A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping

Musheer Ahmad
Department of Computer Engineering
ZH College of Engineering and Technology, AMU,
Aligarh, India

M. Shamsher Alam
Department of Computer Engineering
ZH College of Engineering and Technology, AMU,
Aligarh, India

***Abstract*— The combination of chaotic theory and cryptography forms an important field of information security. In the past decade, chaos based image encryption is given much attention in the research of information security and a lot of image encryption algorithms based on chaotic maps have been proposed. Due to some inherent features of images like bulk data capacity and high data redundancy, the encryption of images is different from that of texts; therefore it is difficult to handle them by traditional encryption methods. In this communication, a new image encryption algorithm based on three different chaotic maps is proposed. In the proposed algorithm, the plain-image is first decomposed into 8x8 size blocks and then the block based shuffling of image is carried out using 2D Cat map. Further, the control parameters of shuffling are randomly generated by employing 2D coupled Logistic map. After that the shuffled image is encrypted using chaotic sequence generated by one-dimensional Logistic map. The experimental results show that the proposed algorithm can successfully encrypt/decrypt the images with same secret keys, and the algorithm has good encryption effect, large key space and high sensitivity to a small change in secret keys. Moreover, the simulation analysis also demonstrates that the encrypted images have good information entropy, very low correlation coefficients and the distribution of gray values of an encrypted image has random-like behavior.**

***Keywords*—Information security, image encryption, chaotic maps, image shuffling, logistic map, information entropy.**

I. INTRODUCTION

Chaos signals are considered good for practical use because they have important characteristics such as they are highly sensitive to initial conditions and system parameters, they have pseudo-random property and non-periodicity as the chaotic signals usually noise-like, etc. Consequently, the combination of chaotic theory and cryptography forms an important field of information security. The characteristics of chaotic signals make chaos system an excellent and robust cryptosystem against any statistical attacks. Due to some inherent features of images like bulk data capacity and high data redundancy, the encryption of images is different from that of texts; therefore it is difficult to handle them by traditional encryption methods. In present years, the chaos based cryptographic algorithms have suggested some new and efficient ways to develop secure image encryption techniques to meet the demand for real-time image transmission over the communication channels. Therefore, chaos based image encryption is given much attention in the research of information security and a lot of image encryption algorithms based on chaotic systems have been proposed [1-13]. There have been many image encryption algorithms based on chaotic maps like the Logistic map [5-7], the Standard map[8], the Baker map [9, 10], the PWNLCM [11] the Cat map [12, 13], the Chen map [6, 13], etc. In order to improve the security performance of the image encryption algorithm, the concept of shuffling the positions of pixels in the plain-image and then changing the gray values of the shuffled image pixels is used. In this paper, a new block based image shuffling is proposed to achieve good shuffling effect using two chaotic maps and the encryption of the shuffled image is performed using a third chaotic map to enforce the security of the proposed encryption process.

II. CHAOTIC MAPPINGS USED

A. 2D Coupled Logistic Mapping

The two-dimensional coupled Logistic map [14] is described as follows:

$$x_{n+1} = \mu_1 x_n(1 - x_n) + \gamma_1 y_n^2 \quad (1)$$

$$y_{n+1} = \mu_2 y_n(1 - y_n) + \gamma_2(x_n^2 + x_n y_n) \quad (2)$$

Three quadratic coupling terms are introduced to strengthen the complexity of 2D Logistic map. This system is chaotic when $2.75 < \mu_1 \leq 3.4$, $2.7 < \mu_2 \leq 3.45$, $0.15 < \gamma_1 \leq 0.21$ and $0.13 < \gamma_2 \leq 0.15$ and generate chaotic sequences x, y in the interval (0, 1). The map of eqn (1)-(2) is iterated for $n = 16000$ times with initial conditions and parameters as: $x_0 = 0.0215$, $y_0 = 0.5734$, $\mu_1 = 2.93$, $\mu_2 = 3.17$, $\gamma_1 = 0.197$ and $\gamma_2 = 0.139$. The statistical analysis of x and y sequences shows that they have poor balance, autocorrelation and cross-correlation properties. The mean values of the sequences are mean(x) = 0.6456 and mean(y) = 0.6590. To improve the statistical properties of the sequences generated by 2D Logistic map, the following preprocessing is performed.

$$x_i = 10^6 x_i - \text{floor}(10^6 x_i) \quad (3)$$

$$y_i = 10^6 y_i - \text{floor}(10^6 y_i) \quad (4)$$

The mean values of the sequences after preprocessing are mean(x) = 0.5004 and mean(y) = 0.4984, which are closer to the ideal value 0.5. Now, the preprocessed sequences have better balance distribution, auto/cross correlation properties and they can be utilized in a cryptographic process.

B. 2D Cat Mapping

A 2D Cat map is first presented by V.I. Arnold in the research of ergodic theory. Let the coordinates of positions of pixels in an image are P = {(x, y) | x, y = 1, 2, 3, . . ., N}, a 2D Cat map with two control parameters [12] is as follows:

$$x' = (x + ay) \bmod(N) \quad (5)$$

$$y' = (bx + (ab+1)y) \bmod(N) \quad (6)$$

Where, a, b are control parameters which are positive integers and (x', y') is the new position of the original pixel position (x, y) of N x N plain-image when Cat map is applied once to the original. Cat map permutes/shuffles the organization of pixels of plain-image by replacing the position of the image pixel points with new coordinate. After several iterations, the correlation among the adjacent pixels is disturbed completely and the image appears distorted and meaningless. But after iterating many times it will return the original image i.e. the Cat map is periodic [13]. To deal with the periodicity of Cat map, a block based image shuffling is performed using 2D Cat map in which the control parameters of the Cat map are randomly generated by using 2D coupled Logistic map for each 8x8 block of the plain image.

C. 1D Logistic Mapping

The one-dimensional Logistic map is proposed by R. M. May [15]. It is one of the simplest nonlinear chaotic discrete systems that exhibit chaotic behavior, defined by the equation:

$$z_{n+1} = \lambda z_n (1 - z_n) \quad (7)$$

where z_o is initial condition, λ is the system parameter and n is the number of iterations. The research shows that the map is chaotic for $3.57 < \lambda < 4$ and z_{n+1} belong to the interval (0, 1) for all n. The sequence generated from eqn(7) has random-like behavior. The sequence doesn't require any type of preprocessing. The sequence generated by Logistic map of eqn(7) is used to encrypt the shuffled image.

III. PROPOSED IMAGE ENCRYPTION ALGORITHM

The proposed image encryption algorithm has two major steps. Firstly, the correlation among the adjacent pixels is disturbed completely as the image data have strong correlations among adjacent pixels. For image security and secrecy, one has to disturb this correlation. To achieve this, a block based image shuffling scheme is proposed using 2D Cat map. Then the pixel values of the shuffled image are encrypted by employing a 1D Logistic map.

The periodicity of Cat map degrades the security, because the possible attack may iterate the map continuously to reappear the plain-image, this makes the straightforward use of conventional Cat map unsafe for image security. To withstand the periodicity attack of Cat map, a new block based image shuffling scheme using Cat map is proposed in which the two control parameters a, b of map are randomly generated through a key dependent chaotic sequences. The control parameters of Cat map are the control parameters of shuffling. The shuffling effect obtained after a number of iterations depends on these parameters. In our algorithm, these control parameters are randomly generated through the chaotic sequences obtained from 2D Logistic map. The two chaotic sequences obtained from 2D Logistic map are first preprocessed through eqns(3)-(4) and then the control parameters a, b are evaluated. The process of generation of control parameters is as follows:

First the map of eqn(2) is iterated for 1000 times with initial conditions as: $x_0 = 0.0215$, $y_0 = 0.5734$, $\mu_1 = 2.93$, $\mu_2 = 3.17$, $\gamma_1 = 0.197$ and $\gamma_2 = 0.139$., these 1000 values of x and y are discarded. The map is again iterated for next nob+2 times and produces x_i and y_i, where 'nob' is the number of 8x8 sized blocks in NxN image and i=1,2, . . ., nob+2. The calculation of a_i and b_i from x_i and y_i respectively is as follows:

$$px_i = 10^{14} (10^6 x_i - \text{floor}(10^6 x_i))$$
$$py_i = 10^{14} (10^6 y_i - \text{floor}(10^6 y_i))$$

$$k_1 = (px_i) \bmod(83) + 17$$
$$k_2 = (py_i) \bmod(107) + 19$$

$$a_i = (px_i) \bmod(k_2) + 1$$
$$b_i = (py_i) \bmod(k_1) + 1$$

The control parameters a_i, b_i are made sensitive to secret keys of 2D Logistic map. As a result, the shuffling scheme becomes sensitive to a small change in secret keys. So, the attacker cannot make use of Cat map's periodicity to obtain the plain-image without secret keys. The whole procedure of new image encryption scheme is as follows:

Step 1. Suppose that the plain-image to be shuffled is I_0(x, y) of size NxN, where x, y=1, 2, 3, . . ., N.

Step 2. Divide the whole image I(x, y) into 8x8 size blocks, $B_1, B_2, \ldots, B_{nob}$.

Step 3. Apply Cat map within block B_i using control parameters a_i and b_i to shuffle the pixels of the block, where i=1, 2, 3, . . ., nob. After repeating this step for n_1 times we get partially shuffled image I_1(x, y).

Step 4. Apply Cat map within image I_1(x,y) to shuffle the whole blocks using control parameters a_j and b_j, where j=nob+1. After repeating this step for n_2 times we get another partially shuffled image I_2(x, y).

Step 5. Apply Cat map within whole image I_2(x, y) to shuffle the pixels using control parameters a_j and b_j, where j=nob+2. After repeating this step for n_3 times we get finally shuffled image S(x, y).

Step 6. Suppose that $SB_{(x,y)}$ is the binary equivalent of the decimal gray value of the shuffled image S(x, y) with pixel coordinate (x, y), where x, y=1, 2, 3, . . ., N and let KB_j is the 8-bit binary number obtained from 1D Logistic map's discrete variable z_j. The evaluation of KB_j from z_j is as follows:

KB_j = DecimalToBinary(mod($10^{14}z_j$, 256))

The function DecimalToBinary(z) converts the decimal number z to binary value and mod(x, y) returns the remainder whenever x is divided by y. The shuffled image S(x, y) is encrypted as:

$EB_{(x, y)} = SB_{(x, y)} \oplus KB_i$

Where i = N(x – 1) + y; and x, y = 1, 2, 3, . . ., N. The $EB_{(x,y)}$ is the binary equivalent of the decimal gray value of the encrypted image with pixel coordinate (x, y). The symbol $\oplus$ represents the exclusive-OR operation bit by bit. The 1D Logistic map is iterated for NxN times to encrypt all the pixels of the shuffled image. All the binary numbers $EB_{(x,y)}$ are converted to decimal numbers to get the resultant encrypted image E(x, y). The block diagram of the proposed image encryption algorithm is shown in Figure 1.

The plain-image can be recovered successfully by applying the proposed algorithm in reverse order.

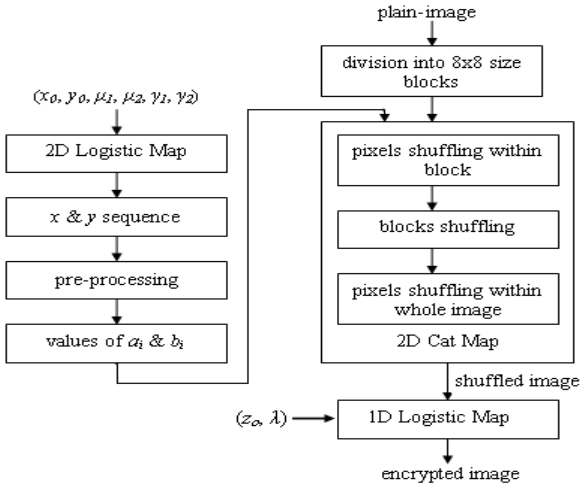

Figure 1. Proposed image encryption algorithm

IV. Experimental Results

The proposed encryption algorithm is implemented in MATLAB for computer simulations. We take a gray-scale "Lena" image of 128x128 in size for experimental purposes. The original Lena image and its histogram are shown in figure 2(a)-(b). The initial conditions and system parameters are: x_0 = 0.0215, y_0 = 0.5734, z_o = 0.3915, μ_1 = 2.93, μ_2 = 3.17, γ_1 = 0.197, γ_2 = 0.139 and λ = 3.9985. The result of proposed block based image shuffling scheme for $n_1 = n_2 = n_3 = 2$, is shown in figure 4 and the corresponding shuffling result of the same image using the conventional Cat map scheme is shown in figure 3. However, the result of proposed encryption algorithm for $n_1 = n_2 = n_3 = 2$ is shown in Figure 5. It is clear from the two shuffled images shown in figure 3 and 4 that the proposed shuffling scheme provides more distortion and more uncorrelated adjacent pixels in resultant shuffled image. Moreover, as we can see in Figure 5(b) that the histogram of the encrypted image is fairly uniform and much different from the histogram of the plain-image shown in Figure 2(b) i.e. the distribution of gray values of the encrypted image has good balance property. Hence, the encrypted image doesn't provide any information regarding the distribution of gray values to the attacker. As a result the proposed algorithm can resist any type of histogram based attacks.

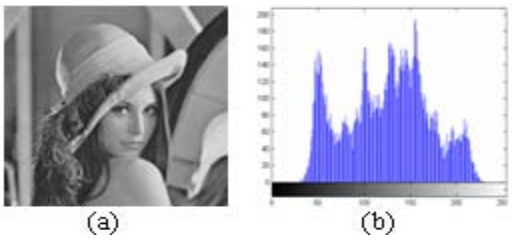

Figure 2. Plain-image and its histogram

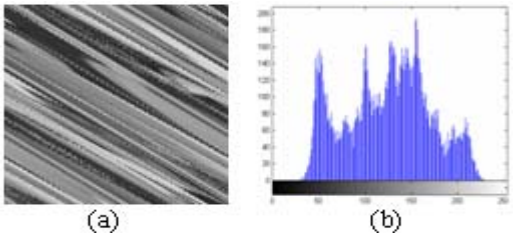

Figure 3. Shuffling result by conventional Cat map: (a) shuffled image; (b) histogram of shuffled image

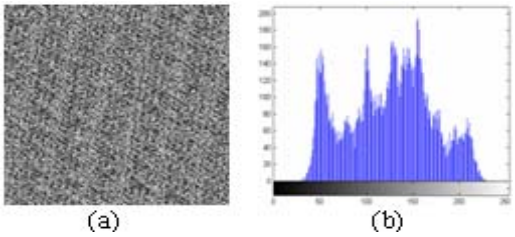

Figure 4. Shuffling result by block based shuffling scheme: (a) shuffled image; (b) histogram of shuffled image

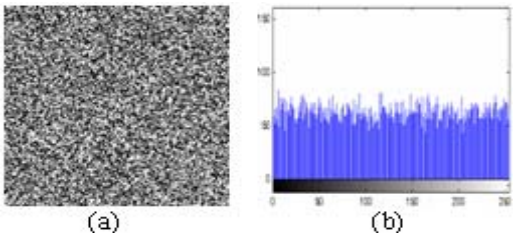

Figure 5. Encryption result by proposed algorithm: (a) encrypted image; (b) histogram of encrypted image

A. Key Space Analysis

Key space is the total number of different keys that can be used in the cryptographic system. A cryptographic system should be sensitive to all secret keys. There are total eight initial conditions of chaotic map used in the algorithm and the initial conditions for x_0, y_0, z_0, μ_1, μ_2, γ_1, γ_2 and λ can be used as secret keys of encryption and decryption. In our case, the

precision is 10^{-14}, the key space size is $(10^{14})^8$ i.e. 10^{112}, which is extensively large enough to resist the exhaustive attack.

B. Key Sensitivity Analysis

A good cryptosystem should be sensitive to a small change in secret keys i.e. a small change in secret keys in decoding process results into a completely different decoded image. Our proposed encryption algorithm is sensitive to a tiny change in the secret keys. If we change a little (10^{-14}) any of the initial conditions then the decrypted image is totally different from the plain-image. As an example, consider the original Lena image, shown in Figure 2, it is encrypted using the proposed algorithm using the initial conditions given earlier for $n_1 = n_2 = n_3 = 2$, the encrypted image is shown in figure 5. The encrypted image shown in Figure 5 is decrypted using the correct secret keys, the image obtained after decryption is shown in figure 6. It is noted that the decrypted image and its histogram are exactly same as that of the plain-image and its histogram, respectively. Hence, we can say that the proposed algorithm can successfully encrypt and decrypt the digital images without any loss of inherent information of the images.

Now, if we change one of the initial conditions, say x_0, z_0 and μ_2 a little (10^{-14}) then the decrypted images obtained are shown in figure 7(a)-(c). As we can see that the images shown in figure 7 are totally different from the plain-image shown in figure 2. Further, the decrypted images appear like a noise. Similar sensitivity is noticed for the case of wrong y_0, μ_1, γ_1, γ_2 and λ. Hence, we can say that the proposed encryption scheme is highly sensitive to a small change in secret keys.

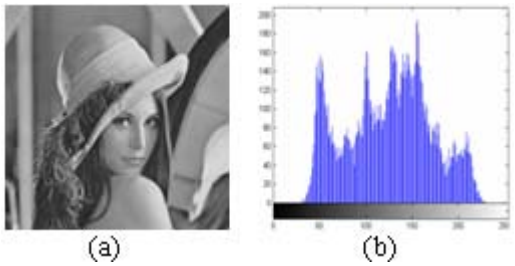

Figure 6. Decrypted image and its histogram

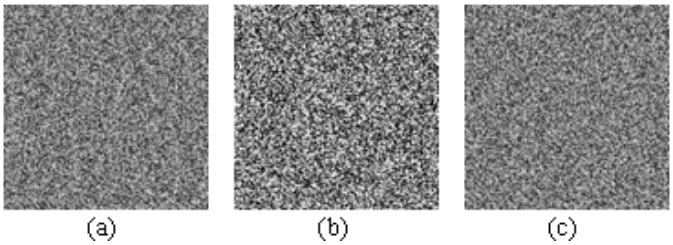

Figure 7. Key sensitivity analysis (a) decrypted image with x0=0.02150000000001; (b) decrypted image with z_o = 0.39150000000001; (c) decrypted image with μ_2 = 3.17000000000001;

C. Correlation Coefficient Analysis

In order to evaluate the encryption quality of the proposed encryption algorithm, the correlation coefficient is used. To calculate the correlation coefficients between two vertically, horizontally and diagonally adjacent pixels of an encrypted image, the following equation is used [9].

$$\gamma(x,y) = \frac{COV(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{8}$$

$$COV(x,y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)]$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

Where x and y are gray values of two adjacent pixels in an encrypted image. We randomly select 1000 pairs of vertically, horizontally and diagonally adjacent pixels and calculate the correlation coefficients in three directions separately. The correlation coefficients among adjacent pixels of plain-image in three directions come out to be 0.9535, 0.9617 and 0.9503, respectively. The values of correlation coefficients obtained in encrypted images for various iterations n_1, n_2, and n_3 are listed in Table 1. The values of correlation coefficients show that the two adjacent pixels in the plain-image are highly correlated to each other and correlation coefficients are almost 1 whereas the values of correlation coefficients in the encrypted images are close to 0, this means that the adjacent pixels in the encrypted images are highly uncorrelated to each other.

TABLE 1: CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN ENCRYPTED IMAGES FOR VARIOUS ITERATIONS

$n_1 = n_2 = n_3$	Vertical	Horizontal	Diagonal
1	0.0106	0.0095	0.0048
2	0.0044	0.0032	0.0063
3	-0.0029	-0.0007	0.0031
4	-0.0114	-0.0298	-0.0004
5	0.0087	-0.0099	-0.0139
7	-0.0058	0.0053	-0.0146
10	-0.0007	0.0093	-0.0062
15	0.0035	0.0086	0.0067

D. Information Entropy Analysis

The entropy H of a symbol source S can be calculated by following equation [16].

$$H(S) = -\sum_{i=0}^{N-1} p(s_i)\log_2 p(s_i) \tag{9}$$

Where $p(si)$ represents the probability of symbol s_i and the entropy is expressed in bits. If the source S emits 2^8 symbols with equal probability, i.e. $S = \{ s_1, s_2, \ldots, s_{256}\}$, then the result of entropy is $H(S) = 8$, which corresponds to a true random source and represents the ideal value of entropy for message source S. Information entropy of an encrypted image can show the distribution of gray value. The more the

distribution of gray value is uniform, the greater the information entropy. If the information entropy of an encrypted image is significantly less than the ideal value 8, then, there would be a possibility of predictability which threatens the image security. The value of information entropy for the plain-image is comes out to be H(*S*) = 7.3881. However, the values of information entropy obtained for the case of images encrypted by the proposed algorithm are very close to the ideal value 8, the entropy values of the encrypted images are listed in Table 2. This means that the information leakage in the proposed encryption process is negligible and the image encryption system is secure against the entropy attack.

TABLE 2: INFORMATION ENTROPY OF ENCRYPTED IMAGES FOR VARIOUS ITERATIONS

$n_1 = n_2 = n_3$	**Information Entropy**
1	7.9892
2	7.9887
3	7.9875
4	7.9890
5	7.9903
7	7.9882
10	7.9873
15	7.9891

V. CONCLUSIONS

In this paper, we presented a new algorithm of encryption and decryption of images. The algorithm is based on the concept of shuffling the pixels positions and changing the gray values of the image pixels. To perform the shuffling of the plain-image's pixels, a block based shuffling scheme is proposed, in which the plain-image is decomposed into 8x8 size blocks and a 2D Cat map is applied in three different ways to achieve good shuffling effect. Moreover, the control parameters of shuffling are randomly generated using a 2D coupled Logistic map to enforce the secrecy of the image. The encryption of the shuffled image is done using chaotic sequence generated through a 1D Logistic map. All the simulation and experimental analysis show that the proposed image encryption system has (1) a very large key space, (2) high sensitivity to secret keys, (3) has information entropy close to the ideal value 8 and (4) has low correlation coefficients close to the ideal value 0. Hence, we can say that all the analysis prove the security, effectivenees and robustnesss of the proposed image encryption algorithm.

REFERENCES

[1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps." International Journal of Bifurcation and Chaos, vol.8, no.6, pp.1259-1284, 1998.

[2] J. C. Yen and J. I. Guo, "A new image encryption algorithm and its VLSI architecture." in Proceedings of IEEE workshop on signal processing systems, pp. 430–437, 1999.

[3] J. C. Yen and J. I. Guo, "A new chaotic key-based design for image encryption and decryption." in Proceedings of IEEE International Symposium on Circuits and Systems, Vol.4, pp. 49–52, 2000.

[4] L. Zhang, X. Liao, X. Wang, "An image encryption approach based on chaotic maps." Chaos, Solitons and Fractals, vol. 24, no. 3, pp. 759–765, 2005.

[5] A. N. Pisarchik, N. J. Flores-Carmona and M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices." CHAOS Journal, American Institute of Physics, vol. 16, no. 3, pp. 033118-033118-6, 2006.

[6] C. Dongming, Z. zhiliang, Y. Guangming, "An Improved Image Encryption Algorithm Based on Chaos." in Proceedings of IEEE International Conference for Young Computer Scientists, pp. 2792-2796, 2008.

[7] N. K. Pareek, V. Patidar, K. K. Sud, "Image encryption using chaotic logistic map." Image and Vision Computing, vol. 24, no. 9, pp. 926–934, 2006.

[8] S. Lian, J. Sun, Z. Wang, "A block cipher based on a suitable use of chaotic standard map." Chaos Solitons and Fractals, vol. 26, no. 1, pp. 117–129, 2005.

[9] Y. Mao, S. Lian, and G. Chen, "A novel fast image encryption scheme based on 3D chaotic Baker maps." International Journal of Bifurcation and Chaos, vol. 14, no. 10, pp. 3616–3624, 2004.

[10] M. Salleh, S. Ibrahim and I. F. Isnin, "Enhanced chaotic image encryption algorithm based on Baker's map." IEEE Conference on Circuits and Systems, vol.2, pp.508-511, 2003.

[11] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavand, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps." Physics Letter A, vol. 366, no. 4-5, pp. 391-396, 2007.

[12] G. Y. Chen, Y. B. Mao, C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps." Chaos Solitons and Fractals, vol. 21, no. 3, pp. 749-761, 2004.

[13] ZH. Guan, F. Huang, W. Guan, "Chaos-based image encryption algorithm", Physics Letters A , vol. 346, no. 1-3, pp. 153–157, 2005.

[14] X.Y. Wang, and Q. J Shi, "New Type Crisis, Hysteresisand Fractal in Coupled Logistic Map." Chinese Journal of Applied Mechanics, pp. 501-506, 2005.

[15] R. M. May, "Simple mathematical model with very complicated dynamics." Nature, vol. 261, pp. 459-467, 1976.

[16] X. Tao, X. F. Liao, G. P. Tang, "A novel block cryptosystem based on iterating a chaotic map." Physics Letter A, vol. 349, no. 1-4, pp. 109-115, 2006.

AUTHORS PROFILE

Musheer Ahmad received his Master of Technology in Computer Science and Engineering in 2008 from ZH College of Engineering and Technology, AMU, Aligarh, India. Currently, he is Faculty in the Department of Computer Engineering, AMU, Aligarh, India. His area of interest includes image processing, encryption techniques, watermarking, steganography.

M Shamsher Alam received his Bachelor of Technology in Computer Engineering in 2008 from ZH College of Engineering and Technology, AMU, Aligarh, India. Currently he is pursuing Master of Technology in the Department of Computer Engineering, AMU, Aligarh, India. His area of interest includes image encryption techniques, ad-hoc networks and artificial immune systems.