric version of tent map is also set to be skew map and it is expressed as

$$r_{n+1}= r_n\beta_s \ ; \ r_n \epsilon [0,\beta_{sk}]$$
$$(1-r_n)/(1-\beta_{sk}) \ ; \ r_n \epsilon [\beta_{sk},1]$$

Where β_{sk} is the control parameter and it takes any value between 0 and 1, $\beta_{sk} \in (0,1)$.

These maps have better dispersion rate than compared to the tent maps and sine maps. Thus, these maps are widely used in most of the cryptographic applications [11].

D. Piecewise Linear Chaotic Map

The piecewise chaotic map is expressed as

$$rn{+}1=f(rn,\gamma)= rn/\gamma \ , \quad 0\leq rn < \gamma$$
$$rn-\gamma/0.5-\gamma, \quad \gamma \leq rm<0.5$$
$$f(1-rn,\gamma), \ 0.5\leq \gamma m<1$$

Where γ is the control parameter and it takes any value between 0 and 0.5.

The map exhibits the chaotic behavior when $\gamma \in (0,0.5)$ such

IJPRSE
Progressive Research
International Journal of Progressive Research in Science and Engineering
Volume-2, Issue-2, February-2021
www.ijprse.com

that γ can be used as the secret key.

The merits of the maps are they possess uniform invariant distribution and better random sequence generation, which makes this map more suitable for image encryption. This map is more suitable for generating a key with larger key space rather than using for confusion and diffusion process.

Two Dimensional Chaotic Map:

A. Henon Map

Henon map is expressed as

$$rn+1=Pn+1=1-\alpha Pn2+qn$$

$$qn+1=\beta Pn$$

The Henon map depends on two parameters (α,β) , where α = 1.4 and β = 0.3.

The p and q are the two points on the image. Henon map exhibits chaotic behavior when the control parameter α,β has the values 1.4 and 0.3 respectively. The Henon map output may not be chaotic or converge to a periodic output for any other values of α, and β. In cryptographic algorithms, Henon maps are used to change the values of the pixels rather than using for confusion and diffusion [12].This Henon map may be iterated for any number of times for better resistance to brute force attack.

B. Baker Map

Baker map is a chaotic bi junction of unit M*M matrix. They are primarily used to change the position of pixels without altering or changing the values of pixels. The basic 2D baker's map is expressed as

$$Pn+1=\Gamma aPn \quad if\ qn<\alpha$$

$$(1-\Gamma b)+\Gamma bPn \quad if\ qn>\alpha$$

$$qn+1=qn/\alpha \quad if\ qn<\alpha$$

$$(qn-\alpha)/\gamma \quad if\ qn>\alpha$$

Where γ=1-α, Γa+ Γb≤ 1 and p,q are computed mod 1.

In many literature researchers have proposed the extended version of baker's map which is more faster than 2D map [13].

C. Arnold's Cat Map:

Arnold cat map relays on the concept of linear algebra to change the position of the original image. The plain image is segregated into blocks and Arnold transformation is performed on the image. Arnold cat map is given by,

Let $X = \begin{bmatrix} x \\ y \end{bmatrix}$ be a nxn matrix and the Transformation is expressed by,

$$T_{arnold}\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} 1 & a \\ b & 1+b \end{bmatrix}\begin{vmatrix} x \\ y \end{vmatrix} mod\ n$$

This transformation shuffles the position of the pixels and makes the image to appear like noise but the drawback of this map is that when iterating the image over a period in certain level of iteration the characteristic of original image is revealed in most of the cases. The original image itself appears at various level of iteration [14].

Three Dimensional Chaotic Map:

A. Chebyshev Map:

The Chebyshev polynomial map is expressed by

$$Cn(x) = \cos(n*\arccos(x))$$

$$Cn(x) = 2*x*Cn-1(x) - Cn-2(x)$$

Where C0(x) = 1 and C2(x) = x for n ≥ 2

Due to the semigroup property and chaos property of Chebyshev polynomial map the maps makes it self-more suitable for encryption algorithms. The have excellent confusion and diffusion properties. Many extended versions of Chebyshev chaotic maps are also proposed in literature [15].

Most of the basic chaotic maps are studied in detail and each and every maps have their own merits and demerits in terms of key space, space perseverance computational complexity etc., In order to overcome the drawbacks of certain chaotic map, they are used in combinations i.e, two or more chaotic maps were also proposed in the literature such as 3D Tent map, modified sine map, unfolded Baker map, Chebyshev map etc.,. These extended versions of chaotic maps yields advantages such as improved confusion/diffusion properties, computational time, faster than traditional algorithms etc.

VII. Analysis Of Different Chaos Based Encryption Techniques

In this section the various works done by the researchers using chaotic maps in the field of image encryption are compares and their performance is evaluated with respect to few parameters such as key space analysis, key sensitivity analysis, correlation coefficient analysis, entropy, NPCR and UACI. The following table summarizes the various image encryption schemes and their results are compared with other schemes of encryption.

Chaotic Map Used	Ref No.	Year	Key Space	Key Sensitivity	Correlation Coefficient	entropy	NPCR	UACI
Chirikov Map	[16]	2019	2167	High	0.0088	7.9902	99.62	33.464
Chebyshev Map	[17]	2019	2716	High	-	7.9993	99.6	33.4
Modified lorenz map	[18]	2018	2286	-	-	7.999	99.7	33.58
Logistic adjusted SINmap	[19]	2018	2100	-	0.001	7.176	99.6	33.4
Henon	[20]	2012	2128	High	0.0096	7.99	0.002	0.0005
Arnold map	[21]	2011	2147	High	-0.0041	-	0	0
Circle map	[22]	2011	2256	High	0.0012	7.9902	99.63	33
ACM	[23]	2011	2148	High	0.001	7.9981	99.62	33.19
Lorenz & Chen	[24]	2011	Large	High	0.0052	-	-	-

VIII. CONCLUSION

The security of digital images has become important for communication over networks and the internet. In this survey paper, the existing chaos based image encryption schemes have been discussed and analyzed to validate their performance against different types of attacks. This paper also compares the performance of various chaos based image encryption schemes. To conclude, all the encryption schemes are useful for real time image encryption and each scheme is unique in its own way which is appropriate for different applications. Security can be enhanced by having multiple chaotic maps for image encryption.

REFERENCES

[1]. Monisha Sharma, Manoj Kumar Rowar "Image Env\cryption techniques using Chotic schemes: A Review", International Journal of Engineering Science and Technology Vol 2(6),2010, pp2359-2363.

[2]. Priya R. Sankpal, PA Vijaya. Image Encryption Using Chaotic Maps: A Survey. In Signal and Image Processing (ICSIP), 2014 Fifth International Conference. 2014: 102-107.

[3]. Sankpal, Priya R, PA Vijaya. Image Encryption Using Chaotic Maps: A Survey. Signal and Image Processing (ICSIP). Fifth International Conference on. IEEE, Jan 8 2014: 102-107.

[4]. Somaya Al-Maadeed, Afnan Al-Ali, Turki Abdalla. A new chaos-based image-encryption and compression algorithm. Journal of Electrical and computer Engineering. 2012: 15.

[5]. Abhinav Srivastava,"A Survey Report on Different techniques of image encryption", International journal of Emerging Technology and Advance Engineering, ISSN 2250-2459, Vol 2, Issue 6, June 2012.

[6]. Pooja Mishra, Biju Thankachan," A Survey on Varioud Encryption and Key Selection Techniques", International journal of Engineering and Innovative Technology, Vol 2, Issue7, January 2013, ISSN:2277-3754.

[7]. Alireza Jolfaci, Abdolrasoul Mighadri, "An Image Encryption Approach Using Chos and Stream Cipher", Journal of Theoretical and Applied Information Technology, pp 117-123.

[8]. Shah.J., Dhobi.J.S., "Review of Image Encryption and Decryption Techniques for 2D Images.

[9]. Alireza Jolfaei, Abdolrasoul Mirghadri, "An Image Encryption Approach using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, pp 117 – 123.

[10]. K.Sakthidasan Sankaran and B.V.Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of information and Educational Technology, Vol. 1, No. 2,June 2011.

[11]. Ali Soleymani, Zulkarnain Md Ali, and Md Jan Nordin, "A Survey on Principle Aspects of Secure image Transmission", World Academy of Science, Engineering and Technology 66 2012, pp 247 – 254.

[12]. D. Chattopadhyayl1, M. K. Mandall and D. Nandi, "Symmetric key chaotic image encryption using circle map", Indian Journal of Science and Technology, Vol. 4 No. 5 (May 2011) ISSN: 0974-6846, pp 593 – 599.

[13]. Parvaz. R, & Zarebnia. M. (2018). A combination chaotic system and application in color image encryption. Optics & Laser Technology, 101, 30-40.

[14]. Elabady. N. F., Abdalkader, H. M. Moussa, M. I. & Sabbeh. S. F. (2014, April). Image encryption based on new one-dimensional chaotic map. In Engineering and Technology (ICET), 2014 International Conference on (pp. 1-6).

[15]. Yuping Hu, Congxu Zhu, and Zhijian Wang, "An Improved Piecewise Linear Chaotic Map Based Image Encryption Algorithm," The Scientific World Journal, vol. 2014, Article ID 275818, 7 pages, 2014.

[16]. Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen, "A chaos-based digital image encryption scheme with an improved diffusion strategy", Optical Society of America, 30 January 2012 / Vol. 20, No. 3 pp 2363 – 2378.

[17]. Akram Belazi, Muhammad Talha, Sofiane Kharbech, Member, IEEE, and Wei Xiang, Senior Member, IEEE " Novel Medical Image Encryption Scheme Based on Chaos

and DNA Encoding", Institute of Electrical and Electronics Engineers (IEEE), 2019.

[18]. M Kaur, V Kumar, "Efficient image encryption method based on improved Lorenz chaotic system", Electronics Letters, 3rd May 2018, Vol. 54, No. 9, pp. 562-564.

[19]. Ping Ping1, Jinyang Fan1, Yingchi Mao1,, Feng Xu1, Zeyu Gao2, "A chaos based image encryption scheme using digital-level permutation and block diffusion", Institute of Electrical and Electronics Engineers (IEEE), 2018.

[20]. Somaya Al-Maadeed, Afnan Al-Ali, and Turki Abdalla, "A New Chaos-Based Image-Encryption and Compression Algorithm,"Hindawi Publishing Corporation, Journal of Electrical and Computer Engineering, Volume 2012.

[21]. Shima Ramesh Maniyath1 and Supriya M, "An Uncompressed Image Encryption Algorithm Based on DNA Sequences, Computer Science & Information Technology (CS & IT), CCSEA 2011, CS & IT 02, pp. 258–270.

[22]. D. Chattopadhyay1, M. K. Mandal1 and D. Nandi, "Symmetric key chaotic image encryption using circle map", Indian Journal of Science and Technology, Vol. 4 No. 5 (May 2011) ISSN: 0974- 6846, pp 593 – 599.

[23]. Kamlesh Gupta1, Sanjay Silakari, "New Approach for Fast Color Image Encryption Using Chaotic Map", Journal of Information Security, 2011, 2, 139-150.

[24]. K.Sakthidasan Sankaran and B.V.Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, Vol. 1, No. 2, June 2011.