Enhancement and Analysis of Chaotic Image Encryption Algorithms

R.Raja Kumar[1], Dr.A.Sampath[2] and Dr.P.Indumathi[3]

[1]Department of Mathematics, Sathyabama University, Chennai, Tamil Nadu, India.
rrkmird@yahoo.com
[2] Department of Mathematics, Sathyabama University, Chennai,Tamil Nadu, India
dr_asampath@yahoo.co.in
[3]Department of Electronics Engineering, Anna University, Chennai, Tamilnadu, India.
indu@mitindia.edu

ABSTRACT

The focus of this paper is to improve the level of security and secrecy provided by the chaotic map based image encryption.An encryption algorithm based on the Logistic and the Henon maps is proposed. The algorithm uses chaotic iteration to generate the encryption keys, and then carries out the XOR and cyclic shift operations on the plain text to change the values of image pixels. Chaotic Map Lattice based image encryption algorithm suggested by Pisarchik is also examined which is based on Logistic map alone. In experiments, the corresponding results showed the proposed method is a promising scheme for image encryption in terms of security and secrecy. At the end, we show the results of a security analysis and a comparison of both schemes.

KEYWORDS

Image Encryption, Security, Chaotic Map Lattice, Binary sequence, Key space.

1. INTRODUCTION

Discrete chaotic dynamical systems are nonlinear, exponentially sensitive to changes of initial conditions, while the systems themselves are ergodic or mixing, are equiprobable and asymptotically statistically independent. Moreover, chaos may occur even in simple recursive equations. These properties are very good from cryptographic point of view, which was intuitively described even by Shannon [1], when he was introducing the concept of mixing in the information theory field. Analogies between features of chaotic systems and properties of good cryptosystems are widely known [2–4]. The main problem, still unsolved is how to transfer chaos into finite-state space-valued digital systems[5]. Despite this, scientists are still trying to find a cryptographic application of mathematical tools of the chaos theory. Many ideas concentrate on ciphers based on discrete (in time) chaotic maps. The first cipher of this class was proposed in 1991 by Habutsu *et al.* [6]. This cipher was easily broken [7]. The second idea was to insert the key into the initial condition of a dynamical system, proposed by Kotulski and Szczepanski [8].

D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 143–153, 2011.

DOI: 10.5121/csit.2011.1215

Afterwards, Baptista [9] suggested a cryptosystem, in which both the initial condition and the control parameters played the role of a secret key. In the next cryptosystem, [10], the inspiration was a thermo dynamical model of a gas particle, enclosed in a container, which is subject to a chaotic reflection law.

This time the map was two-dimensional and the key was one of the two initial conditions. Two-dimensional dynamical systems (previously agreed between communication sides) were a base of the cryptosystem introduced by Alvarez *et al.* [11]. In all of these systems the number of iterations of a chaotic map was limited on the one hand by the condition of obtaining a statistically good ("random") cipher text, on the other hand by the time of computation. These conditions along with the usage of the map and the parameters constituting the key became typical for most of the proposed ciphers. A more detailed review of propositions may be found in [12]. There are attempts to apply discrete in time, chaotic systems also in image encryption. Image encryption is connected with some specific problems [13], such as: huge redundancy and large size of data, strong correlation between pixels, compression, different significance of bits (to human eye), and speed of computation (sometimes more important than high security level), etc. In many applications, conventional encryption schemes are not suitable [14].

In this paper, an image encryption algorithm based on the Logistic and the Henon maps, which ensure the safety of the remote transmission, was proposed. The proposed algorithm II, using chaotic iteration to generate the secret key, combines the merits of the two chaos systems and makes use of the characters of chaotic systems, which are sensitive to the changes of initial values and parameters, to construct a pseudorandom number generator. And then the sequences, which are generated by the chaotic maps, are carried out with the XOR and cyclic shift operations with the clear text.

The paper is organized as follows. In section II, we discuss two Chaos systems. In section III, we discuss the CML based encryption algorithm suggested by Pisarchik with the two proposed algorithms. We present our results in section IV. Finally, we give conclusions in section V.

2. Chaos Systems

Chaos based image encryption methods are considered good for practical use because they have important characteristics like (i) they are very sensitive to initial conditions/system parameters, (ii) they have pseudo-random property and non-periodicity as the chaotic signals are usually noise-like, etc. All these characteristics make chaos an excellent and robust cryptosystem against any statistical attacks.It is more secure because it is difficult to synchronize the unknown chaotic system. Chaotic behaviour is too difficult to predict by analytical methods without the secrete key being known. Even if the initial conditions that the opponent tries are very close to the ones used to encrypt the data, the opponent will still get gibberish as output. [15]

2.1 Logistic map

$$X_{n+1} = aX_n(1 - X_n), \qquad (1)$$

Where Xn and a are the system variable and parameter, respectively, and n is the number of iterations. Logistic map is chaotic for $3.57<a < 4$. The Logistic map has only one parameter, and its range is relatively narrower than other chaotic maps. [16]

2.2 Henon map

$$X_{n+1} = 1\text{-}aX_n^2 + bY_n \qquad (2)$$
$$Y_{n+1} = X_n$$

The well-studied Henon map presents a simple two dimensional map with quadratic non-linearity. This map gave a first example of the strange attractor with a fractal structure. Because of its simplicity, the Henon map easily lends itself to numerical studies. Thus a large amount of computer investigations followed. Nevertheless, the complete picture of all possible bifurcations under the change of the parameters *a* and *b* is far from completion. If one chooses a = 0.3, b =1.4, the system is chaotic as shown by Figure.1. This feature is very useful in image encryption. [17]

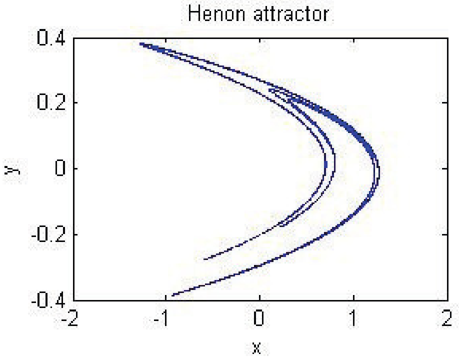


Figure 1. Chaotic behavior of Henon system

One dimensional logistic map was used for image encryption in existing algorithm suggested by Pisarchik. The proposed algorithm combines the Logistic and Henon maps to expand the parameters, so as to fulfill the purpose to enhance security.

3. Image Encryption Algorithms

Chaos based image encryption algorithm suggested by Pisarchik and proposed algorithm are explained below.

3.1 Existing Algorithm

In the Choatic Map Lattice based image encryption algorithm suggested by Pisarchik, the image colour is converted to chaotic logistic maps, pixel by pixel, one way coupled by the initial conditions. The algorithm is as follows [18].

(i) The colour value C of each pixel is converted to the corresponding values of the map variable X_c.

$$X_{min}=0.095062, \; X_{max}=0.975, \; \delta x=X_{max}-X_{min}$$
$$X_c = X_{min} + \delta x(C/255) \qquad (3)$$

(ii) The colour value x_c^m of the last map *m* is used as the initial condition for the first map (*i*=1), i.e., $x_0^1 = x_c^m$.

(iii) After n iterations of the first map by logistic map (1), map variable x_n^1 is obtained and the colour value of the pixel x_c^1 is added to x_n^1. This sum value is used as the initial condition for the map 2. Similarly, all maps are iterated, from first to last map and the coupling direction, in which the values of map variables are updated, is shown in Figure 2.

(iv) All steps are repeated for each colour component and three images are superimposed to get the encrypted image.

To restore the original image, the algorithm is applied in the reverse direction step by step, starting from the last map and moving to the first one by going through same number of iterations for each map as for the encryption.

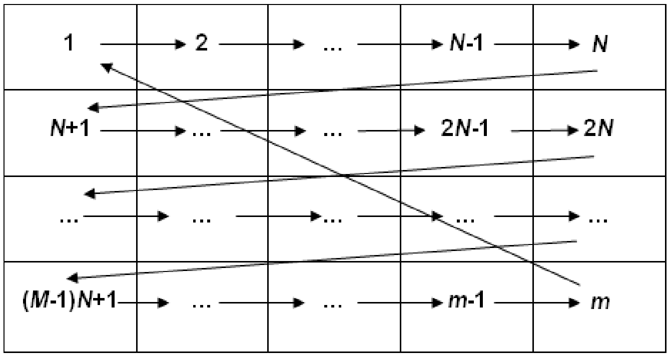


Figure 2: Coupling direction in Pisarchik algorithm

Xn(1)+Xc(1)	Xn(2)+Xc(2)	……	Xn(N-1)+Xc(N-1)	Xn(N)+Xc(N)
Xn(N+1)+Xc(N+1)	……	……	Xn(2N+1)+Xc(2N+1)	Xn(2N)+Xc(2N)
……	……	……	……	……
……	……	……	Xn(m-1)+Xc(m-1)	Xn(m)+Xc(m)

Figure 3: Map variables

3.2 Proposed Algorithm I

In the Pisarchik algorithm, the value of the next map variable depends upon the coupling direction. Pisarchik et al. chose the horizontal direction to update the value of the next map variable using the previous map variable as the initial condition, as seen in the Figure 1. The secret key of the algorithm consists of four numbers: the control parameter a, the number of iterations n, the number of cycles j and the size of the image m=N×M, i.e. the 4-tuple (a; n; j; m). If we alter the coupling direction, then we have a different set of values of map variables and the values of initial condition also changes with the changed direction for the next map variables to be calculated.

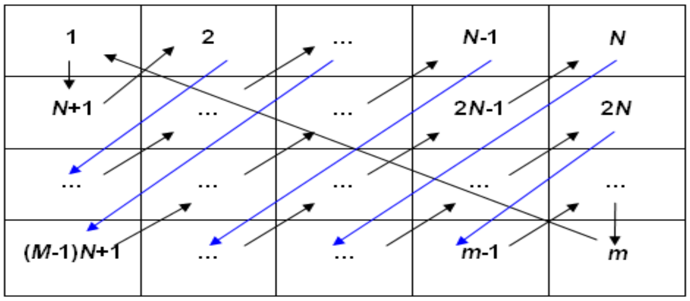


Figure 4: Coupling direction in proposed algorithm

Therefore, computer simulation is done to see the effect of altering the coupling direction on the encrypted images. In the proposed algorithm I, the coupling direction depicted in Figure 4 is chosen. The colour value x_c^m of the last map m is used as the initial condition for the first map x_0^1.After iterating the first map *n* times, map variable x_n^1 is obtained and the colour value of the pixel x_c^1 is added to it. Now, the sum value is utilized as the initial condition for the map *N*+1.

3.3 Proposed Algorithm II

The encryption algorithm can be divided into the following 9 steps:

Step 1: Convert the image I into binary, and then divide I into a series of sequences in length (t) of 128-bit. If the length of the last sequence is less than 128, fulfil it with 0.

Step 2: Get a clear text sequence P(128 bits), and divide it into two parts P_1(64 bits) and P_2(64 bits).

Step 3: Provide the initial value x_1 and parameters μ_1 and n, iterate (1) for n times, then select the last 3 integers as S_1, S_2, S.

Step 4: Carry out circle right shift with P_1 and P_2 for S_1 and S_2 bits respectively, then generate a new P(128 bits) by combining the two parts(P_1 , P_2) together.

Step 5: Give initial value X_2 and parameter μ_2 ,calculate the chaotic sequence X_n according to (1), the chaotic sequence $X_n \in (0,1)$,n is the number of the iterations, hence we can obtain one sequence a_n ,a is the nth value of sequence a_n which is chosen as the initial value of the Henon map.

Step 6: Iterate Henon map (2) to generate two chaotic sequences X_n and Y_n , using the initial values of x_1 and y_1, which values can obtain from the below given expressions.

$$X_1=(S+1)/257 \qquad (4)$$
$$Y_1=S/257$$

Step 7: Convert X_n into binary, and then obtain the intermediate cipher text E by carrying out the XOR operation with P. Last cyclic right shift S bits on E, and obtain the final cipher text En.

Step 8: Stop, if clear texts are all encrypted, else get the next sequence and repeat the encryption procedure from step 2.

Step 9: To get encrypted image convert these binary numbers into color values for the each pixel.

To get the decrypted image the algorithm is applied in reverse direction, After converted into binary, ciphered image will be carried out the XOR operation and the cyclic shift operation with decryption sequences, which could be obtained after the reverse process of the encryption algorithm, then the decrypted image will be obtain[19].

4. SIMULATIONS AND RESULTS

The two algorithms are implemented in MATLAB for computer simulations. For the experimentation purpose, we consider the picture "Nature" as the one original digital image to make a useful comparison. The original image is shown in Figure 5(a). This RGB image is encrypted by using the Pisarchik algorithm and the proposed algorithms. The results of encryption using Pisarchik algorithm and proposed algorithm I are shown in Figure 5(b), 5(c). It can be seen that after applying Pisarchik algorithm and proposed algori8thm I to the RGB original image, still it is distinguishable because the original outlines and patterns are present in the encrypted images. When the original image is encrypted by proposed algorithm II, the image shown in Figure 5(d) is obtained. We can see that this image is much more distorted and indistinguishable encrypted images shown in Figure 5(b),5(c).In the encrypted image no original outlines and patterns are present.

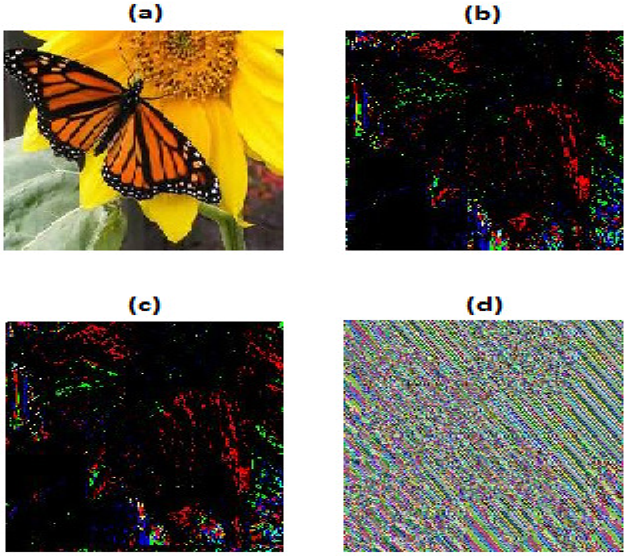


Figure 5: Encryption results (a): Original image of picture "Nature". (b): encrypted image by Pisarchik algorithm. (c): encrypted image by proposed algorithm I, (d): encrypted image by proposed algorithm II.

.

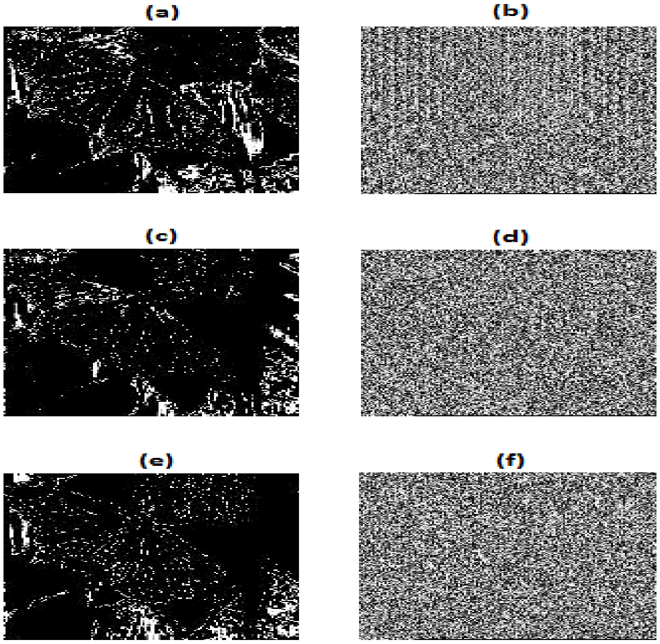


Figure 6: Encryption results. (a),(c) and (e): Red, Green, Blue planes of encrypted image by Pisarchik algorithm respectively.(b),(d) and (f): Red, Green, Blue planes of encrypted image by Proposed algorithm respectively.

For better understanding we can compare Red, Green, Blue planes of the encrypted images by both the algorithms. Red, Green, Blue planes of the encrypted image by using Pisarchik algorithm are shown in Figure 6(a), 6(c) and 6(e) respectively. Red, Green, Blue planes of the encrypted image by using proposed algorithm are shown in Figure 6(b), 6(d) and 6(f) respectively. It can be viewed and analysed that Red, Green, Blue planes of encrypted image by using pisarchik algorithm still have outlines of the original image and some patterns .But the Red, Green, Blue planes of encrypted image by using proposed algorithm are indistinguishable, there are no outlines or patterns of the original image present in these planes

4.1. Response to changes in Plain images

The proposed algorithm has one of the desirable properties, it is more sensitive to a small change in the plain images than the Pisarchik algorithm. In order to test the changing rate of pixel in the plain image on the encrypted image, we have measured the number of pixels change rate by calculating the number of pixel change rate (NPCR) and unified average changing intensity (UACI) [20]. NPCR measures the percentage of different pixel numbers between the two images. The UACI measures the average intensity of differences between the two images. Let two encrypted images, whose corresponding plain images have only one pixel difference (i.e R,G,B colour values in the first pixel is changed for experimental purpose,) be denoted by C_1 and C_2. Define a 2D array D with same size as C_1 and C_2. If C_1 (i,j) = $C_2(i.j)$, then $D(i,j)$= 0, otherwise $D(i,j)$= 1.

The NPCR is defined as

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \qquad (5)$$

and the UACI is defined as:

$$\mathrm{UACI}=\frac{1}{W\times H}\left[\sum_{i,j}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right]\times 100\%, \qquad (6)$$

where W and H are the width and height of encrypted image. It is understandable that the large values of NPCR and UACI are desirable. We performed the test for the plain images shown in Figure 5(a).

TABLE 1. SENSITIVITY TO PLAINIMAGE: NATURE

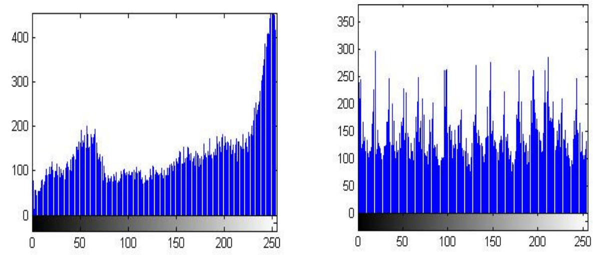
Test	Colour Components	Existing	Proposed I	Proposed II
UACI	Red	1.9528	2.1317	8.1439
	Green	1.2451	1.3317	7.6158
	Blue	1.4745	1.5519	7.8969
NPCR	Red	66.9075	67.9439	99.0107
	Green	63.7953	64.0316	98.8824
	Blue	63.6100	64.8155	98.9866

The original plain images and one pixel changed plain images are encrypted by the two algorithms. The colour values of one pixel can be changed to values between 0 to 255.The comparisons of experimental results of two images are given in Table I. NPCR and UACI are measured. It can be seen in the Table I that the values of NPCR and UACI are higher in case of proposed algorithm than the Pisarchik algorithm. Therefore, we can say that the proposed algorithm is more sensitive to a small change in the plain image than the Pisarchik algorithm.

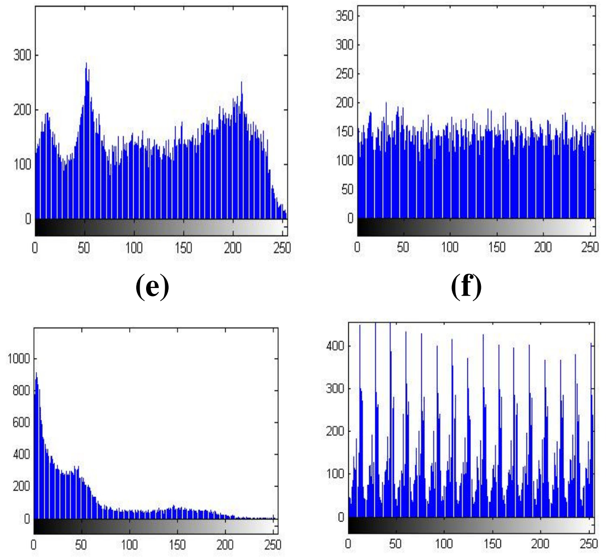
4.2 Histograms of RGB Planes

The differences between original RGB image and encrypted image can be analysed by histograms of each planes in both images. As shown by Figure.7, one of the histogram of the ciphered images is fairly uniform and is significantly different from that of the original image. In encrypted elements are equally distributed in all regions.

(a) **(b)**



(c) **(d)**



(e) (f)

Figure 7: Histogram results: (a), (c) and (e): Histograms of Red, Green, Blue planes of original image respectively.(b),(d) and (f):Histograms of Red, Green, Blue planes of encrypted image by Proposed algorithm respectively.

4.3 Key Space Analysis

Chaotic encryption schemes are symmetric key algorithms, which means same key is used for both encryption and decryption process. A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible. In Table (2) secret keys used in existing and proposed methods is given.In existing method only one parameter is used as a key. In proposed method four parameters are used as key parameters. In order to enhance the security of the encryption process the key space is enlarged in proposed algorithm by using more number of key parameters.

TABLE 2 KEY PARAMETERS AND RANGES

Secret Key used in Existing method and proposed method I	Secret Key used in proposed method II	Range
µ (3.56 to 4)	µ1, µ2	(3.56 to 4)
	a	(0 to 1)
	t	(1 to128)

Ranges of the secret key parameters are given in the Table (2). The probability of finding the secret key is very very low in proposed method than existing method

4.4 Summary

The encrypted image by proposed algorithm is more distorted and indistinguishable than the encrypted image by Pisarchik algorithm. The proposed algorithm provides more distortion to the colour digital plain images. Therefore, the proposed digital image encryption algorithm provides more security and secrecy to the colour digital images than the algorithm suggested by Pisarchik. Comparison of these two algorithms can be done by using NPCR and UACI values, it can be shown that proposed algorithm has more changes in intensity of pixels. This algorithm, from the view of security, combines the Logistic and Henon maps to expand the parameters, so as to fulfill the purpose to enhance security.

The need for quick encryption of bulky data like images has prompted the development of chaos-based encryption schemes, which enjoy advantages like ease of implementation and simplicity in contrast to the traditional cryptosystems like RSA [21] which rely on the complexity of computationally hard problems to ensure security.

5. CONCLUSION

In this paper an encryption algorithm based on combining two chaos systems is proposed, it changes the pixel values of image by carrying out the XOR operation with chaos sequences, which were generated by Logistic and Henon maps, and cyclic shift in binary. In proposed algorithm two chaotic systems are used, but in Pisarchik algorithm and proposed algorithm I only one chaotic system is used to encrypt the digital colour image. So in proposed method II security has been enhanced by increasing number of parameters. It is also shown that the proposed algorithm II is more sensitive to a small change in plain images. We conclude that the proposed algorithm II is cryptographically better than the algorithm suggested by Pisarchik and provides more security and secrecy to the colour digital images.

REFERENCES

[1] C.. E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, 28, 656–715, 1949.

[2] Z. Kotulski, Building block-ciphers: new possibilities, Matematyka Stosowana 4 (45),1–24, 2003.

[3] N. Masuda, G. Jakimoski, K. Aihara, L. Kocarev, Chaotic block ciphers: from theory to practical algorithms, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 53, 6, 1341–1352, 2006.

[4] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos,16, (8), 2129–2151, 2006 .

[5] D.-I. Curiac, D. Iercan, O. Dranga, F. Dragan, O. Banias, Chaos Based Cryptography: End of the Road?, Proc. IEEE Int. Conf. Emerging Security Information, Systems and Technologies,71–76, 2007.

[6] T. Habutsu, Y. Nishio, I. Sasase, S. Mori, A secret key cryptosystem by irating chaotic map, Proc. EUROCRYPT'91, LNCS 547, 127–140, Springer, Berlin 1991.

[7] E. Biham, Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at EUROCRYPT'91, LNCS, 547, 532, Springer, Berlin 1991.

[8] Z. Kotulski, J. Szczepanski, Discrete chaotic cryptography, Annalen der Physik, 509 ,(5), 381–394, 1997.

[9] M. S. Baptista, Cryptography with chaos, Physics Letter A, 240, 1, 50– 54, 1998.

[10] Z. Kotulski, J. Szczepanski, K. Górski, A. Paszkiewicz, A. Zugaj, Application of discrete chaotic dynamical systems in cryptography–DCC method, International Journal of Bifurcation and Chaos, 9, 6, 1121–1135, 1999..

[11] E. Alvarez, A. Fernandez, P. Garcia, J. Jimenez, and A. Marcano, New Approach to chaotic encryption, Physics Letter A, 263, 4–6, 373–375, 1999.

[12] S. Li, Analyses and New Designs of Digital Chaotic Ciphers, Ph.D thesis, http://www.hooklee.com/Thesis/ethesis.zip, 2005.

[13] S. Li, G. Chen, X. Zheng, Chaos-Based Encryption for Digital Image and Videos, [in:]Multimedia Security Handbook, [Eds.] B. Furht and D. Kirovski 133–167, CRC Press, Boca Raton 2004.

[14] Y. Mao, G. Chen, Chaos Based Image Encryption, [in:] Handbook of Computational Geometry for Pattern Recognition, Computer Vision,Neural Computing and Robotics, edited by E. Bayro-Corrochano, Springer, New York 2003.

[15] S.Li Shuaijun and Peng Fei, "An Encryption Algorithm for 2D Engineering Graphics' Content Based on Chaos Systems, " Young Computer Scientists, pp.1435 – 1439, Nov. 2008

[16] R.M.May., "Simple mathematical models with very complicated dynamics," Nature. VoL 261. No. 5560. pp. 459 467. Junr 10. 19761.

[17] M, Sonls, "Once more on Henon map: analysis of bifurations," Pergamon Chaos, Sotilons Fractals Vol. 7, No. 12, pp. 2215-2234, 1996

[18] P. Pisarchik, N. J. Flores–Carmona, M. Carpio–Valadez, Encryption and decryption of images with chaotic map lattices, Chaos, 16, 033118, 2006.

[19] Beilei Wang, Zhe Lin,Zhiliang Zhu,"A Chaos-based Encryption Algorithm for Industrial Design Images" in proceedings of the International Conference on Advanced Computer Control(ICACC'10),pp.255-259,2010.

[20] G. R. Chen and Y. B. Mao and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps",Chaos,Solitons &Fractals, vol. 21, issue 3, pp. 749–761, 2004 .

[21] A. Krishnamurthy, Y. Tang, C. Xu, and Y. Wang, "An efficientimplementation of multi-prime RSA on DSP processor,"in Proceedings of the International Conference on Accoustics,Speech, and Signal Processing (ICASSP '03), vol. 2, pp. 413–416,Hong Kong, April 2003.

[22] Meng Jianliang, Pang Huijing and Gao Wanqing, "New color image encryption algorithm based on chaotic sequences ranking," Intelligent Information Hiding and Multimedia Signal Processing, pp.1348-1351, Aug. 2008.

[23] YU Li, LI Yuanxiang and XIA Xuewen, "Image Encryption Algorithm Based on Self-adaptive Symmetrical-coupled Toggle Cellular Automata," Image and Signal Processing, 2008. Vol 3, 27-30 , pp.32-36, May 2008.

R. Rajakumar graduated from Sivanthi Aditanar College, Nagercoil, Tamilnadu and post graduated from Kamaraj College,Tuticorin, Tamilnadu. He has M.Phil from Madurai Kamaraj University. He is working as a Assistant Professor in the Department of Mathematics, Sathyabama University, Chennai. He has 20 years of teaching experience and is currently pursuing his research in the area of Chaos. He has 4 International papers and 5 National papers to his credit.