http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (4): 680-685, 2010
ISSN 1812-5638

Image Encryption Algorithm Based on Universal Modular Transformation

Xue Yang, Xiaoyang Yu, Qifeng Zou and Jiaying Jia
The Higher Educational Key Laboratory for Measuring and Control Technology and Instrumentations, Harbin University of Science and Technology, No. 4 Lin Yuan Road, Xiang Fang District, Lina Shan, P.O. Box 326, Heilongjiang Province 150040, People's Republic of China

Abstract: Image encryption is essential to assure information security. Universal modular transformation is a widely applied encryption method, but it has some disadvantages such as a relatively small quantity of keys and insecurity. A uniform block encryption method is proposed in this study to improve the image entropy of encryption and an image is encrypted with the universal modular transform combined with a chaotic mapping. Experimental results show that this algorithm can provide good encryption quality and reach high safety. Moreover, the proposed algorithm is robust to shear attack and noise attack.

Key words: Image encryption, universal modular transformation, uniform encryption, chaotic map

INTRODUCTION

With the development of computer and communication, the security of the multimedia digital image has become the focus of Internet. Universal modular transformations such as Fibonacci transformation (Zou and Liu, 2007), Arnold Cat transformation (Huang and Xiao, 2009; Chen, 2006) and affine modular transformation (Zou *et al*., 2000) are the most widely used methods nowadays for their simplicity. However, such algorithms have to be iterated several times to achieve good results and they have too small key quantities to resist exhaustive attack. A new approach which leads to uniform scrambling is proposed to increase the entropy of encrypted image in this study. Furthermore, a uniform block encryption algorithm combined with a class of chaotic mapping (Kwok and Tang, 2007; Fan and Jiang, 2004; Huang and Feng, 2007; Ren *et al*., 2008) based on the universal modular transformation is proposed to increase the key quantities. Finally, experimental results are provided to verify the effectiveness of the proposed method.

UNIVERSAL MODULAR TRANSFORMATION

Suppose an image consisting of N×N pixels, where (x, y) and (x', y') are the coordinate of a pixel in the original image and the scrambled image, respectively. The universal modular transformation is given as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} L(x,y) \\ \Gamma(x,y) \end{bmatrix} = \left\{ \begin{bmatrix} a & b \\ c & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} \right\} \bmod(N) \qquad (1)$$

where, mod (N) means the modular, which is to ensure that the pixels of the image still fall on the original region after transformed.

When the matrix determinant $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1$, the transform is area-preserving and one-to-one mapping which can be used to image scrambling. Because $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1$ and N are prime numbers each other, the universal modular transformation is periodical. While e = f = 0, if a = b = c = 1, d = 0 the transform is Fibonacci transformation; if a = b = c=1, d =2 it is Arnold Cat transformation. While e≠0 and f≠0, the transform is affine transformation. The universal modular transformations can be considered as the combination of the basic universal transformations including translation transformation, stretching transformation, symmetry transformation, shearing transformation, all of which have the similar characteristics.

UNIFORM BLOCK ENCRYPTION

The essence of image encryption or image scrambling is to reduce the correlation of pixel positions and the correlation of pixel values until they are irrelevant. From the perspective of information theory, digital image should be seen as information source composed of the non-overlapping blocks with arbitrary shapes and numbers and the pixels of image can be seen as messages of the information source. Image scrambling process can be considered as the process of enhance uncertainty, also as the process of increasing the amount of image information. The correlation of the natural image pixels is

Corresponding Author: Xue Yang, The Higher Educational Key Laboratory for Measuring and Control Technology and Instrumentations, Harbin University of Science and Technology, No.4 Lin Yuan Road, Xiang Fang District, Lina Shan, P.O. Box 326, Heilongjiang Province 150040, People's Republic of China

deemed to be the largest in respective block and the uncertainty is as well. If some original image pixels in block σ_1 still distribute in the same block σ_2 of the scrambled image, even if the block σ_1 and σ_2 have different situation, the certainty of these pixels are still large and the corresponding information content generated by scrambling is less. Therefore, the study defines the concept of image position entropy by Eq. 2:

$$H(S) = \sum_{k=1}^{B} H_k(P) \tag{2}$$

where, B is the total number of image blocks, $H_k(P)$ is the entropy of the kth block and denotes the average information capacity in this block. H(S) is the image position entropy.

$$H_k(P) = -\sum_{ij} P(i,j)\log P(i,j) \tag{3}$$

where, P(i,j) is the probability of pixel which coordinates (i,j) in original image appears at the kth block in the scrambled image. By the property of discrete information source entropy, we known that $H_k(P)$ will reach the maximum when the probability P(i,j) is equal. At the same time H(S) will get its maximum value. So, the perfect state of image scrambling is the random pixel in respective block of the scrambled image has the equal probability of coming from the random situation in original image. It also means that average information content will get the maximum when the probability that pixels in the same block of original image distribute into different blocks is equal. Temporality the effect of image scrambling is the best. The definition of uniform scrambling proposed is as follows:

- All the pixels in the same block of original image distribute into all the blocks of scrambled image and the every block has one pixel at least, without regarding to the order of the pixels appearance, accordingly all the pixels in the same block of scrambled image come from different blocks of original image, this condition is described uniform scrambling

Figure 1 shows that all the pixels in the first block of the original image are distributed into all the blocks of the scrambled image. Thus, the ideal block numbers is N for an original image of size N×N. But the number maybe not the integer for images of different size, so we can take the two numbers which has the approximate value to N.

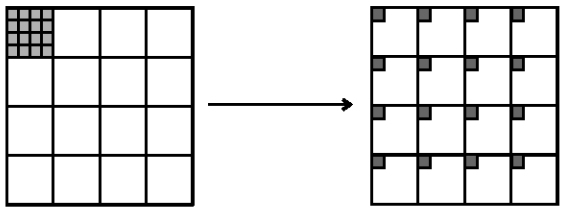

Fig. 1: Image uniform encryption

UNIFORM BLOCK ENCRYPTION ALGORITHM BASED ON UNIVERSAL MODULAR TRANSFORMATION

The basic principle of the algorithm: In order to apply the definition of uniform scrambling to Universal modular transformation, we need to improve the transformation because the classical methods are maps for the whole image, while according to the proposed method pixels should mapped from blocks to the whole image. The Universal modular transformation in block (i, j) is described by Eq. 4:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} L_{ij}(x,y) \\ \Gamma_{ij}(x,y) \end{bmatrix} = \left\{ \begin{bmatrix} a_{ij} & b_{ij} \\ c_{ij} & d_{ij} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e_{ij} \\ f_{ij} \end{bmatrix} \right\} \bmod \left(\frac{N}{B} \right) \tag{4}$$

where, N is the size of the image, B is the total number of original image blocks just means there are B×B blocks in the image and a_{ij}, b_{ij}, c_{ij}, d_{ij}, e_{ij}, f_{ij} is the parameters of each block. i, j∈(1,B) and i, j are positive integers.

Uniform block encryption algorithm based on universal modular transformation is given by Eq. 5:

$$\begin{cases} \begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} L^m(X,Y) \\ \Gamma^m(X,Y) \end{bmatrix} \\ \begin{bmatrix} X'' \\ Y'' \end{bmatrix} = B \times \begin{bmatrix} L_{ij}^k(X'-1,Y'-1) \\ \Gamma_{ij}^k(X'-1,Y'-1) \end{bmatrix} + \begin{bmatrix} L(i,j) \\ \Gamma(i,j) \end{bmatrix} \end{cases} \tag{5}$$

where, X and Y are the coordinates of original image pixels, X' and Y' are the coordinates of whole scrambled image pixels, X'' and Y'' are the coordinates of image pixels which are taken uniform block encryption on whole scrambled image m, k are the times of scrambling.

The equation means that we first scramble the image in the whole for several times and then encrypt image k times by uniform block encryption algorithm. If m = 0 that means encrypt image k times by uniform block encryption algorithm directly.

The study proposed a scheme to realize uniform block encryption algorithm by affine modular encryption transformation. To simplify the arithmetic and make the transformation area-preserving, the parameters are constrained. The formula is described by Eq. 6:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \left\{ \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} \right\} \bmod(N) \tag{6}$$

The affine modular transformation of digital image keeps the cycles of Arnold Cat transformation while it has more parameters to choice, so it can increase the secrecy of image. The equation of uniform block encryption algorithm based on affine modular transformation is described by Eq. 7:

$$\begin{cases} \begin{bmatrix} X' \\ Y' \end{bmatrix} = \left\{ \left(\begin{bmatrix} 1 & a_0 \\ b_0 & a_0 b_0 + 1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} + \begin{bmatrix} e_0 \\ f_0 \end{bmatrix} \right) \bmod(N) \right\}_{n_1} \\ \begin{bmatrix} X' \\ Y' \end{bmatrix} = B \times \left\{ \left(\begin{bmatrix} 1 & a_i \\ b_i & a_i b_i + 1 \end{bmatrix} \begin{bmatrix} X'-1 \\ Y'-1 \end{bmatrix} + \begin{bmatrix} e_i \\ f_i \end{bmatrix} \right) \bmod\left(\frac{N}{B}\right) \right\}_{n_2} + \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} \end{cases} \tag{7}$$

where a_0 and b_0 are parameters of image scrambling in the whole, a_i, b_i, e_i and f_i are parameters after image taken in uniform block encryption, $i \in (1, B^2)$ and i is positive integers. (k_1, k_2) is the coordinate of partitioned matrix for image block, n_1, n_2 are the number of iterative process.

The proposed method can take a_0, b_0, a_i, b_i, e_i and f_i as cipher keys and the key space is large because parameters of different blocks are different. It is impractical remembering all the parameters so we use chaotic map to deal with that.

Improved logistic map: The equation of logistic map is described with Eq. 8:

$$x_{n+1} = f(\mu, x_n) = \mu x_n (1 - x_n) \tag{8}$$

where, $0 < \mu \le 4$, $x_n \in (0,1)$.

The logistic map is chaotic map when $3.5699456 < \mu \le 4$, we often make $\mu = 4$. For Logistic map does not satisfy uniform distribution, a better random system is given as:

$$y_n = (2/\pi)\arcsin\left(\sqrt{x_n}\right), \quad n = 1,2,3,\cdots \tag{9}$$

where, y_n is also the chaotic sequence and it satisfies uniform distribution. Simulation shows that the system response is extremely sensitive to the initial values, so we can amplify each value of y_n and get round-off to generate the parameters of different blocks.

The Implementation of the algorithm
Encryption scheme:

- **Step 1:** Provide four initial values $x_1(0)$, $x_2(0)$, $x_3(0)$, $x_4(0)$ to generate chaotic sequence $\{x_1(k)\}, \{x_2(k)\}, \{x_3(k)\}, \{x_4(k)\}$; then improving the four sequences to $\{y_1(k)\}, \{y_2(k)\}, \{y_3(k)\}, \{y_4(k)\}$ by Eq. 9. Get the sequence values which are in the place after the second and third of decimal point to decimal integers. Array those decimal integers to integer sequences $\{a(k)\}$, $\{b(k)\}$, $\{e(k)\}$, $\{f(k)\}$ by nature order and assign these values to the parameters a_i, b_i, e_i, f_i in different blocks
- **Step 2:** Perform affine modular transformation n_1 times for original image F(X,Y) with $a_0 = a(0)$, $b_0 = b(0)$, $e_0 = e(0)$, $f_0 = f(0)$. Then the whole scrambled image F'(X',Y') is obtained
- **Step 3:** Divide the image F'(X',Y') into B×B blocks, generate the last scrambled image by taking Eq. 7 n_2 times with the parameters $\{a(k)\}$, $\{b(k)\}$, $\{e(k)\}$, $\{f(k)\}$

Decryption scheme:

- **Step 1:** Perform the same operation as step 1. in the encryption scheme. Then, Calculate the lowest common multiple T_2 for different cycle with a_i, b_i, , let $n_{22} = T_2 - n_2$
- **Step 2:** Split the image F''(X'',Y'') into N^2/B^2 blocks, generate image F'(X',Y') by taking Eq. 7 n_{22} times with the parameters $\{a(k)\}$, $\{b(k)\}$, $\{e(k)\}$, $\{f(k)\}$
- **Step 3:** Take affine modular transformation n_1 times for image F'(X',Y') with parameters $a_0 = a(0)$, $b_0 = b(0)$, $e_0 = e(0)$, $f_0 = f(0)$. After that the decrypted image F(X,Y) is generated

RESULTS AND DISCUSSION

To demonstrate the effectiveness of the proposed method, experimental results are given in this section. For the classical Lena image with 256×256 pixels as in Fig 2, the initial values for the chaotic mapping is set as $x_1(0) = 0.1$, $x_2(0) = 0.2$, $x_3(0) = x_4(0) = 0.3$ and the image is divided into 16×16 blocks.

Encryption experiments and some analysis: In this part, the universal modular encryption algorithm without uniform block scrambling is compared with the proposed method under the condition of the same number of

Fig. 2: Original image

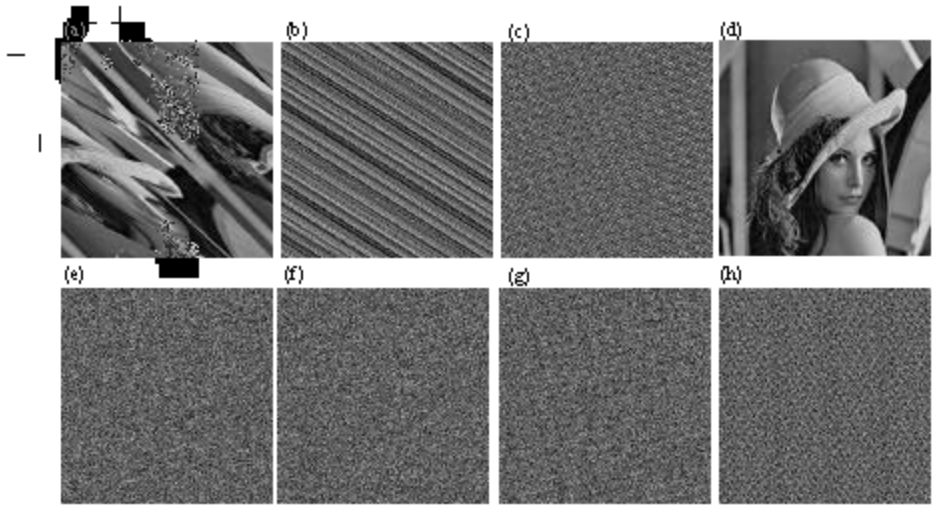

Fig. 3: Comparing the effect of encryption

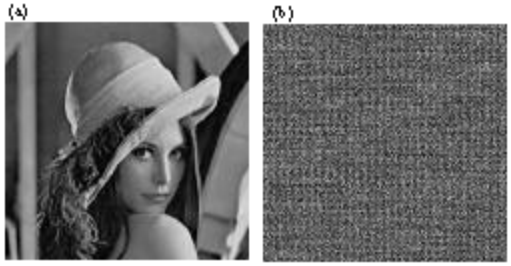

Fig. 4: Decrypting image adopting little difference key. (a) $x_1(0) = 0.218$, (b) $x_1(0) = 0.218+10^{-12}$

transformation times. The experimental results are given in Fig. 3, where, Fig. 3a-d are the output results by the Universal modular encryption algorithm with 1, 4, 64 and 192 times of transformations, respectively. And Fig. 3e-h are the corresponding experimental results with the uniform block scrambling encryption algorithm.

From the above comparison, it can be seen that the Universal modular encryption algorithm without uniform block scrambling has the periodic characteristics and the encryption results may not be good with the first several times of iteration. Also, the encryption quality fluctuates with increased iteration times. With the uniform block scrambling method, however, good encryption result can be obtained even without any iteration and thus may be better than the Universal modular encryption method.

Key sensitivity experiments and some analysis: Suppose an image is encrypted with the key $x_1(0) = 0.218$, $x_2(0) = 0.25$, $x_3(0) = 0.7$, $x_4(0) = 0.95$ and it is decrypted with $x_2(0)$, $x_3(0)$, $x_4(0)$ fixed to the right value. After that, the decryption results with $x_1(0) = 0.218$ and $x_1(0) = 0.218000000001$ are shown in Fig. 4a and b, respectively.

From this experiment results, it is shown that the original image can not be obtained even with a bias of 10-12 in one of the key components. Thus, the proposed encryption method in this paper can have a very large key space and ensure the security of the encryption from exhaustive attacking with the hardware condition of c today.

Anti-shearing attack experiments: In this experiment, an image is respectively encrypted with the universal modular encryption algorithm with and without uniform block scrambling at first. Then, the shearing attack is performed on the encryption results with the shearing area being about 10~20%. Image restoration is performed with the attacked encryption results at last as can be seen from Fig. 5a-d and 6a-d, respectively.

From the above experimental results, it can be seen that if the universal modular encryption algorithm is applied with limited iteration times, the contour of the restored image is smeared when suffering from the shear-attack. With the uniform block scrambling encryption algorithm, the contour can be better restored and the information loss can be less because the shear-attacked part of the image can be distributed to the whole image and thus makes it more robust to shear-attack.

Anti-noise experiments: Zero-mean Gaussian noise with the variance of 0.5 is added to images encrypted by the affine transform scrambling encryption algorithm and universal modular encryption algorithm, respectively. The decryption results are shown in Fig. 7a-d and 8a-d.

From the decryption results, it can be seen that when the encryption result is polluted by the Gaussian noise, the contour of the restored image can be better reserved by the uniform block scrambling encryption algorithm.

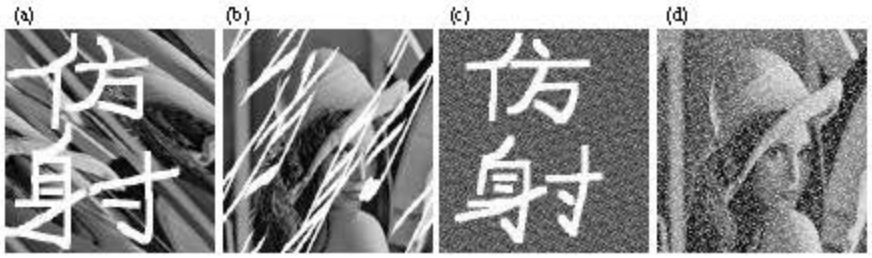

Fig. 5: The cutting effect and decrypting by affine transform (a) encrypting one time and cutting, (b) decrypting with a, (c) encrypting 64 times and cutting and (d) decrypting with c

Fig. 6: The cutting effect and decrypting by uniform algorithm. (a) encrypting one time and cutting, (b) decrypting with a, (c) encrypting 64 times and cutting and (d) decrypting with c

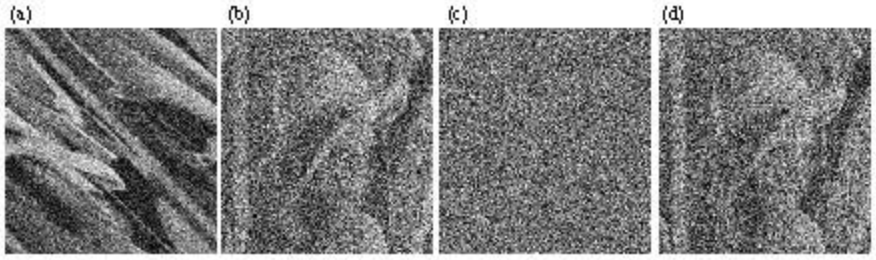

Fig. 7: The noising effect and decryption by affine transform. (a) encrypting one time and adding noise, (b) decrypting with a, (c) encrypting 64 times and adding noise and (d) decrypting with c

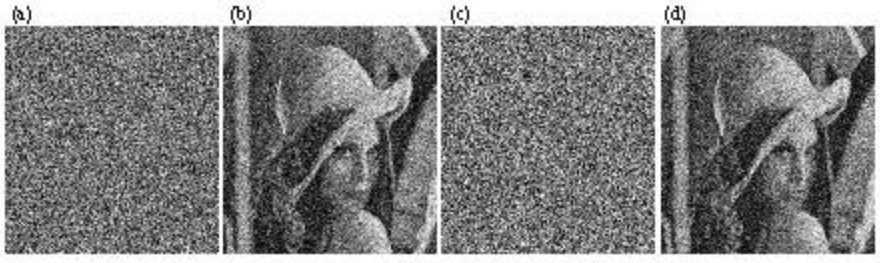

Fig. 8: The noising effect and decryption by universal algorithm. (a) encrypting one time and adding noise, (b) decrypting with a, (c) encrypting 64 times and adding noise and (d) decrypting with c

In present experiments, independent runs of present proposed method, we choose the classical Lena image with 256×256 pixels as original image and compare performance of our proposed method with the affine modular transform methods through three experiments. Figure 3 shows that the affine modular encryption algorithm without uniform block scrambling is compared with the proposed method under the condition that we

scramble original image 1, 4, 64 and 192 times. Figure 5 and 6 show the universal modular encryption algorithm is applied with limited iteration times, the contour of the restored image is smeared when suffering from the shear-attack. Figure 7 and 8 show that Zero-mean Gaussian noise with the variance of 0.5 is added to images encrypted by the affine transform scrambling encryption algorithm and uniform modular encryption algorithm.

In addition, Fig. 4 show the proposed encryption method in this study can have a very large key space and ensure the security of the encryption from exhaustive attacking with the hardware condition of today. As a whole, our approach is superior to the existing universal modular encryption algorithm methods. The traditional universal modular transformation algorithms have to be iterated several times to achieve good encryption results and they have too small key quantities to resist exhaustive attack. This method can obtain good encryption result even without any iteration and it has the advantage such as large quantity of keys, robust to cutting attack and noise attack. Also, it has feasibility and validity.

CONCLUSIONS

From essential analyzing to image scrambling, a concept of uniform block scrambling is proposed from enhancing encryption image entropy and makes use of affine modular transform, combines to chaos theory, provides a image block uniform encryption algorithm. A number of experiments analysis proved that the proposed algorithm has the advantage such as large quantity of keys, robust to cutting attack and noise attack. Also, it has feasibility and validity.

ACKNOWLEDGMENT

This study was supported by the National Natural Science Foundation of China (60572030) and the Chun Hui Program of Chinese Education Department (Z2007-1-15014).

REFERENCES

Chen, M., 2006. Image steganography based on Arnold transform. Appl. Res. Comput., 1: 235-237.

Fan, C. and C. Jiang, 2004. Image encryption based on discrete chaotic maps. Opt. Precis. Eng., 12: 179-184.

Huang, F. and Y. Feng, 2007. Novel 2D chaotic map based on image segementation and image encryption approach. Opt. Precis. Eng., 15: 1096-1103.

Huang, L. and D. Xiao, 2009. The best image scrambling degree of binary image based on Arnold transform. J. Comput. Appl., 2: 474-476.

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

Ren, H., Z. Shang and J. Zhang, 2008. Image encryption algorithm based on new two-dimensional map for rectangular image. Opt. Precis. Eng., 8: 1483-1480.

Zou, J., X. Tang and G. Li, 2000. Affine module transformation of digital image and its periodicity. J. North China Univ. Technol., 03: 13-16.

Zou, W. and H. Liu, 2007. Digital image scrambling technology based on three dimension similar fibonacci transformation and its periodicity. Comput. Digital Eng., 9: 133-135.