Journal of Theoretical and Applied Information Technology
15 September 2012. Vol. 43 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NEW ALGORITHM FOR COLOR IMAGE ENCRYPTION USING CHAOTIC MAP AND SPATIAL BIT-LEVEL PERMUTATION

[1]RUI LIU, [2]XIAOPING TIAN
[1] College of Electronic Engineering, Xi' an University of Posts
and Telecommunications, Xi' an 710121, China
E-mail: [1]liu_rui_ok@163.com, [2]xptian@xupt.edu.cn, [3]corresponding author

ABSTRACT

With the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. This paper proposed a new algorithm for color image encryption using chaotic map and spatial bit-level permutation (SBLP).Firstly, use Logistic chaotic sequence to shuffle the positions of image pixels, then transform it into a binary matrix including the red, green and blue components simultaneously, and permute the matrix at bit-level by the scrambling mapping generated by SBLP. Secondly, use another Logistic chaotic sequence rearrangement of the position of the current image pixels. Experiment results and security analysis show that the algorithm can achieve good encryption result and low time complexity, in addition, the key space is large enough to resist against common attack.

Keywords: *Image Encryption, Chaotic Map, Spatial Bit-Level Permutation (SBLP).*

1. INTRODUCTION

Color images are being transmitted and stored in large amount over the Internet and wireless networks, which take advantage of rapid development in multimedia and network technologies. However, as there is always a potential risk of information security in such interconnected environments, protecting confidentiality of color images has become an increasingly important issue in many areas such as remote sensing and satellite imagery, astrophysics, seismology, agriculture, radiology, telemedicine, ecosystems, industrial processes, military communications, and image archiving.

In recent years, plenty of color image encryption approaches have been proposed. However, due to some inherent features of image such as bulk data capacity and high correlation among pixels, traditional encryption techniques, such as DES, AES and RAS, are found to be inefficient for color image encryption. The chaos-based encryption has suggested a new efficient way to deal with the intractable problem of fast and highly security image encryption. It was first proposed in 1989 [1], since then, many researchers have proposed and analyzed a lot of chaos-based encryption algorithms, these work all have been motivated by the chaotic properties such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity. In [2], Behnia et al. have proposed an implementation of digital image encryption scheme based on the mixture of chaotic systems. They use high-dimensional chaotic systems such as a coupled map to enhance the cryptosystem security. In [3] Gao et al. presents a new image encryption scheme, which employs an image total shuffling matrix to shuffle the positions of image pixels and then uses a hyper-chaotic system to confuse the relationship between the plain-image and the cipher-image. More recently, a block encryption algorithm using dynamic sequences generated by multiple one-dimensional chaotic systems is proposed in [4].

This paper proposes a new color image encryption algorithm which based on chaotic map and SBLP. Firstly, use Logistic chaotic sequence to shuffle the positions of image pixels, then transform it into a binary matrix including the red, green and blue components simultaneously, and permute the This paper proposed a new algorithm for color image encryption using chaotic map and spatial bit-level permutation (SBLP)matrix at bit-level by the scrambling mapping generated by SBLP. Secondly, use another Logistic chaotic sequence

Journal of Theoretical and Applied Information Technology
15 September 2012. Vol. 43 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

rearrangement of the positions of the current image pixels. Experiment results and security analysis show that the algorithm can achieve good encryption result and low time complexity, in addition, the key space is large enough to resist against common attack.

(a)

(b)

Figure 1 Original and encrypted image (144×255): (a) original plain image, (b) encrypted image

2. CHAOTIC MAP

Chaos is a definite pseudo-random process produced in nonlinear dynamical systems. It is nonperiodic, non convergent and extremely sensitive to the initial condition. In general, the chaotic system model is given as:

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

Where f is a nonlinear function, and μ is a control parameter, Xk is a real number in the range [0, 1]. If we repeatedly apply it to an initial condition X0, then we will get a chaotic sequence {Xk: k=0, 1, 2…}. Logistic map is a kind of chaotic system that was researched early and used widely in many occasions for its high-level efficiency and simplicity, which is mathematically expressed as:

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

Where $0 < \mu \leqslant 4$ is called bifurcation parameter and Xk is defined as above. When $3.569955672 < \mu \leqslant 4$, the system becomes chaotic [5].

3. THE PROPOSED ENCRYPTION ALGORITHM

Image Encryption. Assume that a 24-bits true color image F contains m×n pixels each having a pixel value f (i, j), where i and j are the coordinates of the pixel. To reduce the workload of the time consuming diffusion part, we suggest introducing certain diffusion effect in the confusion stage by SBLP operation so that shorten the time. The whole procedure of new color image encryption algorithm was as follows:

Step 1. Took the Logistic map as the model, generate two different one-dimensional (1-D) chaotic sequences (Xk1, Xk2) of size (m × n). These sequences are generated based on some given controlling parameters (μ1, μ2) and initial values (X01, X02) which are considered as shared keys for encryption and decryption.

Step 2. Sorted the chaotic sequence {Xk1: k=1,2,…,m×n} from small to large, and got the sorted sequence {X'k1: k=1,2,…,m × n }. Calculated the set of scrambling address codes { Mk1: k=1,2,…,m×n }, where Mk1∈{1,2,…,m×n}. Mk1 was the new subscript of Xk1 in the sorted sequence X'k1.

Step 3. Converted the plain color image F's pixel matrix into a one-dimensional (1-D) sequence {Pk: k=1, 2… m× n}. According to the scrambling address codes { Mk1: k=1,2,…,m×n } to shuffle the positions of image pixels in the sequence {Pk: k=1,2,…,m×n}, got the sequence {P'k: k=1,2,…,m ×n }.

Step 4. Each pixel of {P'k: k=1, 2… m× n} could be represented by an equivalent k-bits binary number, extending from the most significant bit to the least significant bit. At that time, we got a 2-D bit matrix P' with the size of h×w, where h was k-bit binary number (e.g., h=24 for 24-bits true color image, including the red, green and blue components simultaneously), w was the total number of pixels in the image (e.g., w=m×n for image F).

Step 5. To de-correlate the relationship between adjacent pixels, there was SBLP in the confusion stage. These elements in the bit matrix P' were used SBLP and got a new bit matrix E with same size, the key principle of SBLP was showed in Eq. 3, Eq. 4, Eq. 5:

Journal of Theoretical and Applied Information Technology
15 September 2012. Vol. 43 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$\text{Pixel\_index} = \text{Bit\_index} + \text{newpixel\_index} + \text{Offset} \quad (3)$$

In the Eq. 3, Offset is a preset constant, here using it as another key for encryption and decryption, Offset $\in\{1,2,\ldots,m\times n\}$. It could make each bit of the pixel in the image has change, got better confusion-diffusion effect.

$$P' = \begin{pmatrix} \cdots & \cdots & P'_i & P'_{i+1} & P'_{i+2} & P'_{i+3} & \cdots & \cdots \end{pmatrix} = \begin{bmatrix} \cdots & \cdots & P'_{1,i} & P'_{1,i+1} & P'_{1,i+2} & P'_{1,i+3} & \cdots & \cdots \\ \cdots & \cdots & P'_{2,i} & P'_{2,i+1} & P'_{2,i+2} & P'_{2,i+3} & \cdots & \cdots \\ \cdots & \cdots & P'_{3,i} & P'_{3,i+1} & P'_{3,i+2} & P'_{3,i+3} & \cdots & \cdots \\ \cdots & \cdots & P'_{4,i} & P'_{4,i+1} & P'_{4,i+2} & P'_{4,i+3} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \cdots & P'_{24,i} & P'_{24,i+1} & P'_{24,i+2} & P'_{24,i+3} & \cdots & \cdots \end{bmatrix} \quad (4)$$

$$E = \begin{bmatrix} \cdots & \cdots & P'_{1,i} & P'_{1,i+1} & P'_{1,i+2} & P'_{1,i+3} & \cdots & \cdots \\ \cdots & \cdots & P'_{2,i+1} & P'_{2,i+2} & P'_{2,i+3} & P'_{2,i+4} & \cdots & \cdots \\ \cdots & \cdots & P'_{3,i+2} & P'_{3,i+3} & P'_{3,i+4} & P'_{3,i+5} & \cdots & \cdots \\ \cdots & \cdots & P'_{4,i+3} & P'_{4,i+4} & P'_{4,i+5} & P'_{4,i+6} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \cdots & P'_{24,i+23} & P'_{24,i+24} & P'_{24,i+25} & P'_{24,i+26} & \cdots & \cdots \end{bmatrix} = \begin{pmatrix} \cdots & \cdots & E_j & E_{j+1} & E_{j+2} & E_{j+3} & \cdots & \cdots \end{pmatrix} \quad (5)$$

In the Eq. 4 and Eq. 5, i and j represented the number of pixel (i.e., pixel _index and newpixel_index), where i=j+Offset.

Using these elements in the bit matrix E to generate pixels of the image with new values, formed a new 1-D sequence {Ek: k=1, 2,…, m× n }.

Step 6. Using the same method as sequence {Xk1: k=1,2,…,m×n} to get the set of scrambling address codes { Mk2: k=1,2,…,m×n }, where Mk2 ∈{1,2,…,m×n}. Mk2 was the new subscript of Xk2 in the sorted sequence X'k2. According to the { Mk2: k=1,2,…,m × n } to rearrangement of the positions of the image pixels in the {Ek: k=1,2,…,m × n }, got the sequence {E'k: k=1,2,…,m×n }.

Step 7. Transformed 1-D sequence {E'k: k=1,2,…,m×n } into 2-D matrix B with the size of m×n, the B was the cipher image.

Image Decryption. The decryption phase is the inverse process. For the encrypted color image, we use the decryption algorithm by Logistic map to get the permuted color image, and then recover the plain image by the inverse SBLP.

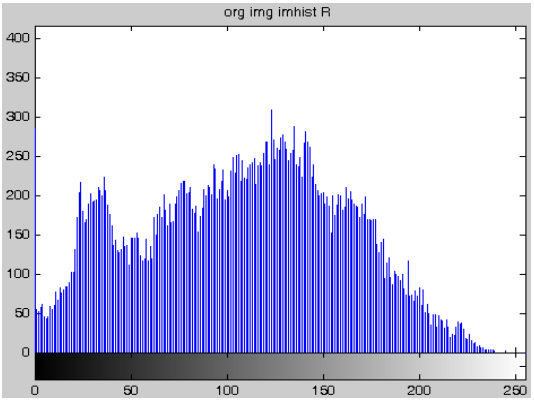
4. EXPERIMENTAL RESULTS AND ANALYSES

Experimental Results and Histogram Analysis. Here we set the initial values X01=0.25, X02=0.35. The controlling parameters are μ1=3.98164, μ2=3.71194 and Offset =3. The size of the plain 24-bits color image of City is cropped to 144×255. The resulting encrypted image is shown in Figure1 (b).

The histograms of red channel of the plain and the encrypted images are shown in Figure2. It is clear from Figure2 that the histogram of the encrypted image is uniform and significantly different from the histogram of the plain image. This result indicates that it is very difficult to use statistical analysis to attack the proposed encryption algorithm.

Key Space and Sensitivity 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 (μ1, X01, μ2, X02, Offset), where μi ∈ (3.569955672…, 4] and X0i∈(0,1), i=1,2, μi and X0i 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 $(10^{14})^2\times(10^{16})^2\times 108=10^{68}$. Note that the range of μi is (3.569955672…, 4], therefore a 14-digit precision is assumed. Thus, brute-force attacks on the key are computationally infeasible.

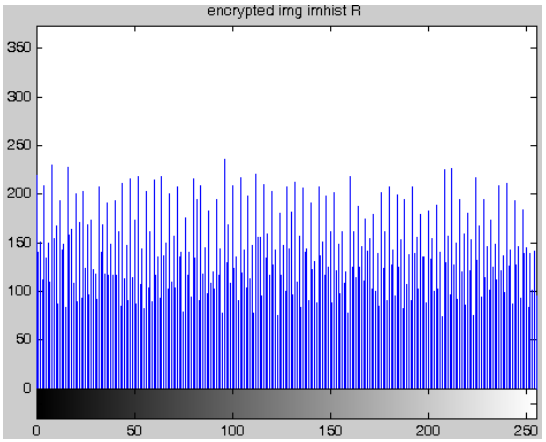
We have carried out a key sensitivity test using a key that is one digit different from the original key to decrypt the encrypted image. The resulting image is totally different from the original image as shown in Figure3. This demonstrates that the proposed algorithm is very sensitive to any change in the secret key value.



(a)

Journal of Theoretical and Applied Information Technology
15 September 2012. Vol. 43 No.1

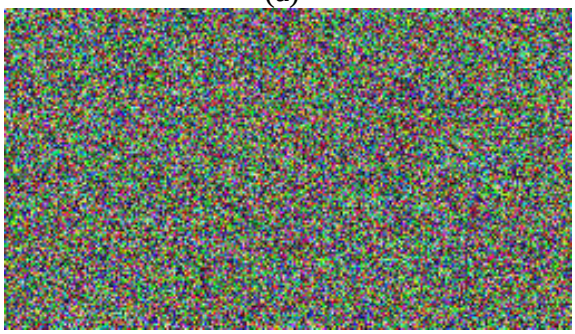
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



(b)

Figure 2 Histogram analysis: (a) histogram of red channel of the plain image shown in Figure1 (a), (b) histogram of red channel of the encrypted image shown in Figure1 (b)

(a)



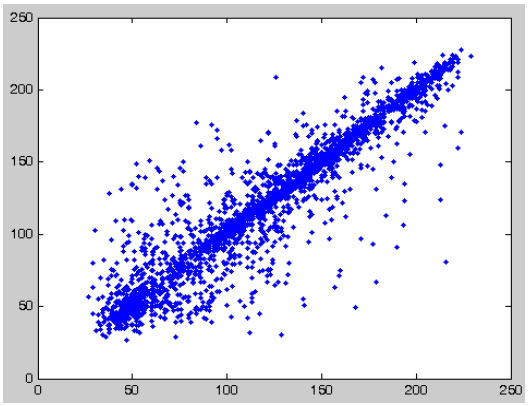
(b)

Figure 3 Key sensitivity: (a) decrypted image shown in Figure1 (b) with key= {3.98164, 0.25, 3.71194, 0.35, 3}, (b) decrypted image shown in Figure1 (b) with key= {3.98165, 0.26, 3.71195, 0.36, 4}

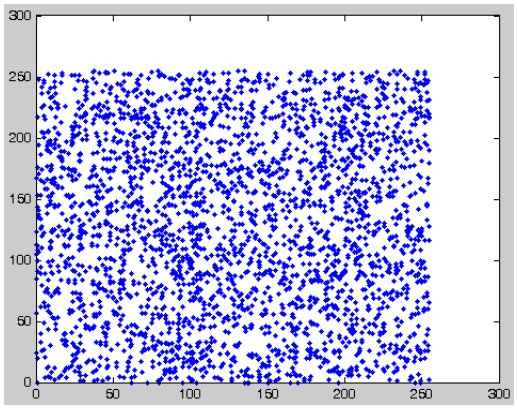
Correlation of Two Adjacent Pixels. In order to evaluate the encryption quality of the proposed encryption algorithm, the correlation coefficient is used. To calculate the correlation coefficients between two vertically, horizontally and diagonally adjacent pixels of an encrypted image, the following equation is used [6].

$$r_{xy} = \frac{|Cov(x,y)|}{\sqrt{D(x)} \cdot \sqrt{D(y)}}$$

$$\begin{cases} E(x) = \frac{1}{K}\sum_{i=1}^{K} x_i \\ D(x) = \frac{1}{K}\sum_{i=1}^{K} (x_i - E(x))^2 \\ Cov(x,y) = \frac{1}{K}\sum_{i=1}^{K} (x_i - E(x))(y_i - E(y)) \end{cases} \quad (6)$$



(a)



(b)

Figure 4 Correlation of two adjacent pixels: (a) distribution of two horizontally adjacent pixels in the red channel of the plain image (Figure1 (a)), (b) distribution of two horizontally adjacent pixels in the red channel of the encrypted image (Figure1 (b))

Where x and y are gray values of two adjacent pixels in the image. We randomly select 3000 pairs of vertically, horizontally and diagonally adjacent pixels of red channel of the plain and encrypted images and calculate the correlation coefficients in three directions separately. Figure4 shows the correlation distribution of two horizontally adjacent pixels in the original and its encrypted image. The results are the same to vertical and diagonal directions.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The correlation coefficients for the two adjacent pixels of red channel of the plain and encrypted images are shown 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 Adjacent Pixels-

Correlation Calculation Based on	Correlation Coefficients of Adjacent Pixels		
	Horizontal direction	Vertical direction	Diagonal direction
red channel of Figeur1(a)	0.9678	0.9596	0.9304
red channel of Figeur1(b)	0.0019	0.0042	0.0087

5. SUMMARY

This paper proposes a SBLP and chaotic map to encrypt color image. Firstly, use Logistic chaotic sequence to shuffle the positions of image pixels, then transform it into a binary matrix including the red, green and blue components simultaneously, and permute the matrix at bit-level by the scrambling mapping generated by SBLP. Secondly, use another Logistic chaotic sequence rearrangement of the positions of the current image pixels. The security analysis and experimental results show that the proposed algorithm can achieve good encryption result and low time complexity, in addition, the key space is large enough to resist against common attack. This makes it suitable for securing video surveillance systems, multimedia applications and real-time applications such as mobile phone services.

6. ACKNOWLEDGMENT

This work was supported by the Natural Science Foundation of Shaanxi Province of China (No. 2009JM8004), the Young Scholars Plan Project of Xi'an University of Posts and Telecommunications (No.ZL2010-03), and the Natural Science Foundation of Education Department of Shaanxi Provincial Government of China (No. 2010JK821).

REFERENCES

[1] R. Matthews, "On the derivation of a chaotic encryption algorithm", *Cryptologia*, Vol.13, No.1, 1989, pp:29-42

[2] S. Behnia, A. Akhshani, H. Mahmodi and A.Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps, Chaos", *Solitons & Fractals*. Vol.35, No.2, 2008, pp:408-419.

[3] T. Gao, Q. Gu and Z. Chen, "A new image encryption algorithm based on hyper-chaos", *Phys Lett* , Vol.374, No.4, 2008, pp:394-400.

[4] X.Y.Wang and Q. Yu, "A block encryption algorithm based on dynamic sequences of multiple chaotic systems", *Commun Nonlinear Sci Numer Simul*. Vol.14, No.2, 2009, pp:574-581.

[5] Y. Feng J. Li and X. Yang, "Discrete chaotic based 3D image encryption scheme", *in Proc. of the Sympos*. on Photonics and Optoelectronics, (SOPO 2009), Aug. 2009, pp1-4.

[6] Z.W. Shang, H.G. Ren and J. Zhang, "A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation", *ICYCS* 08, Sep.2008, pp:2942-2947.