Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):621-629

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

New binary image encryption algorithm based on combination of confusion and diffusion

Rui Liu

College of Electronic Engineering, Xi' an University of Posts and Telecommunications, Xi' an, China

ABSTRACT

Encryption of binary images is essential since it is vulnerable to eavesdropping in wired and wireless networks. The security of data becomes important since the communications over open network occur frequently. A new binary image encryption algorithm is proposed in this paper. The proposed algorithm is based on combination of confusion and diffusion. Firstly, used Logistic chaotic sequence to confuse the addresses of the binary image pixels, then decomposed the confused image into a number of bit planes, finally defined a new diffusion algorithm to achieve the pixel value diffusion by the bit plane transposed encryption. In this way, the proposed algorithm transforms drastically the statistical characteristic of original image information, so, it increases the difficulty of an unauthorized individual to break the encryption. The simulation results and the performance analysis show that the algorithm can encrypt binary images of different sizes and has large secret-key space, high security, fast encryption speed and strong robustness, and is suitable for practical use to protect the security of digital binary image information over the Internet.

Key words: Binary image encryption; chaotic sequences; bit-plane; confusion; diffusion

INTRODUCTION

Binary images are the simplest type of image which is used widely in a variety of industrial and medical applications. Binary image will be a black-and-white or silhouette image. Binary images are images that have been quantized to two values, usually denoted 0 and 1, representing black and white. Binary images can be classified as either halftone or non-halftone. Halftone images are binary representations of grayscale images. Non-halftone binary images may be composed of characters, drawings, schematics, diagrams, cartoons, equations etc. [1]. The advantage of binary image is that it is easy to acquire, simple digital cameras can be used together with very simple frame stores or low-cost scanners. Binary images have a low storage since it has no more than 1 bit per pixel.

With the popularity of digitized information on a global scale, many important text materials have been scanned digital documents including personal information file, medical diagnostic records, personal diploma, digital signatures, collection of books, etc. These documents have been stored and transferred over the network in the form of binary image. Because of these binary image data involves personal privacy or sensitive information, so how to protect these data against illegal copying and distribution has become extremely important.

Generally, there are two major approaches that are used to protect digital image from attacker. One is information hiding such as digital watermarking of image. The other is encryption, which includes conventional encryption and others such as chaotic encryption [2]. Most conventional ciphers, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), linear feedback shift register (LFSR), etc. [3-4] with high computational security consider plaintext as either block cipher or data stream and are not suitable for image encryption in real time because their speed is slow due to a large data volume and strong correlation among image pixels. The implementation of traditional algorithms for image encryption is even more complicated when undertaken with commercial software.

Many fundamental characteristics of chaos, such as a broadband spectrum, ergodicity and high sensitivity to initial conditions are directly connected with two basic properties of good ciphers: confusion and diffusion [5]. The aim of confusion phase is to disturb the high correlation among pixels. Most of the confusion phases design to permute the image by changing the pixel positions without modifying pixel values, so the histograms of the encrypted image and the plain image are identical [6]. They are insecure against known/chosen-plaintext attack, for the histogram is a measure of the important characteristics of an image, the attacker can use the histogram to obtain the original image's approximate content [7]. In addition to, these methods restricted to image size specification and need multiple iterations. Fridrich [8] was the first one to suggest a permutation of the pixel positions in a chaotic fashion, using either the Baker map or the cat map as a key for chaotic confusion. In the diffusion stage, the pixel values are modified so that a minute change in one-pixel spreads out to as many pixels as possible. In other words, all pixels should be mixed somehow. Patidar et al. [9] proposed a substitution diffusion method using chaotic standard and logistic maps. Liu et al. [10] proposed a cryptosystem based on multi-chaotic maps. Many papers proposed image encryption algorithms which use chaotic flows for key generation and then applying confusion and diffusion on the image [11]. Zhu et al. [12] proposed an innovative permutation method to confuse and diffuse the grayscale image at the bit-level, which not only changes the position of the pixel but also modifies its value, but they also use the Arnold cat map to permute the bits, and the Logistic map to further encrypt the permuted image.

However, the main problem in modern communication technology is not the security of an encryption algorithm, but rather its good dynamic properties, i.e. its robustness against noise or other external disturbances [13]. The binary image encryption process demands 100% exact results after decryption, so put forward higher requirement for its dynamic properties. Although the aforementioned methods could achieve better encryption effect, but its dynamic properties couldn't meet the demand of binary image encryption.

This paper proposes a new binary image encryption algorithm which based on combination of confusion and diffusion. Firstly, used Logistic chaotic sequence to confuse the addresses of the binary image pixels, then decomposed the confused image into a number of bit planes, finally defined a new diffusion algorithm to achieve the pixel value diffusion by the bit plane transposed encryption. The objectives of this new algorithm includes: 1) to simultaneously perform permutation and diffusion operations for fast encryption and large secret-key space; 2) to efficiently obtain good dynamic properties for binary image to resist against malicious attacks like cropping, noising. This algorithm is easy to operate and it can also deal with gray image and color image. In addition to, there is no limit to the scale of image, i.e. the square image and the non-square image can also be processed.

LOGISTIC CHAOTIC MAP

Since Robert A. J. Matthews presented the concept of chaotic cipher in 1989, chaotic encryption method has attracted more and more attention. A discrete time dynamical system can be defined as following equation:

$$X_{k+1} = f(\mu, X_k) \quad (1)$$

Where f is a nonlinear function, and μ is a control parameter, X_k is a real number in the range [0, 1]. If we repeatedly apply it to an initial condition X_0, then we will get a chaotic sequence $\{X_k : k=0,1,2,\ldots\}$. The typical chaotic dynamical systems, such as Logistic map, Lorenz system and Tent map, etc, that can be used for image encryption. One-dimensional (1-D) Logistic system is due to simplicity and efficiency, which widely has been used now. It's mathematical expressed as:

$$X_{k+1} = \mu X_k (1 - X_k) \quad (2)$$

Where $0<\mu\leq 4$ is called bifurcation parameter and X_k is define as above. It has been proved that when $3.569955672<\mu\leq 4$, Logistic map will operate in chaotic state. That is to say, $\{X_k: k=0,1,2,\ldots\}$ is produced with initial condition X_0 will be non-periodic, non-converging and non-correlated [14]. The probability density function of logistic map can be described as follows, which is shown in Fig. 1.

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{1-x^2}} & -1 < x < 1 \\ 0 & \text{else} \end{cases} \quad (3)$$

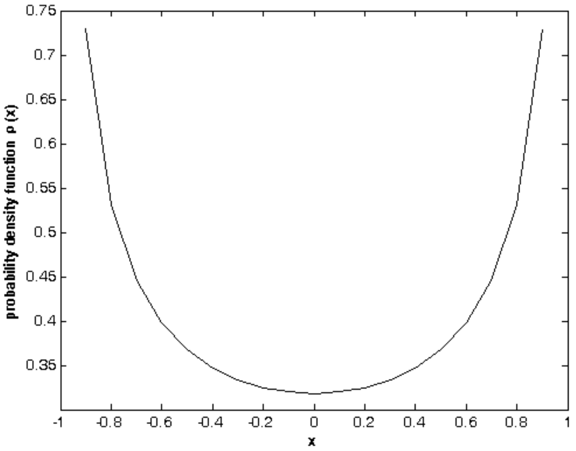


Fig. 1: Probability density of Logistic map

Form Fig. 1 we can see, the probability density of Logistic map is symmetric, ρ(x) does not depend on the initial value X_0, indicating that the chaos system is ergodic. The advantages of chaotic sequences can be concluded as follows:

- Sensitive to initial conditions. A small difference in initial conditions will lead to a significant difference of chaotic sequences. That is important from the view of security.
- Easy to generate. Chaotic sequences are generated with fast speed and low computing complexity.
- Noise-like. Some statistical characteristics of chaotic sequence are the same as white noise, which make it has good randomness.

THE PROPOSED NOVEL ENCRYPTION ALGORITHM FOR BINARY IMAGES

There are two classes of key-based cryptographic algorithms, which are symmetric (private-key) and asymmetric (public-key) algorithms. Symmetric algorithms use the same key for both encryption and decryption, and asymmetric algorithms are different. In practice, public-key encryption schemes are many times slower than their symmetric-key counterparts [15]. In this section, a novel symmetric approach to encrypt binary images based on combination of confusion and diffusion processes is proposed.

Encryption of Binary Image Take a binary image F (size M×N) as an example. The two-dimensional input image array is denoted by f (m, n), where m and n represent the vertical and horizontal coordinates respectively, which unit are pixel. The value of f (m, n) is one or zero. Fig. 2 shows a model of encryption and decryption system for binary image.

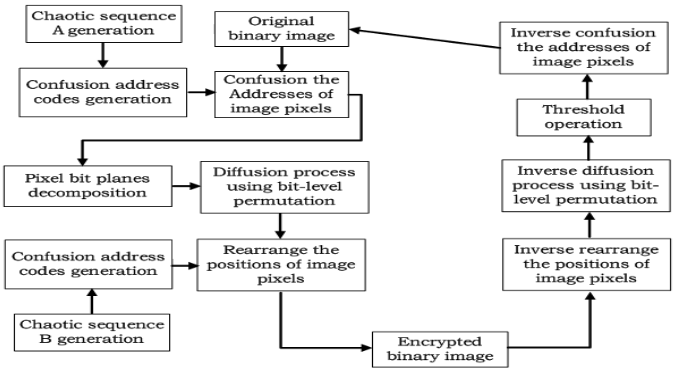

Chaotic sequence A generation
Original binary image
Inverse confusion the addresses of image pixels
Confusion address codes generation
Confusion the Addresses of image pixels
Threshold operation
Pixel bit planes decomposition
Diffusion process using bit-level permutation
Inverse diffusion process using bit-level permutation
Confusion address codes generation
Rearrange the positions of image pixels
Inverse rearrange the positions of image pixels
Chaotic sequence B generation
Encrypted binary image

Fig. 2: Model of encryption and decryption system

Chaotic sequence generation: Took the Logistic map as the model, used (2) generate two different one-dimensional (1-D) chaotic sequences $\{X^1_k: k=1,2,\ldots, M\times N\}$ and $\{X^2_k: k=1,2,\ldots, M\times N\}$. These sequences are generated based on some given controlling parameters (μ_1, μ_2) and initial values (X^1_0, X^2_0) which are considered as shared keys for encryption and decryption.

Confusion address codes generation: Sorted the two different chaotic sequences from small to large, respectively, and got the two sorted sequences {$X^{1'}_k$: k=1,2,…, M×N } and {$X^{2'}_k$: k=1,2,…, M×N }. Calculated the sets of confusion address codes { M^1_k: k=1,2,…, M×N } and { M^2_k: k=1,2,…, M×N }, where M^1_k∈{1,2,…, M×N }, M^2_k∈{1,2,…, M×N }. M^1_k was the new subscript of X^1_k in the sorted sequence $X^{1'}_k$, and M^2_k was the new subscript of X^2_k in the sorted sequence $X^{2'}_k$.

Confusion the addresses of image pixels: Converted the original binary image F's pixel matrix into a 1-D sequence {P_k: k=1,2,…, M×N }. According to the confusion address codes M^1_k to confuse the addresses of image pixels in the sequence P_k, got the sequence {$P^{'}_k$: k=1,2,…, M×N }.

Pixel bit planes decomposition: The L-bits image was decomposed into L-bits plane, each pixel in every bit-plane corresponds to 0 or 1. Used (4) each pixel of the binary image sequence $P^{'}_k$ could be mapped to equivalent L-bits binary number. For the pixel value of '1' in $P^{'}_k$, each pixel in every bit-plane corresponds to 1. For the pixel value of '0' in $P^{'}_k$, each pixel in every bit-plane corresponds to 0. At this point, the binary image information spread to L-bits plane, so encryption algorithm can resist against malicious attacks like cropping, noising. Also increase generality of the algorithm, make it can apply to the color image and gray image. Along with the increase of value of L dynamic properties get better, but the data capacity of encrypted image is enlarged.

$$\begin{cases} 1 \to 2^{L} - 1 \\ \;0 \to \;\;0 \end{cases} 8 \le \boldsymbol{L} \le 24, \quad \boldsymbol{L} \in \boldsymbol{Z}^{+} \quad (4)$$

After the above processing, I got a 2-D bits matrix with the size of h×w, where h was L-bit binary number (e.g., h=8, 16 or 24, et.), w was the total number of pixels in the image (e.g., w= M×N for image F). For simplicity, I take h=8 as an example.

Diffusion process using bit-level permutation: To de-correlate the relationship between adjacent pixels, a bit-level permutation was used to diffuse the values of image pixels. These elements in the bits matrix were used bit-level permutation and got a new bits matrix with same size, using these elements in the new bits matrix to generate pixels of the image with new values, formed a new 1-D sequence {E_k: k=1,2,…, M×N }. The key principle of bit-level permutation was as follows:

$$\mathrm{g} = (\mathrm{pixel\_index} + \mathrm{bit\_index} + \mathrm{offset}) \bmod \mathrm{w} \quad (5)$$

$$\mathrm{q} = \mathrm{bitget}\left(\mathrm{P}'\left(\mathrm{M}^1(\mathrm{g})\right), \mathrm{bit\_index}\right) \quad (6)$$

$$\boldsymbol{E}(\boldsymbol{pixel\_index}) = \boldsymbol{bitset}(\boldsymbol{P}'(\boldsymbol{pixel\_index}), (9 - \boldsymbol{bit\_index}), \boldsymbol{q}) \quad (7)$$

Where offset is a preset constant, using it as key for encryption and decryption, offset ∈{1,2,…, M×N }. It could make each bit of the pixel in the image has change, got better diffusion effect.

$$\begin{gathered}(\cdots \;\; P'_i \;\; P'_{i+1} \;\; P'_{i+2} \;\; P'_{i+3} \;\; \cdots) \\ \Rightarrow \begin{bmatrix} \cdots & P'(1,i) & P'(1,i+1) & P'(1,i+2) & P'(1,i+3) & \cdots \\ \cdots & P'(2,i) & P'(2,i+1) & P'(2,i+2) & P'(2,i+3) & \cdots \\ \cdots & P'(3,i) & P'(3,i+1) & P'(3,i+2) & P'(3,i+3) & \cdots \\ \cdots & P'(4,i) & P'(4,i+1) & P'(4,i+2) & P'(4,i+3) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & P'(8,i) & P'(8,i+1) & P'(8,i+2) & P'(8,i+3) & \cdots \end{bmatrix} \quad (8)\end{gathered}$$

$$\begin{gathered}\begin{bmatrix} \cdots & P'(8,i) & P'(8,i+1) & P'(8,i+2) & P'(8,i+3) & \cdots \\ \cdots & P'(7,i+1) & P'(7,i+2) & P'(7,i+3) & P'(7,i+4) & \cdots \\ \cdots & P'(6,i+2) & P'(6,i+3) & P'(6,i+4) & P'(6,i+5) & \cdots \\ \cdots & P'(5,i+3) & P'(5,i+4) & P'(5,i+5) & P'(5,i+6) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & P'(1,i+7) & P'(1,i+8) & P'(1,i+9) & P'(1,i+10) & \cdots \end{bmatrix} \quad (9) \\ \Rightarrow (\cdots \;\; E_j \;\; E_{j+1} \;\; E_{j+2} \;\; E_{j+3} \;\; \cdots)\end{gathered}$$

Where i and j represented the number of pixel (i.e., pixel _index), where i=j+offset+1.

Rearrange the positions of image pixels: According to the confusion address codes M^2_k to rearrange the positions of the image pixels in the sequence E_k, got the new sequence $\{E'_k$: k=1,2,…, M×N $\}$.

Encrypted image generation: Transformed 1-D sequence E'_k into 2-D matrix with the size of M×N, it was the encrypted binary image.

Decryption of Binary Image

Inverse rearrange the positions of image pixels: Transformed the encrypted binary image into 1-D sequence, used same keys for encryption to generate chaotic sequence, performed inverse rearrange the positions of image pixels.

Inverse bit-level permutation: According to the principle of bit-level permutation to inverse diffuse the values of image pixels, get a bits matrix H.

Threshold operation: The binary image information spread to L-bits plane by using pixel bit planes decomposition. When image information in several bit planes was polluted with cropping or noising, the encrypted binary image could be fully recovered by setting an appropriate threshold. Used (10) for these elements in the bits matrix H, then generate a new 1-D sequence $\{B_k$: k=1,2,…, M×N $\}$.

$$B_j = \begin{cases} 1, h(8,i) + h(7,i+1) + \cdots + h(1,i+7) \geq 3 \\ \qquad\qquad 0, \text{else} \end{cases} \quad (10)$$

Inverse confusion the addresses of image pixels: Inverse confusion the addresses of image pixels in the sequence B_k, got the new sequence $\{B'_k$: k=1,2,…, M×N $\}$. Transformed 1-D sequence B'_k into 2-D matrix with the size of M×N, it was the decrypted binary image.

EXPERIMENTAL RESULTS AND SECURITY ANALYSES

In order to test the performance of the encryption algorithm, this paper used MATLAB to simulate this algorithm. Took two binary images as experimental images, they were binary fingerprint image of 480×363 and binary text image of 114×252. Here I set the initial values X^1_0=0.25, X^2_0=0.35. The controlling parameters are μ_1=3.98264, μ_2=3.71294 and offset =5. Then results of encryption and decryption are showed as Fig. 3 - Fig.4

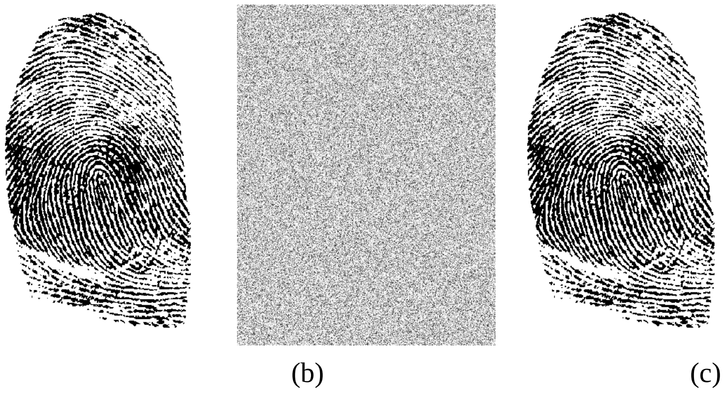


Fig. 3: Original, encryption and decryption binary fingerprint image (480×363): (a) Original image, (b) encryption image, (c) decryption image

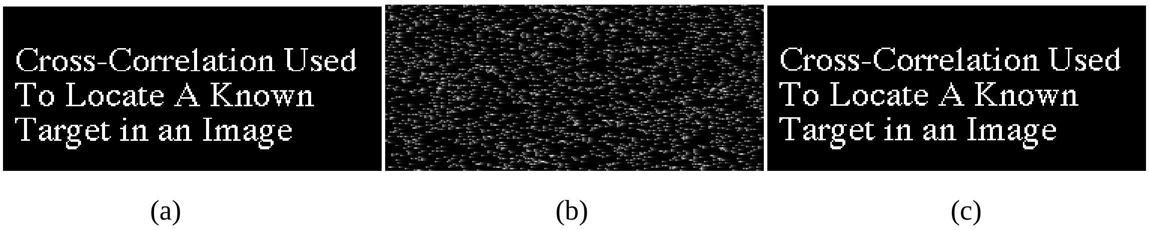
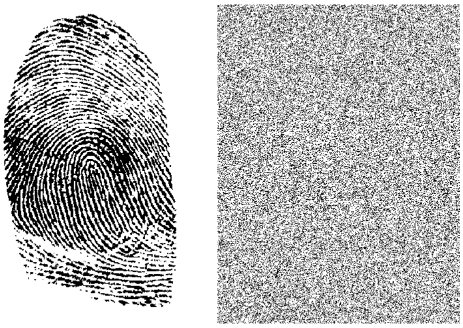


Fig. 4: Original, encryption and decryption binary text image (114×252): (a) Original image, (b) encryption image, (c) decryption image

From the experimental results we can see that, the encrypted images have completely change the characteristics of the original images, and there are no difference between the decrypted images and the original images in the visual, the purpose of image encryption has been achieved.

Secret-key Security Sensitivity Analysis Higher security level of the encrypted image can be achieved since the algorithm has five security secret-keys (X^1_0, X^2_0, μ_1, μ_2, offset) and all the security secret-keys have many possible choices. I have carried out a key sensitivity test using a key that is one digit different from the original key to decrypt the encrypted image (Fig. 3(b)). The resulting image is totally different from the original image as shown in Fig. 5(b). This demonstrates that the proposed algorithm is very sensitive to any change in the secret key value.

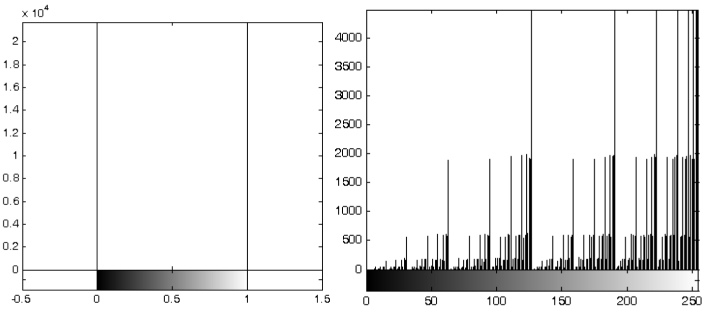


(a) (b)

Fig. 5: Secret-key security sensitivity analysis: (a) decrypted image shown in Fig. 3(b) with key={3.98264, 0.25, 3.71294, 0.35, 5}, (b) decrypted image shown in Fig. 3(b) with key={3.98265, 0.26, 3.71295, 0.36, 6}

Secret-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. The secret key of the proposed technique is (X^1_0, X^2_0, μ_1, μ_2, offset), where $\mu_i \in (3.569955672\ldots, 4]$ and $X^i_0 \in (0,1)$, i=1,2, μ_i and X^i_0 are both double precision, offset is single precision. Since double precision can represent about 16 decimal digits, the key space of the proposed algorithm can be estimated as $(10^{14})^2 \times (10^{16})^2 \times 10^8 = 10^{68}$. Note that the range of μ_i is (3.569955672…, 4], therefore a 14-digit precision is assumed. Thus, brute-force attacks on the key are computationally infeasible.

Histogram Analysis Histogram reflects image statistical distribution, and usually is used for statistics analysis attack. The histograms of original image and its encrypted image as shown in Fig. 6, compare them that we can see great differences. From Fig. 6, the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the histogram of the original image. Hence the encrypted image does not provide any clue to employ any statistical attack on the proposed image encryption procedure, which makes statistical attacks difficult.



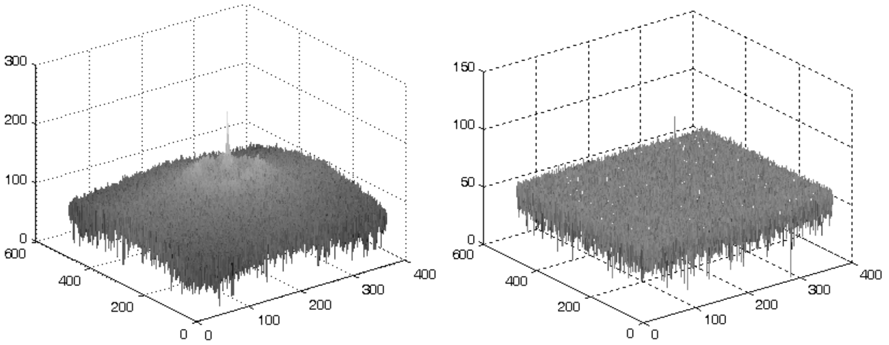
(a) (b)

Fig. 6: Original and encryption image histograms: (a) original binary image (Fig. 3(a)) histogram, (b) encryption image (Fig. 3(b)) histogram

Spectrum Analysis In order to verify the effectiveness of the binary image encryption approach proposed in this paper, the 2-D discrete Fourier transform (2D-DFT) is used to analyze the relative images. The 2D-DFT algorithm is given below:

$$F(u,v) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} f(m,n) e^{-j(2\pi/M)um} e^{-j(2\pi/N)vn} \quad (11)$$

where m and n are coordinates pair of image, M and N are the size of image, f(m, n) is the image value corresponding to the pixel (m, n). The spectrum of the original binary image (Fig. 3(a)) and the encrypted image (Fig. 3(b)) are depicted in Fig. 7(a)–(b), respectively. Note that in Fig. 7, the highest narrow spectrums in the middle correspond to the effectiveness of the image edge; they should be ignored in the spectrum analysis. From Fig. 7(a), it is observed that the frequency distribution of the original binary image is concentrated in a small area, which suffers the risk of information leakage. While in Fig. 7(b), the frequency distribution of encrypted image has been flattened. Therefore, it has validated that the original binary image is hidden perfectly against statistic attack with the proposed chaotic cryptographic approach.



(a) (b)

Fig. 7: Spectrum analysis: (a) spectrum of the original image shown in Fig.3 (a), (b) spectrum of the encrypted image shown in Fig.3 (b)

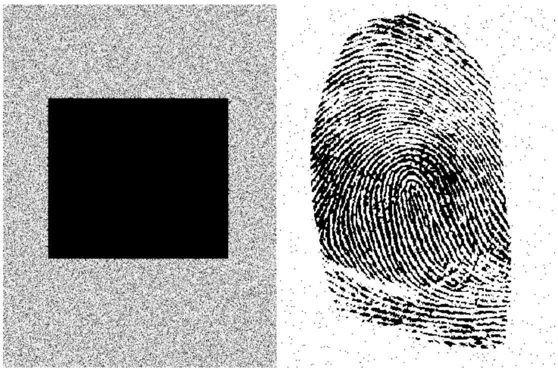
Correlation Coefficient Analysis The correlation coefficient between the plain image and the encrypted image is also studied to show the similarity between images. The similarity between images will reveal the identity of the plain image. The correlation coefficients of the plain image and encrypted image establish that the proposed algorithm has a good ability of confusion and diffusion and highly resistive against the statistical attack [16]. If the correlation value is between 0.5 and 1.0 or -0.5 and -1.0, it implies a strong positive correlation or strong negative correlation between the images. If the correlation value is between 0.0 and 0.5 or -0.1 and -0.5, it implies a weak positive correlation or weak negative correlation between the images. The correlation coefficient between the plain image and the encrypted image were shown in TableI.

Table I Correlation coefficients between plain and encrypted image

	Image	
	Binary Fingerprint Image	Binary Text Image
Correlation Coefficients Between Plain and Encrypted Image	0.0095	0.0257

From the TableI, it is inferred that there is weak correlation between the plain images and encrypted images. This implies that the binary images encrypted using the proposed chaotic cryptographic approach is resistive to statistical attacks.

Data Loss Attacks Data loss attacks are common image attacks. These attacks are to verify the ability of the encrypted images for tolerating the distortions in the public media transmission channels. Consequently, the encryption algorithm in the paper show great advantages in data loss attacks. Fig. 8 gave an example of cutting attacks. I did cutting attack on the encrypted image (Fig. 3(b)). The reconstructed image shown in Fig. 8 was derived from the encrypted image with cutting attack. The reconstructed image was visually acceptable since it include almost all visual information of the original binary fingerprint image.

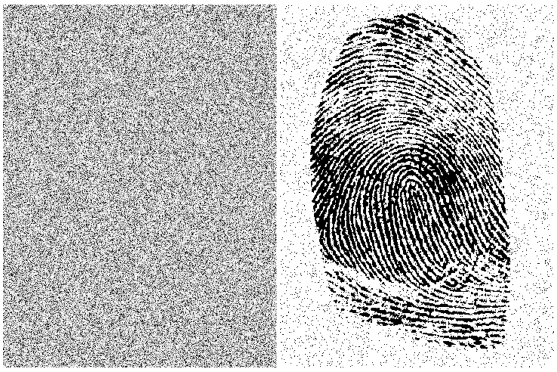


(a) (b)

Fig. 8: Cutting attack and reconstructed image: (a) Fig. 3(b) of center cut, (b) reconstructed image of (a)

The experimental result demonstrates that the encryption method shows excellent performance in data loss attacks. From Fig. 8 we can see that the image is attacked by cutting, which decryption image is able to get the most of original binary image information, but have some spots. This also shows that the encryption algorithm has uniform encryption effect.

Noise Attacks There are many different noises in the public media transmission channels such as networks. Noise attacks show the ability of the encrypted images for enduring the noise attacks. This shows another advantage of the image encryption algorithm. The experimental results in Fig. 9 show the performance of the encryption algorithm in noise attacks. I added salt and pepper noising on the encryption image (Fig. 3(b)). The image was recovered from the encrypted image with noise. The recovered image was shown in Fig. 9.



(a) (b)

Fig. 9: Noise attacks and reconstructed image: (a) Fig. 3(b) with 20% Salt & Pepper noise, (b) reconstructed image of (a)

The recovered image contains almost all the visual information of the original binary image even though they contain noises. The experimental result demonstrates that the encryption method show good performance in the presence of noise attacks. The encrypted images can be recovered when subjected to noisy environments.

CONCLUSION

Encryption is an important issue in wired and wireless communication since the data transmitted in the network is more vulnerable to fraud and eavesdropping. In this paper, a new binary image encryption algorithm based on combination of confusion and diffusion processes was proposed. Chaotic map is used for the confusion the addresses of the binary image pixels while bit-level permutation is used to diffuse the values of image pixels so as to enhance the security. Experimental results demonstrate that the proposed algorithm can achieve good encryption result, low time complexity, and large key space, in addition to it has good dynamic properties to resist the various attacks. Spectrum analysis has also demonstrated that an excellent information hiding has been achieved.

Acknowledgments
The author wish to thank the Natural Science Foundation of Shaanxi Province of China for contract 2014JM8331, and the Natural Science Foundation of Shaanxi Province of China for contract 2014JQ5183, under which the present work was possible.

REFERENCES

[1] N.K. Sreelaja; G.A. Vijayalakshmi Pai, *Applied Soft Computing*, no.12, pp. 2879-2895, **2012**.
[2] L. Zhang; X. Liao; X. Wang, *Chaos, Solitons & Fractals*, vol.24, pp. 759-765, **2005**.
[3] B. Schneier. Applied Cryptography _ Protocols, Algorithms, and Source Code, 2st Edition, C. John Wiley & Sons, Inc., New York, **1996**.
[4] J. Daemen, B. Sand, V. Rijmen. The Design of Rijndael: AES _ The Advanced Encryption Standard, Springer-Verlag, Berlin, **2002**.
[5] A.N. Pisarchik, M. Zanin. *Physica D*, Vol.237, pp. 2638-2648, **2008**.
[6] Hongjun Liu, Xingyuan Wang, *Optics Communications*, no.284, pp. 3895-3903, **2011**.
[7] Wang Yanling, Image Scrambling Method Based on Chaotic Sequence and Mapping, *Proc. IEEE Symp. First International Workshop on Education Technology and Computer Science (ETCS 09), IEEE Press,* pp. 453-457, Jun. **2009.**
[8] J. Fridrich, *Int. J. Bifurc. Chaos,* vol. 8, no. 6, pp. 1259-1284, **1998**.
[9] V. Patidar, N.K. Pareek, K.K. Sud, *Communications in Nonlinear Science and Numerical Simulation,* vol.14, no. 7, pp. 3056-3075, **2009**.
[10] Liu, J.M., Qiu, S.S., Xiang, F., Xiao, H.J. *International Symposiums on Information Processing*, pp. 740-743, **2008**.
[11] Zhang Han, Wang Xiu Feng, Li Zhao Hui, Liu Da Hai, and Lin You Chou, A new image encryption algorithm based on chaos system, *In Proceedings of IEEE International Conference on Robotics, Intelligent Systems and Signal Processing,* pp. 778-782, **2003**.
[12] Z. L. Zhu, W. Zhang, K. W. Wong, and H. Yu, *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, **2011**.
[13] A.N. Pisarchik, M. Zanin, *Physica D: Nonlinear Phenomena*, vol. 237, no. 20, pp. 2638-2648, **2008**.
[14] Sun Xin, Yi Kaixiang, Sun Youxian, *Journal of Computer Aided Design & Computer Graphics,* vol. 14, no. 2, pp. 136-139, **2002**.
[15] A. Menezes, P. Oorschot, and S. Vanstone, Handbook of Applied Cryptography. CRC Press, **1996**.
[16] P. Fei, S.S. Qiu, L. Min, An image encryption algorithm based on mixed chaotic dynamic systems and external keys, *IEEE International Conference in Communication Circuits & Systems*, pp. 1135-1139, **2005**.