Research Journal of Applied Sciences, Engineering and Technology 4(4): 322-328, 2012
ISSN: 2040-7467

Submitted: August 08, 2011 Accepted: September 25, 2011 Published: February 15, 2012

A New Image Encryption Scheme for Secure Digital Images Based on Combination of Polynomial Chaotic Maps

[1]Ahmed A. Abd El-Latif, [2]Li Li, [1]Ning Wang, [1]Jia-Liang Peng, [1]Zhenfeng Shi and [1,2]Xiamu Niu
[1]School of Computer Science and Technology, Harbin Institute of Technology, 150080 Harbin China
[2]School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518055, China

Abstract: In recent times, research on image encryption using chaotic systems has emerged. However, some of the proposed schemes still hinder the system performance and security. In this study, we introduce an efficient image encryption scheme based on pixel bit and combination of polynomial chaotic maps with variable initial parameters. The algorithm takes advantage of the best features of chaotic maps combined with the pixel value bits. The initial parameters and the keystream employed in the encryption process are generated from two chaotic maps. Simulation results and analyses both confirm that the new algorithm possesses high security with less computation for practical image encryption.

Key words: Chaotic systems, image encryption, security analysis

INTRODUCTION

With the rapid development of Internet and universal application of multimedia technology, more and more information including audio, image, and other multimedia has been transmitted over unsecured channels. In particular, image encryption has attracted more attention since images have been widely used in various areas. Examples of areas in which image encryption has been applied are biometric image, strategic communication, telemedicine, medical imaging, images of protected geographical area of military impotance and drawings which correspond to critical components of the system.

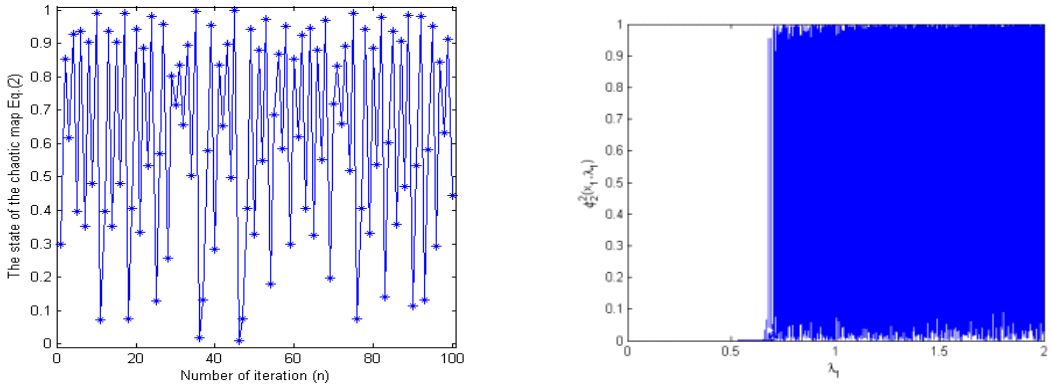
Image encryption is the process of realign the original image into an incomprehensible/unintelligible one that is non-recognizable in appearance, disorderly, and unsystematic (Abd El-Latif *et al*., 2011). It is a challenging task which is quite different from text encryption due to some intrinsic properties of images such as high redundancy and bulky data capacity, which are generally difficult to handle by using traditional techniques such as DES, triple-DES, RSA, IDEA, or AES. An overview of recent developments in the design of traditional cryptographic algorithms is given in (Menezes *et al*., 1996; Schneier, 1996).

In recent years, chaos theory has received ever increasing research interests from cryptographers. This is because of the fact that the chaotic systems have many important cryptographically desirable features, such as high sensitivity to initial conditions/parameters, long periodicity, high randomness and mixing (Amin *et al*., 2010; Lian, 2009). Moreover, chaotic maps are easy to be implemented by microprocessors and personal computers. Therefore, these features make its chaos-based image cryptosystems excellent and robust against statistical attacks.

Towards this direction, many scholars have made an effort to investigate chaotic encryption schemes in order to promote communication security (Akhavan *et al*., 2011; Chen *et al*., 2004; Gao *et al*., 2006; Gao *et al*., 2008; Kwok and Tang, 2007; Pareek *et al*., 2006; Patidar *et al*., 2009; Pisarschik, 2006; Wang *et al*., 2009). Despite these efforts, there are a number of major problems detected in some of those schemes such as weakness against differential attack and sometimes neglecting the tradeoff between the operation speed, required memory space, and security (Arroyo *et al*., 2009; Arroyo *et al*., 2010; Ge *et al*., 2011; Rhouma and Belghith, 2008; Rhouma *et al*., 2010).

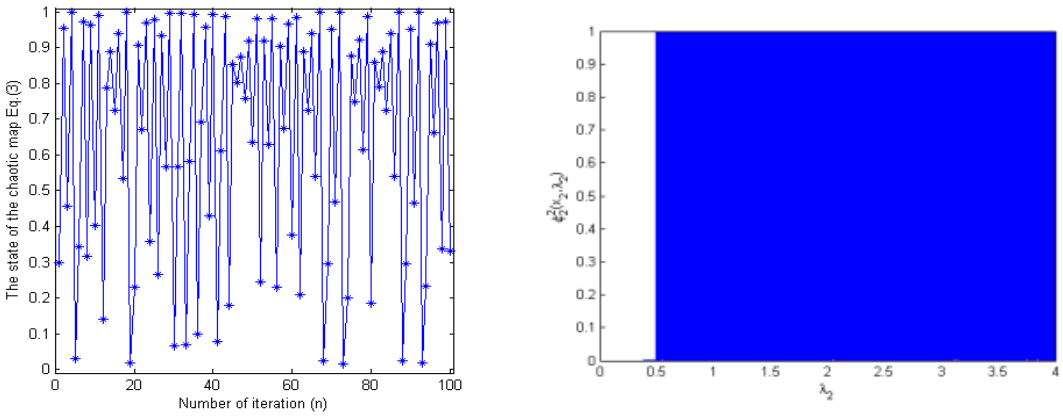
To enhance the security as well as the performance of the image encryption, we propose an efficient image encryption algorithm based on pixel bit and combination of chaotic systems. Two chaotic maps are performed in the encryption process. The initial parameters of the two chaotic maps are randomly generated by each other. Therefore, the keystream employed for encryption is distinct in different rounds, which effectively remedies the flaws mentioned above and enhances the encryption performance.

Corresponding Author: Ahmed A. Abd El-Latif, School of Computer Science and Technology, Harbin Institute of Technology, 150080 Harbin China



(a) (b)

Fig. 1: (a) Chaotic behavior of the chaotic map Eq. (2) ($x_1(0) = 0.3$, $\lambda_1 = 2$) (b) Bifurcation behavior of the chaotic map Eq. (2)



(a) (b)

Fig. 2: (a) Chaotic behavior of the chaotic map Eq. (3) ($x_2(0) = 0.3$, $\lambda_2 = 1.97$). (b) Bifurcation behavior of the chaotic map Eq. (3)

THE PROPOSED SCHEME

Chaotic systems: In this study, we consider the one-dimensional families of chaotic maps of the interval [0, 1] with an invariant measure which can be defined as the ratio of polynomials of degree N (Akhvan *et al.*, 2011):

$$\phi_N^{(1,2)}(x,\lambda) = \frac{\lambda^2 F}{1+(\lambda^2-1)F} \qquad (1)$$

where, F is substituted with chebyshev polynomial of type one $T_N(x)$, for $\phi_N^{(1)}(x_1, \lambda_1)$ and the chebyshev polynomial of type two, $U_N(x)$ for $\phi_N^{(2)}(x_1, \lambda_1)$. As an example, we give below one of these maps:

$$\phi_2^{(2)}(x_1,\lambda_1) \Rightarrow x_1(n+1) = \frac{2\lambda_1^2(0.5-|x_1(n)-0.5|)}{1+2(\lambda_1^2-1)(0.5-|x_1(n)-0.5|)}, \qquad (2)$$

$$\phi_2^{(2)}(x_2,\lambda_2) \Rightarrow x_2(n+1) = \frac{4\lambda_2^2 x_2(n)(1-x_2(n))}{1+4(\lambda_2^2-1)x_2(n)(1-x_2(n))} \qquad (3)$$

Note that the map Eq. (2) is reduced to tent map if $\lambda_1 = 1$. Also, the map Eq. (3) is reduced to logistic map if $\lambda_2 = 1$.

Indeed, the diagrams of bifurcation and chaotic behaviors help the algorithms designer to distinguish the space in which the parameters can be used as valid keys. Figure 1 and 2 show the bifurcation and the chaotic

behavior diagrams of the chaotic map Eq. (2) and (3), respectively. The continuous black regions are the spaces in which the parameters can be used as valid keys.

Pixel bit decomposition and reconstruction: Let p(I, j) denote the pixel in the ith row and jth column of original image, and let p^t(i, j) denote the t(t = 0, 1,.., 7) digit after transforming. Then:

$$p^t(i,j) = \begin{cases} 1 & if\ (p(i,j)/2^t) \bmod 2 = 1 \\ 0 & otherwiswe \end{cases} \quad (4)$$

So, we can transform a gray image into bit matrix composed of zero and one by formula (4). Contrarily, we also can transform the p^t(i, j) into gray pixels if using the following formula:

$$p(i,j) = \sum_{t=0}^{7} 2^t \times p^t(i,j) \quad (5)$$

For an original image of size M×N, a matrix M×8N will be got according to formula (4); the pixels of it are zeros and ones. The encrypted bit matrix is also of size M×8N. An encrypted decimal image will finally be obtained by computing formula (5).

Image encryption scheme based on chaotic systems: In the proposed encryption scheme, two chaotic systems are employed to achieve the goal of image encryption. The image encryption process consists of the following steps:

Step 1: The plain image is transformed into bit matrix composed of zero and one by formula (4)

Step 2: The secret keys, including initial condition and control parameters, and the chaotic maps in Eq. (2) and (3) are iterated 100 times and new values are set to x_1 and x_2 to avoid the transient effect.

Step 3: Repeat step 4 to 7 for k = 1 to M×N

Step 4: The chaotic map Eq. (2) is iterated once and the new x_1 is used as new initial parameter for chaotic map (Eq. 3) as well as in $t = x_1 \times 10^{14} \bmod 2^L$

Step 5: The chaotic map of Eq. (3) is iterated once and the new x_2 is used in $l = x_2 \times 10^{14} \bmod 2^L$

Step 6: Generate the masked chaotic key *Key* from *t* and *l* and then calculate the cipherimage using the following formula:

$$C_k = (\lfloor t * l + t)^2 \rfloor) \bmod 2^L \ XOR\ M_k \quad (6)$$

where $L = \log_2 G$ and *G* is the number of possible gray levels in image pixels. For example, L is 8 if the plainimage is a 256 gray-scale image

Step 7: Transforming contrarily the encrypted matrix by formula (5) and getting decimal matrix of size M×N

Step 8: The encryption process is complete and a gray image is genrated

The process of decryption is an inverse process of encryption. With the correct key, the final reconstructed image is exactly the same as the original plainimage, without any distortion.

SIMULATION RESULTS AND ANALYSIS

In this section, we do experiments for validating the security and practicability of the proposed algorithm. All the simulation was done by Matlab 7.1 in a computer of Dual-Core CPU 2.7 GHz and 1.99 GB of RAM.

To demonstrate the security and efficiency of our algorithm, we use several standard gray images like Lena, Baboon, Pepper, Cameraman, Barbara, MRI, Goldhill, Boat and Airplane of 256×256 size. Among them, the plainimages of Lena and Cameraman and their respective histograms are shown in Fig. 3. As can be seen in this Figure, the gray value distributions of plainimages are not uniform. The initial parameters taken for experimentation are $\lambda_1 = 2$, $x_1(0) = 0.3$, $\lambda_2 = 1.97$, $x_2(0) = 0.6$.

The cipher images of Lena, Cameraman using the proposed encryption algorithm and their histograms are shown in Fig. 4, respectively. It is clear from the Fig. 4 that the cipherimages are very much indistinguishable and appears like a noise. Moreover, as seen in Fig. 4 that the distribution of gray values of the cipherimages is fairly uniform and much different from the histograms of the plainimages as shown in Fig. 3. In addition, the cost of whole encryption is approximately 2.9s, which is acceptable for security.

Key space analysis: The key space is the total number of different keys that can be used in the encryption. For a secure image encryption, the key space should be large enough to make brute force attacks infeasible (Amin *et al*., 2010; Lian, 2009). Considering the calculation precision is 10^{14}, the size of key space for initial conditions and control parameters would be almost 2^{186}, not including the number of iterations, which is large enough for any encryption purpose (Chen *et al*., 2004).

Key sensitivity: An efficient encryption algorithm should be sensitive to secret key i.e. a small change in secret key during decryption process results into a completely different decrypted image (Abd El-Latif *et al*., 2011; Amin and Abd El-Latif, 2010; Amin *et al*., 2010). In the proposed algorithm, an incremental change in key; even

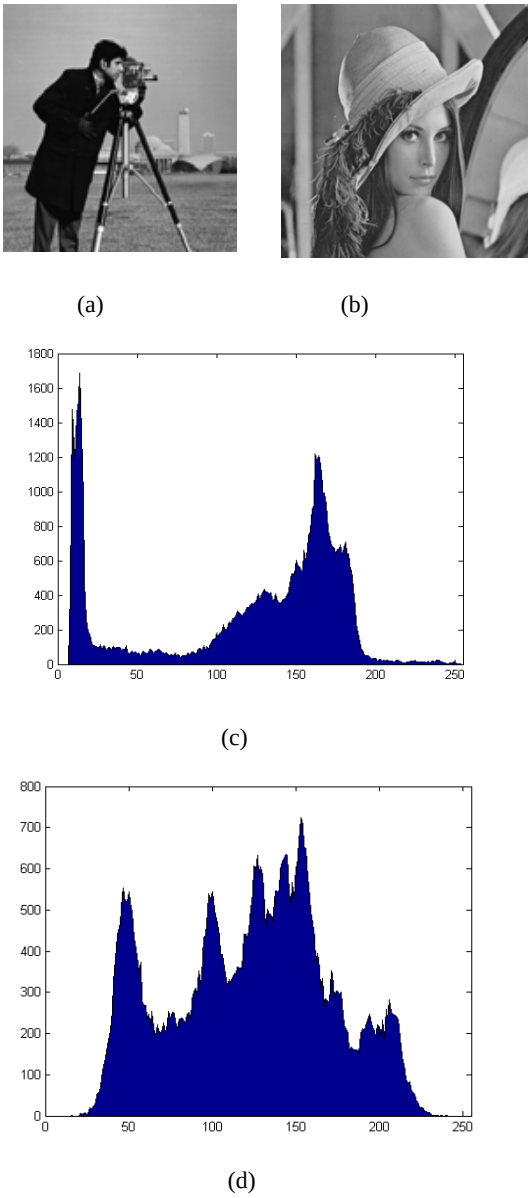


Fig. 3: (a) *Cameraman* (b) *Lena* (c) histogram of original *Cameraman* and (d) histogram of original *Lena*

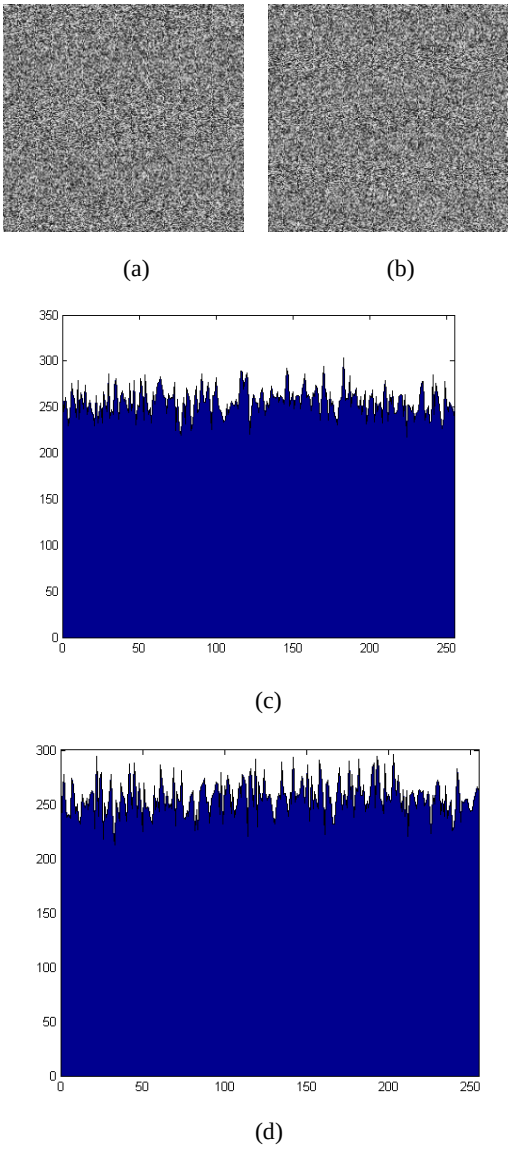
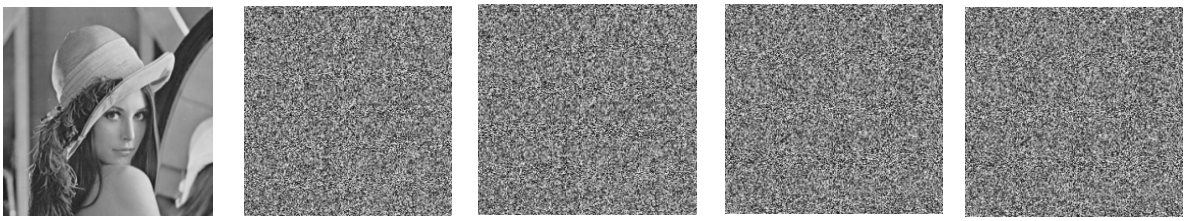


Fig. 4: (a) Encrypted *Cameraman* (b) Encrypted *Lena* (c) histogram of encrypted *Cameraman* and (d) histogram of encrypted *Lena*

of the order of $(\Delta=)10^{-10}$, results into completely unrecognizable decrypted image. The cipher images shown in Fig. 5 is decrypted images using $\lambda_1+\Delta$, $x_1(0)+\Delta$, $x_2(0)+\Delta_2$, $\lambda_2+\Delta$, separately, the resultant decrypted images shown in Fig. 5 are unrecognizable and noise like. Hence, it can be said that the proposed algorithm has high sensitivity to secret key.

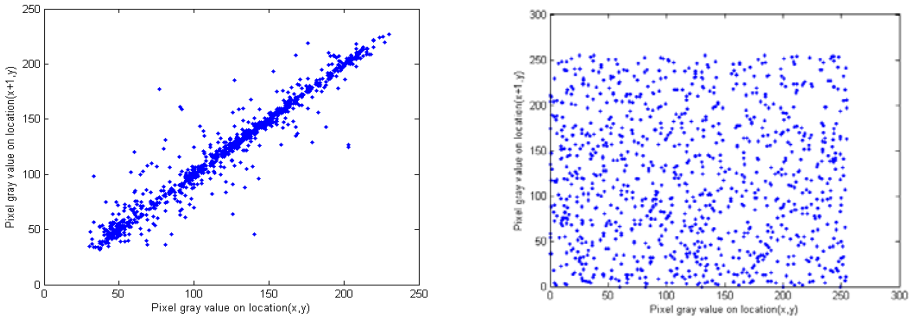
Correlation coefficient analysis: For an ordinary image having definite visual content, each pixel is highly correlated with its adjacent pixels. An ideal encryption technique should produce the cipher images with no such correlation in the adjacent pixels (correlation coefficient ≈ 0) (Amin *et al*., 2010; Chen *et al*., 2004). The visual testing of the correlation of adjacent pixels can be done by plotting the distribution of the adjacent pixels in the plain image and its corresponding cipher image. The correlation coefficient between two adjacent pixels in an image is determined as:

$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \quad (7)$$



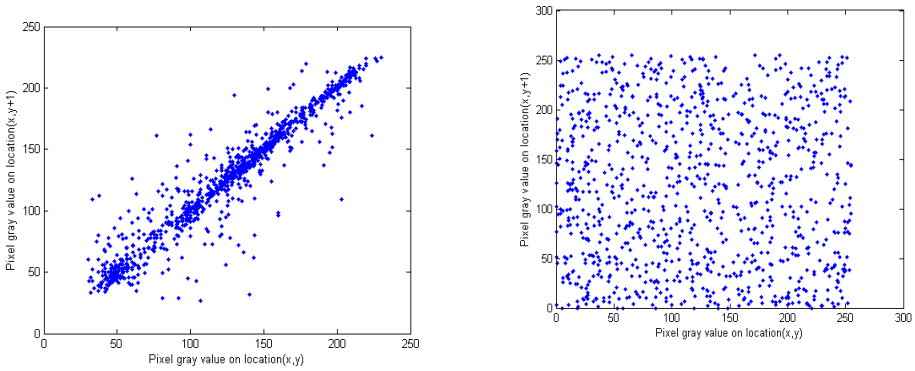
(a) (b) (c) (d) (e)

Fig. 5: Key sensitivity: (a) decrypted image with corrcet key, (b) decrypted image with wrong key 1, (c) decrypted image with wrong key 2, (d) decrypted image with wrong key 3, and (e) decrypted image with wrong key 4



(a) (b)

Fig. 6: Two horizontally adjacent pixels correlation in original image/encrypted image, respectively



(a) (b)

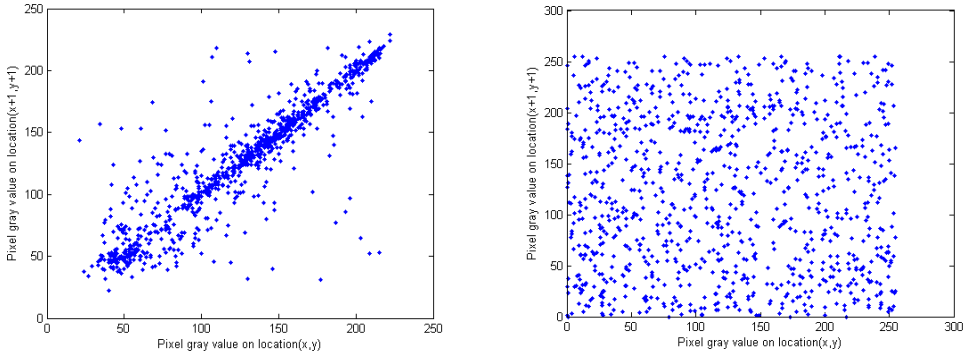
Fig. 7: Two vertically adjacent pixels correlation in original image/encrypted image, respectively

where E(x) = mean (x_i) and x, y are gray values of two adjacent pixels in the image.

The correlation coefficients of the adjacent pixels are calculated and listed in Table 1. The corresponding distribution for the horizontal, vertical and diagonal directions are shown in Fig. 6-8. The figures demonstrate that the encryption algorithm has covered up all the plain image characters image and shows good performance with balanced 0-1 ratio.

The values of correlation coefficient shown in Table 1 and Fig. 6-8 show that the two adjacent pixels in the plain images are highly correlated to each other, whereas the values obtained for cipher images are close to 0 (zero co-correlation).

Information entropy analysis: Entropy is a statistical measure of randomness in information theory (Shannon,



(a) (b)

Fig. 8: Two diagonally adjacent pixels correlation in original image/encrypted image, respectively

Table 1: Correlation coefficient of two adjacent pixels in plain image

Test Images	Vertical	Horizontal	Diagonal
Original Image	0.9475	0.9681	0.92790
0Encrypted Image	0.00146	0.0019	0.00201

Table 2: The entropy analysis of plain images and cipher images

Test Images	Plain image	Cipher image
Lena	7.4433	7.9980
Cameraman	7.0097	7.9975
Elain	7.4841	7.9974
Boat	7.1640	7.9976
Airplane	6.7794	7.9973

Table 3: Comparison between the proposed algorithm and Zhang and Liu (2011)

Considered items	Zhang and Liu (2011)	Proposed Algorithm
Key space	2^{104}	2^{186}
Horizontal correlation coefficient	- 0.000848277	0.0019
Vertical correlation coefficient	0.00370914	0.00146
Diagonal correlation coefficient	- 0.000188985	0.00201
Information Entropy	7.9975	7.9980
NPCR (%)	99.60	99.62
UACI (%)	33.45	33.50

1949). To calculate the entropy H(m) of a source m, we have:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i)\log_2 \frac{1}{p(m_i)} bits \quad (8)$$

where, $p(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, i.e., $m = \{m_0, m_1, ..., m_{255}\}$ after evaluating Eq. (8), we obtain its entropy H(m) = 8, corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.

The values of entropies obtained for plain images and cipher images of the proposed scheme are given in Table 2. The entropy values for cipherimages of the proposed scheme are very close to the ideal value 8. This implies that the information leakage in the proposed encryption process is negligible and the encryption algorithm is secure against the entropy based attack.

Resistance to differential attacks: To resist the differential attack, a minor alternation in the plainimage should cause a substantial change in the cipherimage. To test the influence of a one-pixel change on cipher image, two common measures (Amin *et al*., 2010; Patidar *et al*., 2009) are used, i.e., Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI), they can be defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (9)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (10)$$

where, C_1 and C_2 are the two cipherimages whose corresponding plainimages have only one-pixel difference. The gray-scale values of the pixels at grid (i, j) are labeled as C_1(i, j) and C_2(i, j), respectively; W and H are width and height of the cipherimage; Define a bipolar array, D, with the same size as images C_1 and C_2. Then, D(i, j) is determined by C_1(i, j) and C_2(i, j), namely, if C_1(i, j) = C_2(i, j) then D(i, j) = 1; otherwise, D(i, j) = 0.

The NPCR measures the different pixel numbers between two images, and the UACI measures the average intensity of differences between two images. Here, the encrypted image of Lena is called "Lena-test1", and the

encrypted image after changing the first pixel grey value from Lena is called "Lena-test2". We obtained the result, NPCR = 99.62% and all the UACI = 33.50%, from the simulation. This result demonstrates that our algorithm has a strong ability to resist differential attack.

Comparison with other chaos-based algorithms: Here, we will compare our proposed algorithm with (Zhang and Liu, 2011). We mainly focus on the security consideration. The test image is 256 gray-scales "*Lena*" image with a size of 256×256 and the results are shown in Table 3. From Table 3 we can see that our algorithm has a better security performance than (Zhang and Liu, 2011).

CONCLUSION

In this study, an efficient image encryption scheme based on pixel bit and a combination of two chaotic polynomial maps has been presented. In the presented algorithm we have combined these two maps in order to enhance the security and the performance of image encryption algorithm. All the simulation and experimental analyses show that the proposed image encryption system has large key space, high sensitivity to secret keys, better diffusion of information in the ciphered images and low correlation coefficients. Hence, the proposed image encryption algorithm has high level of security with less computation and is more robust towards cryptanalysis.

ACKNOWLEDGMENT

This study is supported by the National Natural Science Foundation of China (Project Number:60832010).

REFERENCES

Abd El-Latif, A.A., X. Niu and N. Wang, 2011. Chaotic image encryption using bézier curve in DCT domain scrambling. Communications Comp. Inf. Sci., 194: 30-41.

Akhavan, A., A. Samsudin and A. Akhshani, 2011. A symmetric image encryption scheme based on combination of nonlinear chaotic maps. J. Franklin Institute, 348(8): 1797-1813.

Amin, M. and A.A. Abd El-Latif, 2010. Efficient modified RC5 based on chaos adapted to image encryption. J. Electron. Imag., 19(1): 013012-1-10.

Amin, M., O.S. Faragallah and A.A. Abd El-Latif, 2010. A chaotic block cipher algorithm for image cryptosystems. Commun. Nonlinear Sci. Numer. Simulat., 15: 3484-3497.

Arroyo, D., C. Li, S. Li, G. Alvarez and W.A. Halang, 2009. Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos, Solitons Fractals, 41: 2613-2616.

Arroyo, D., S. Li, J.M. Amigó, G. Alvarez and R. Rhouma, 2010. Comment on "Image encryption with chaotically coupled chaotic maps. Physica D., 239: 1002-1006.

Chen, G., Y. Mao and C.K. Chui, 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitions Fractals, 21: 749-761

Gao, H., Y. Zhang, S. Liang and D. Li, 2006. A new chaotic algorithm for image encryption. Chaos Solitons Fractals, 29(2): 393-399.

Gao,T., Q. Gu and Z. Chen, 2008. A new image encryption algorithm based on hyper-chaos. Phys. Lett. A., 374(4): 394-400.

Ge, X., F. Liu, B. Lu and W. Wang, 2011. Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem and its improved version. Phys. Lett. A., 375: 908-913.

Kwok, H.S. and W.K.S. Tang, 2007. A fast image encryption system based on chaotic maps with finite precision representation. Chaos Solitons Fractals, 32(4): 1518-1529.

Lian, S., 2009. Efficient image or video encryption based on spatiotemporal chaos system. Chaos Solitons Fractals, 40(5): 2509-2519.

Menezes, A.J., P.C. Van Oorschot and S. Vanstone, 1996. Handbook of Applied Cryptography. CRC Press, Boca Raton FL, USA.

Pareek, N.K., V. Patidar and K.K. Sud, 2006. Image Encryption Using Chaotic Logistic Map. Image Vision Comp., 24: 926-934.

Patidar, V., N.K. Pareek and K.K. Sud, 2009. A new substitution-diffusion based image cipher using chaotic standard and logistic maps. Commun. Nonlinear Sci. Numer. Simulat., 14: 3056-3075.

Rhouma, R. and S. Belghith, 2008. Cryptanalysis of a new image encryption algorithm based on hyper-chaos. Phys. Lett. A., 372: 5973-5978.

Rhouma, R., E. Solak and S. Belghith, 2010. Cryptanalysis of a new substitution-diffusion based image cipher. Commun. Nonlinear Sci. Numer. Simulat., 15: 1887-1892.

Schneier, B., 1996. Applied Cryptography-Protocols Algorithms and Source Code in C. 2nd Edn., John Wiley & Sons, Inc., New York.

Shannon, C.E., 1949. Communication theory of secrecy system. Bell Syst. Tech. J., 28: 656-715.

Wang,Y., K.W. Wong, X. Liao, T. Xiang and G. Chen, 2009. A chaos-based image encrypttion algorithm with variable control parameters. Chaos Solitions Fractals, 41: 1773-1783.

Zhang, G. and Q. Liu, 2011. A novel image encryption method based on total shuffling scheme. Optics Commun., 284: 2775-2780.