International Journal of Soft Computing 2 (2): 285-291, 2007

An Efficient Image Encryption Scheme Based Chaotic Logistic Maps

[1]I.A. Ismail, [2]Mohammed Amin and [2]Hossam Diab
[1]Faculty of Computers and Informatics, Zagazig University, Egypt
[2]Faculty of Science, Menoufia University, Egypt

Abstract: Encryption of images is different from that of texts due to some intrinsic features of images such as bulk data capacity, high correlation among pixels and high redundancy, which are generally difficult to handle by traditional methods. Due to the exceptionally desirable properties of mixing and sensitivity to initial conditions and parameters of chaotic maps, chaos based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. In this study, an image encryption scheme is presented, in which shuffling the positions and changing the grey values of image pixels are combined simultaneously to ensure a high level of security. Firstly, the Arnold cat map is used to shuffle the positions of the image pixels in the spatial-domain. Then another chaotic map is used to confuse the relationship between the cipher image and the plain image. In the proposed image encryption scheme, an external secret key of 128-bit is employed. Further, to make the cipher more robust against any attack, the secret key is modified after encrypting of each pixel of the plain image. Thereby, significantly increasing the resistance to statistical and differential attacks. Visually and computationally, experimental results demonstrate the high security and significantly superior encryption quality of the proposed scheme.

Key words: Image encryption, decryption, Arnold cat map, data security, logistic maps, chaos cryptography, statistical analysis

INTRODUCTION

The fascinating developments of computer network technology during the last decade and many applica-tions like military image databases, confidential video conferencing, medical imaging system, cable TV, online personal photograph album, etc. require reliable, fast and robust security system to store and transmit digital images. In general, conventional symmetric and asymmetric cryptography such as DES, 3DES, AES and RSA algorithms cannot be used to encrypt images directly. It is well known that images are different from texts in many aspects, such as bulk data capacity, high correlation among pixels and high redundancy. So a variety of image encryption schemes (Bourbakis and Alexopoulos, 1992; Refregier, 1995; Chang and Liu, 1997; Fridrich, 1998; Scharinger, 1998; Yen and Guo, 1999, 2000 a,b; Cheng, 2000; Chang *et al*., 2001; Li and Zheng, 2002; Li, *et al*., 2002; Chen *et al*., 2004) have been proposed in the literature based on different principles. Among them, chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power. In fact, Chaotic system has many important features related to the fundamental requirements of conventional cryptography, such as aperiodicity, sensitive dependence on initial conditions (useful for confusion and diffusion processes), ergodicity and random-like behaviors (useful for producing output with satisfactory statistics). Therefore, chaotic dynamics are expected to provide a fast and easy way for building cryptosystems.

A number of chaos based image encryption scheme have been developed in recent years which we discuss in brief. Fridrich (1998) demonstrated the construction of a symmetric block encryption technique based on two-dimensional standard baker map. There are three basic steps in the method of Fridrich (1998).

- Choose a chaotic map and generalize it by introducing some parameter.
- Discretize the chaotic map to a finite square lattice of points that represent pixels.
- Extend the discretized map to three-dimensions and further compose it with a simple diffusion mechanism.

Further, Scharinger (1998) designed a chaotic based image encryption technique, in which whole image is taken as a single block and which is permuted through a key-controlled chaotic system. In addition, a shift register

Corresponding Author: I.A. Ismail, Faculty of Computers and Informatics, Zagazig University, Egypt

pseudo random generator is also adopted to introduce the confusion in the data. Yen and Guo (1999) proposed an encryption method called BRIE based on chaotic logistic map. The basic principle of BRIE is bit recirculation of pixels, which is controlled by a chaotic pseudo random binary sequence. The secret key of BRIE consists of two integers and an initial condition of the logistic map. Further, Yen and Guo (2000) also proposed an encryption method called CKBA (Chaotic Key Based Algorithm) in which a binary sequence as a key is generated using a chaotic system. The image pixels are rearranged according to the generated binary sequence and then XORed and XNORed with the selected key. Later in 2002, Li and Zheng (2002) pointed out some defects in the encryption schemes presented in the references (Yen and Guo, 1999, 2000 a,b) and also discussed some possible improvements on them. Very recently, Chen *et al*. (2004) have proposed a symmetric image encryption in which a two-dimensional chaotic map is generalized to three dimension for designing a real time secure image encryption scheme. This approach employs the three-dimensional cat map to shuffle the positions of the image pixels and uses another chaotic map to confuse the relationship between the encrypted and its original image. In this study, we propose an approach for image encryption based on chaotic logistic maps in order to meet the requirements of the secure image transfer. In the proposed image encryption scheme, an external secret key of 128-bit and two chaotic logistic maps are employed to encrypt the plain image.

THE PROPOSED IMAGE ENCRYPTION ALGORITHM

The proposed image encryption algorithm includes two steps: Firstly, the positions of the pixels of the original image are shuffled by Arnold cat map. Then the pixel values of the shuffled image are encrypted by another chaotic map.

Encryption by Arnold cat map: Image data have strong correlations among adjacent pixels. Statistical analysis on large amounts of images shows that averagely adjacent 8 to 16 pixels are correlative in horizontal, vertical and also diagonal directions for both natural and computer-graphical images. In order to disturb the high correlation among pixels, we adopt Arnold cat map to shuffle the pixel positions of the plain-image. Assume that the dimension of the original grayscale image I is N×N. The coordinates of the pixels are S = {(x,y): x,y = 0,1,...N-1}. Arnold cat map is described as (http://online.redwoods.cc.ca.us/instruct/darnold/laproj/Fall97/Gabe/catmap.pdf.)

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \bmod N = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (1)$$

where p and q are positive integers, det(A) = 1 the (x',y') is the new position of the original pixel position (x,y) when Arnold cat map is performed once. Iterated actions of A on a pixel $r_0 \in S$ form a dynamic system

$r_{n+1} = A^n r_0 \bmod N$ or $r_{n+1} = A\ r_n \bmod N, n = 0,1,2,\cdots$

Thus, the parameters p, q and the number of iterations M all can be used as the secret keys.

Since there only exists a linear transformation and mod function, it is very efficient to shuffle the pixel positions using the Arnold cat map (http://online.redwoods.cc.ca.us/instruct/darnold/laproj/Fall97/Gabe/catmap.pdf.). After several iterations, the correlation among the adjacent pixels can be disturbed completely. Some experiments are given in this study to demonstrate the efficiency of Arnold cat map. However, the periodicity of Arnold cat map should degrade the security the encryption, because the possible attacks may iterate the Arnold cat map continuously to reappear the original plain-image. As a remedy, we adopt another chaotic map to change the pixel values next to improve the security.

Encryption the shuffled image: The second step of the proposed encryption scheme is to encrypt the shuffled image by changing its pixel values based on one dimension logistic map, we can depict this procedure as follows,

The proposed image encryption process utilizes an external secret key of 128-bit long. Further, the secret key is divided into blocks of 8-bit each, referred as session keys.

$$K = k_1 k_2 \cdots k_{32} \text{ (in hexadecimal)}, \quad (2)$$

here, k_i's are the alphanumeric characters (0-9 and A-F) and each group of two alphanumeric characters represents a session key. Alternatively, the secret key can be represented in ASCII mode as

$$K = k_1 k_2 \cdots k_{16} \text{ (in ASCII)}, \quad (3)$$

here, each k_i represents one 8-bit block of the secret key.

The shuffled image is shifted by some constant C as,

$$I = C \times F \quad (4)$$

where I is the shifted image obtained from the shuffled image F by the constant C.

The chaotic logistic map, Eq. 5, is employed as follow:

$$x(n+1) = 4x(n)[1 - x(n)] \tag{5}$$

First, we choose two numbers: one (denoted by L) is a floating number in (0,1), to be used as an initial condition; another (denoted by S) is an integer, to be used as a seed (Chen *et al*., 2004). Then, use L as the initial value to compute the chaotic logistic map x as Eq. 5.

If the next value obtained is within the subinterval (0.2,0.8), then go to the next step; otherwise, the iteration goes on until a desired number in (0.2,0.8) is obtained. Here, notice that the value of 0.5 is a 'bad¡¯ point, trapping the iterations to the fixed point 0. If this case is encountered, a tiny perturbation should apply. Once a proper value is obtained from the logistic map, digitize it by amplifying it with a proper scaling and sampling. The digitized value is designated as $\phi(n)$.

Determine the selected key k(n) for encrypting the current pixel according to,

$$y = \phi(n) \bmod 15 \tag{6}$$

$$k(n) = k_{y+1} \tag{7}$$

Now, the resultant ciphered pixel can be obtained as,

$$\begin{aligned} C(n) = \phi(n) \oplus \{[(I(n) + k(n) + \phi(n))] \bmod N\} \\ \oplus C(n-1) \oplus k(n) \end{aligned} \tag{8}$$

where I(n) is the currently operated pixel, C(n-1) is the previously output cipher-pixel, C(0) = S and N is the color level (for a 256 grey scale image, N = 256).

After encryption of each pixel, we modify the keys k^{16} and k_{y+1} as follows:

$$\begin{aligned} k_{16} &= k_{16} \oplus k_{y+1}, \\ k_{y+1} &= (k_{y+1} + k_{16}) \bmod 256 \end{aligned} \tag{9}$$

the steps (3-6) are repeated for encrypting each pixel of the shifted-shuffled image.

RESULTS AND DISCUSSION

Some results are given in this study to demonstrate the efficiency of the proposed scheme. In our experimental results, several images are evaluated. These images are Ship, Lena and Penguin. For the evaluations of encryption quality, the Correlation Coefficient (C.C) is used which can be calculated by Chen *et al*., 2004; Pareek *et al*., 2006.

$$C.C = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum x_j^2 - (\sum_{j=1}^{N} x_j)^2) \times (N\sum y_j^2 - (\sum_{j=1}^{N} y_j)^2)}} \tag{10}$$

where x and y are grey scale pixel values of the original and encrypted images.

A striking example of the degree to which the proposed cipher can reveal patterns in the plaintext is shown in Fig. 1, where the plain images are first shuffled by Arnold cat map, secret keys p = 3, q = 4, M = 5 and then the shuffled image is encrypted (changing pixels values) by the secret key"782AFE394123E4A0BEB9175 FC9AD3673" (in hexadecimal). The results are also compared with the encryption scheme presented by Guan *et al*. (2005), as abbreviation *Guan* and an encrypted image generated by the Chen *et al*. (2003), as abbreviation Chen. Obviously, the proposed method hides all features of the original image where the ciphered image is significantly different from its plain image, i.e., the encrypted images are visual indistinguishable. Computationally, it clear that there is negligible correlation between the plain image and ciphered image, Table 1, where the proposed scheme retains the smallest Correlation Coefficients (C.C). Thus, the proposed scheme outperforms both Guan method and Chen method.

SECURITY ANALYSIS

A good encryption scheme should resist all kinds of known attacks, such as known-plain-text attack, ciphertext only attack, statistical attack and various brute force attacks (Chen *et al*., 2004; Pareek *et al*., 2006). Some security analysis on the proposed image encryption scheme, including the most important ones like key space analysis and statistical analysis, which demonstrated the satisfactory security of the proposed scheme, are described . Different images have been tested and similar results are obtained. However, due to page limit, only the results for Ship (Fig. 1) are used for illustration.

Key space analysis: A good image encryption algorithm should be sensitive to the cipher keys and the key space should be large enough to make brute force attacks infeasible. For the proposed image encryption algorithm, key space analysis and testing have been performed and completely carried out, with results summarized as follows:

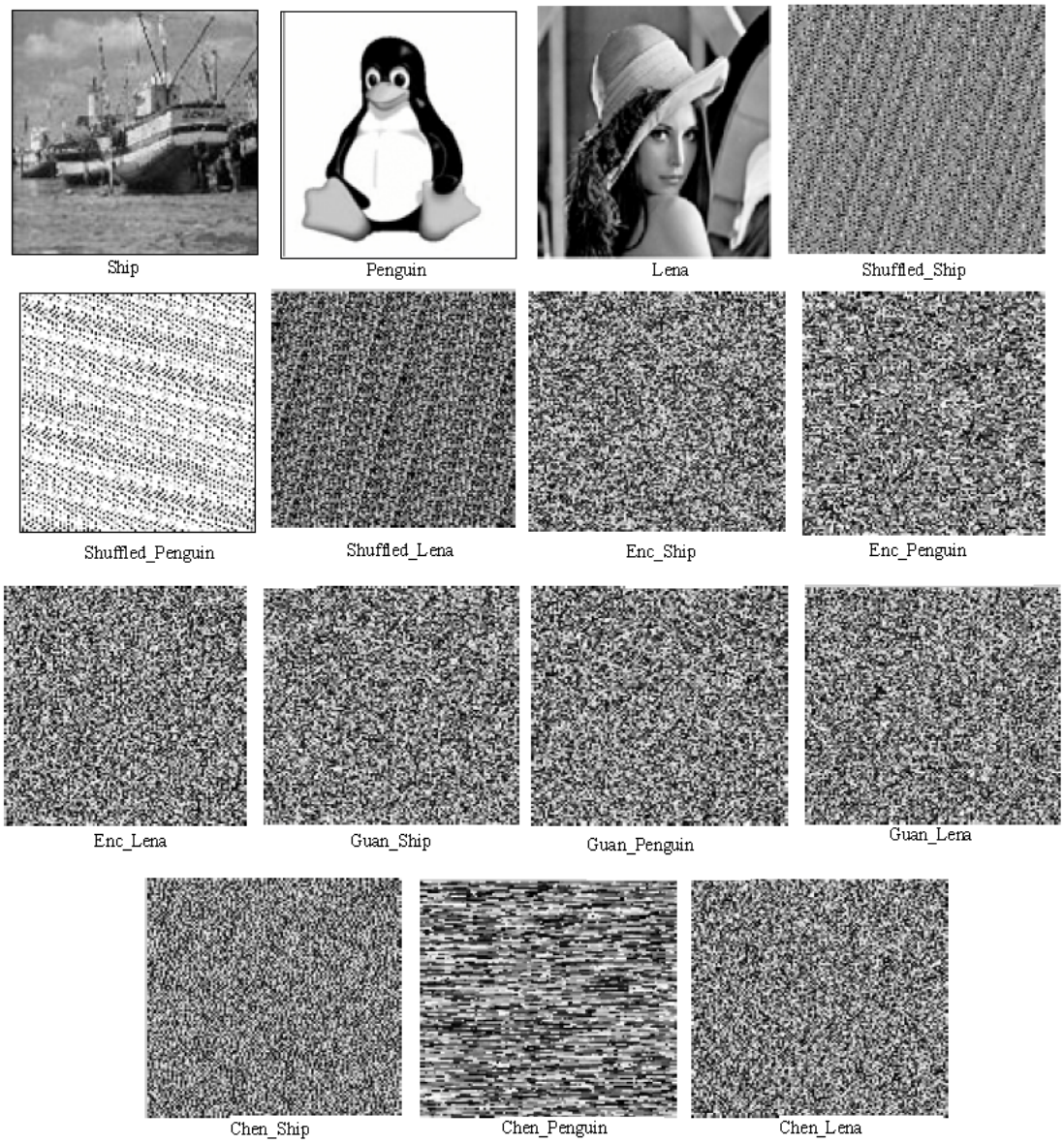

Fig. 1: Encryption of Ship, Penguin and Lena images by the proposed scheme(*Enc_Ship*, *Enc_Penguin and Enc_Lena*), Guan scheme and Chen scheme

Key space: the proposed image cipher has $2^{128}(\approx 3.4028\times10^{38})$ different combinations of secret key. An image cipher with such a large key space is sufficient for reliable practical use and can resist all kinds of brute force attacks.

Key sensitivity test: An ideal image encryption procedure should be sensitive with respect to the secret key, i.e., the change of a single bit in the secret key should produce a completely different encrypted image (Pareek *et al*., 2006).

For testing the key sensitivity of the proposed encryption scheme, we have performed the following steps:

- An original image (Ship) is encrypted by using the secret key"782AFE394123E4A0BEB9175 FC9AD3673" (in hexadecimal) and the resultant image is referred as encrypted image A.
- The same original image is encrypted by making the slight modification in the secret key i.e., "882AFE39 4123E4A0BEB9175FC9AD3673" (the most significant

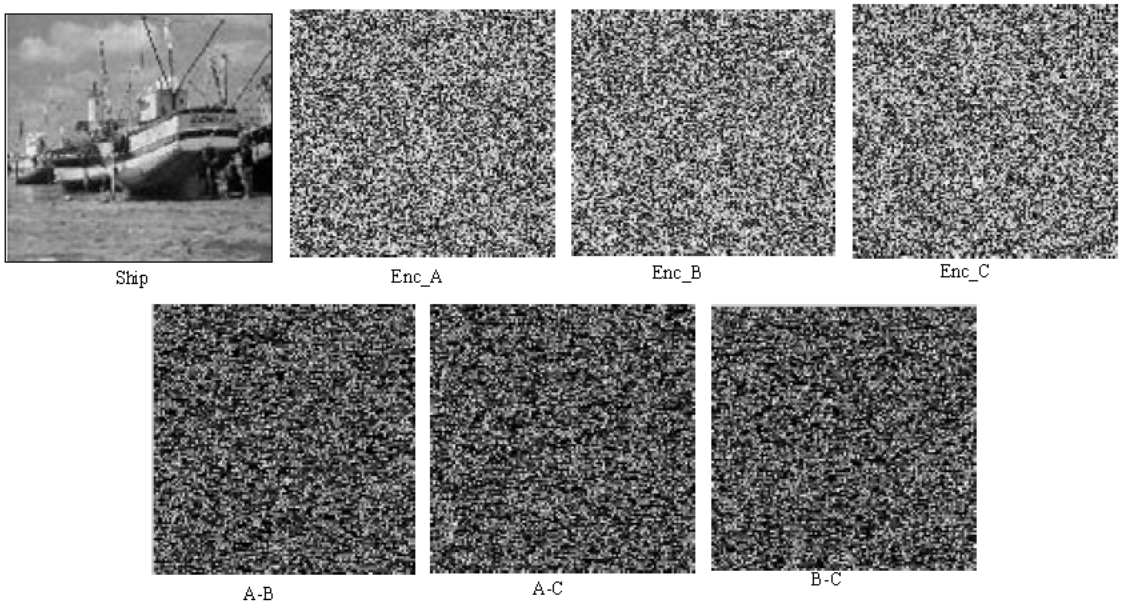

Fig. 2: Key sensitive test of the proposed scheme by encrypting the plain image by several slightly different keys

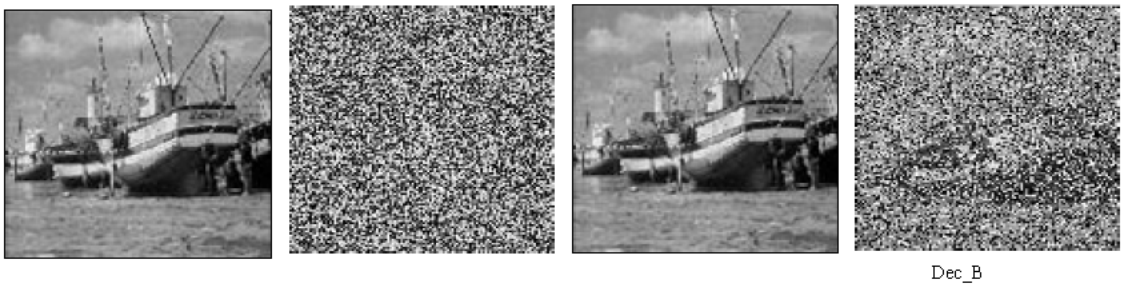

Fig. 3: Key sensitive test of the proposed scheme by decrypting the cipher image by slightly wrong key

bit is changed in the secret key) and the resultant image is referred as encrypted image B.

- Again, the same original image is encrypted by making the slight modification in the secret key i.e., "782AFE394123E4A0BEB9175FC9AD3674"(theleast significant bit is changed in the secret key) and the resultant image is referred as encrypted image C.
- Finally, the three encrypted images A, B and C are compared.

In Fig. 2, we have shown the original image, the three encrypted images produced in the aforesaid steps and the three difference images(A-B, A-C and, B-C). It is not easy to compare the encrypted images by simply observing these images. So for comparison, we have calculated the correlation between the corresponding pixels of the three encrypted images. For this calculation, we have used the same formula as given in Eq.10 except that in this case x and y are the values of corresponding pixels in the two encrypted images to be compared. In Table 2, we have given the results of the correlation coefficients and pixel difference between the corresponding pixels of the three encrypted images A, B and C. It is clear from the table that no correlation exists among three encrypted images even though these have been produced by using slightly different secret keys. Also, for example, The encrypted image by "782AFE394 123E4A0BEB9175FC9AD3673" has 99.3125% of difference from the one encrypted by the key"782AFE394123E4A0BEB9175 FC9AD3674" in terms of pixel grey scale values, although there is only one bit difference in the two keys.

Moreover, when a key is used to encrypt an image while another slightly different key is used to decrypt the ciphered image, the decryption also completely fails. Figure 3 clearly shows that the image encrypted by the key782AFE394123E4A0BEB9175FC9AD3673 (Enc.image

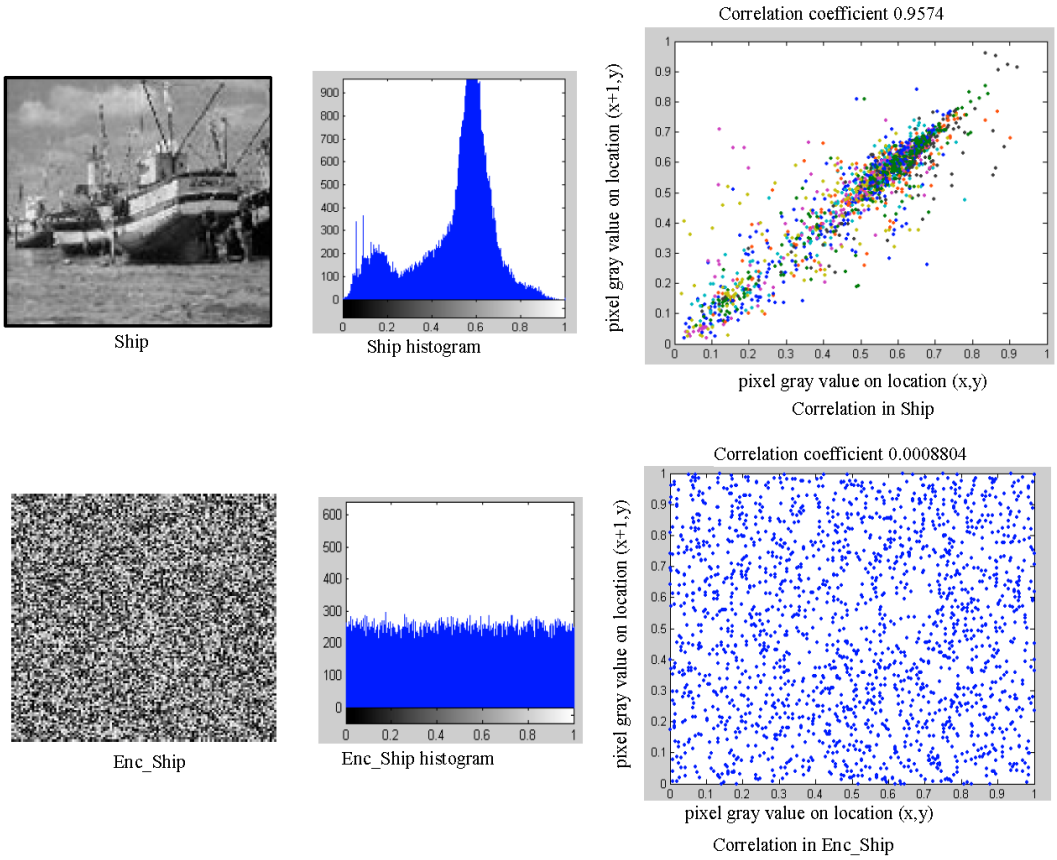

Fig. 4: Histogram and correlation coeffieint of two horizantally adjacent pixel in orignal and encrypted images

Table 1: The numerical evaluation, C.C, for encryption quality

Image	Proposed scheme	Guan *et al.*, 2005	Chen *et al.*, 2004
Ship	-0.0000425	0.0090000	0.0022000
Lena	-0.0001046	0.0042000	0.0089000
Penguin	-0.0005917	0.0114000	0.0100000

Table 2: Pixel difference & correlation coefficient between images encrypted by keys with 1-bit difference

Image 1	Image 2	Pixel difference	C.C
Encrypted A	Encrypted B	87.8194%	0.001100
Encrypted C	Encrypted A	99.3125%	0.000757
Encrypted B	Encrypted C	99.1944%	0.000780

Table 3: Correlation coefficients of two adjacent pixels In original and encrypted images

Direction	Plain image	Cipher image
Horizontal	0.9574	0.0008804
Vertical	0.9399	0.0066000
Diagonal	0.9183	0.0021000

A) is not correctly decrypted by using the key "782AFE394123E4A0BEB9175FC9AD3674"(Dec.image B), there is only one bit difference between the encryption and decryption keys (the least significant bit in the secret key is changed), thereby, the proposed encryption scheme is highly key sensitive.

Statistical analysis: It is well known that many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. Therefore, an ideal cipher should be robust against any statistical attack (Pareek *et al.*, 2006). To prove the robustness of the proposed image encryption procedure, we have performed statistical analysis by calculating the histograms and the correlations of two adjacent pixels in the encrypted images.

Histograms of encrypted images: An image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each intensity level. We have calculated and analyzed the histograms of the several encrypted as well as its original images that have widely different content. Statistical analysis of Ship image and its encrypted image yielded their grey-scale histograms given in Fig. 4. This figure shows that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. Also, it demonstrates that the encryption algorithm has

covered up all the characters of the plain image and has complicated the dependence of the statistics of the output on the statistics of the input.

Correlation of two adjacent pixels: For an ordinary image, each pixel is usually highly correlated with its adjacent pixels either in horizontal, vertical or diagonal directions. These high-correlation properties can be quantified as the correlation coefficient for comparison. To test the correlation between two adjacent pixels in plain-image and ciphered image, the following procedure was carried out. First, randomly select 1000 pairs of two adjacent (in horizontal, vertical and diagonal direction) pixels from an image. Then, referring to Chen *et al.* (2004), calculate the correlation coefficient of each pair by Eq. 10. Figure 4 shows the correlation distribution of two horizontally adjacent pixels in the plain-image and that in the ciphered image. Similar results for diagonal and vertical directions were obtained, which are shown in Table 3. These correlation analysis prove that the proposed encryption technique satisfies zero co-correlation.

CONCLUSION

In this study, a potential method for image encryption based on chaotic logistic maps is proposed, in which shuffling the positions and changing the grey values of image pixels are combined simultaneously to ensure a high level of security. Firstly, the Arnold cat map is used to shuffle the positions of the image pixels in the spatial-domain. Then another chaotic map is used to confuse the relationship between the cipher image and the plain image. In the proposed image encryption scheme, an external secret key of 128-bit is employed. Further, to make the cipher more robust against any attack, the secret key is modified after encrypting of each pixel of the plain image. Thereby, significantly increasing the resistance to statistical and differential attacks. The experimental results demonstrated that the proposed image encryption technique have advantages of large key space and high-level security, while maintaining acceptable efficiency. From the analysis of these results, the proposed algorithm satisfies uniform distribution property and has many characteristics of traditional cryptography, such as almost zero correlation. Although the algorithm presented in this paper has focused on image encryption, it is not just limited to this area and can be widely applied in the secure transmission of confidential information over the Internet.

REFERENCES

Bourbakis, N. and C. Alexopoulos, 1992. Picture data encryption using SCAN pattern, Pattern Recogn., 25: 567-581.

Chang, H.K.L. and J.L. Liu, 1997. A linear quad tree compression scheme for image encryption, Signal Process, 10: 279-290.

Chang, C.C., M.S. Hwang, T.S. Chen, 2001. A new encryption algorithm for image cryptosystems, J. Sys. Software, 58: 83-91.

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

Cheng, H. and X.B. Li, 2000. Partial encryption of compressed image and videos, IEEE Trans. Signal Process, 48: 2439-2451.

Fridrich, J., 1998. Symmetric ciphers based on two dimensional chaotic maps, Int. J. Bifurcat Chaos, 8: 1259-1284.

http://online.redwoods.cc.ca.us/instruct/darnold/laproj/Fall97/Gabe/catmap.pdf.

Kai, W., W. Pei, Liuhua, Z.A. Song and Z. He, 2005. On the Security of 3D Cat Map Based Symmetric Image Encryption Scheme, Phys. Lett., A 343: 432-439.

Li, S. and X. Zheng, 2002. Cryptanalysis of a chaotic image encryption method, in: Proceedings of the IEEE International. symposium on circuits and systems, Scottsdale, AZ, USA.

Li, S., X. Zheng, X. Mou, Y. Cai, 2002. Chaotic encryption scheme for real time digital video, Proceedings of the SPIE on electronic imaging, San Jose, CA, USA.

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

Refregier, B.J., 1995. Optical image encryption based on input plane and fourier plane random encoding, Opt. Lett., 20: 767-769.

Scharinger, J., 1998. Fast encryption of image data using chaotic Kolmogrov flow, J. Elec. Eng., 7: 318-325.

Yen, J.C. and J.I. Guo, 1999. A new image encryption algorithm and its VLSI architecture, in: Proceedings of the IEEE workshop signal processing systems, pp: 430-437.

Yen, J.C. and J.I. Guo, 2000. An efficient hierarchical chaotic image encryption algorithm and its VLSI realization, IEE Proc. Vis. Image Process, 147: 167-175.

Yen, J.C. and J.I. Guo, 2000. A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE Int. Symp. Circ. Sys., 4: 49-52.

Zhi-Hong Guan, 2005. Fangjun Huang and Wenjie Guan, Chaos-Based Image Encryp. Algo. Phys. Lett., A 346: 153-157.