TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 15, No. 3, September 2015, pp. 569 ~ 575
DOI: 10.11591/telkomnika.v15i3.8230

Hybrid Encryption Algorithm Based on Spatial and Gray Level Information

Suolan Liu[1,2]*, Chen Chen[2], Yue Chen[1], Hongyuan Wang[1]
[1]School of Information Science & Engineering, Changzhou University, Changzhou, PR China,
Ph./Fax:+086-051986330284/051986330558
[2]Department of Electrical Engineering, University of Texas at Dallas, Richardson, Texas, United States,
Ph.: +001-2149857479
*Corresponding author, e-mail: lan-liu@163.com

Abstract

With the rapid development of image production and applications, image security has become very important. Traditional image encryption algorithms, such as Arnold transform is used widely, but it has the defect of long transform periodicity, which costs large time and computation memory. Therefore, based on the analysis of the defect of traditional image scrambling methods, a novel hybrid encryption scheme is proposed. It uses image's spatial and gray level information at the same time. Comparative experiments show it has the advantages of easy implementation, large key space, and good scrambling effect by only one time processing instead of many times.

.

Keywords: *hybrid encryption, spatial information, gray level information*

1. Introduction

With the advance of computer network, data transmission becomes very convenient. One can use a network to transfer text, image, audio, video and other multimedia information. However, some data have to be encrypted before transmission due to privacy and security, such as military satellite photos, design drawings, etc. Image scrambling technology is an approach for image information encryption [1]. It can scramble the original image so that the transformed image cannot reflect the original image information. There are three main kinds of scrambling methods including spatial scrambling, gray transform scrambling and hybrid scrambling which is the combination of the former two schemes.

Image scrambling based on spatial transformation is easy to realize, but it has the disadvantage of not being able to change the histogram of the image. In recent years, chaotic map is widely used in the process of encryption [2, 3]. But this kind of scheme has shortcoming as proposed in literature [3]. Some chaos-based image encryption schemes using plain-images independent secret code streams have weak encryption security and are vulnerable to chosen plaintext and chosen cipher-text attacks. Arnold transform (ART) proposed by V. I. Arnold in 1960 in the research of ergodic theory. It is also called cat mapping [4]. It is also a chaotic map from the torus into itself. Fibonacci transform [5] and Hilbert transform [6] are similar to ART in scrambling image. They only change the positions of the image pixels rather than the pixel values. Once the set of pixels is identified, each permutation and combination of pixels can be determined and the decrypted image is one of them. Especially, if the size of an image is small, it becomes easy to crack the encryption.

Image scrambling based on pixel gray level transformation aims at changing the pixel gray value. The correction algorithm based on Virginia encryption [7], encryption algorithm based on the gray value transform [8], and the gravitational model [9] all belong to gray level transformation methods. These encryption algorithms only use image gray information. Experiments find that the contour of original image always shown in the encrypted images. This might cause security issues in data transmission.

Scrambling algorithms based on spatial transformation or pixel gray level transformation only use a single feature (position or gray value) to achieve the scrambling effect. With their disadvantages, the image safety cannot be guaranteed [10, 11]. Therefore, in this paper a

Received May 18, 2015; Revised July 29, 2015; Accepted August 16, 2015

hybrid encryption scheme based on Arnold transform and gravitational model is described. The proposed algorithm integrates two different image features (pixel positions and gray values) to achieve effective encryption image. The experimental results demonstrated that our proposed algorithm not only meets the large key space requirement of image transmission, but also has good properties in anti-clipping and compression.

The remaining of this paper is organized as follows. Section 2 presents related work. Section 3 describes the proposed scheme. Section 4 shows experimental results and reports the security of our method. Finally, we conclude in section 5.

2. Related work

2.1. Image Spatial Scrambling Based on Arnold Transform

Arnold transform (ART) was proposed by Arnold in the research of Ergodic theory [4]. It redirects pixel positions by a series of cutting and splicing.

For each pixel with position (x, y) in an $N \times N$ image I, its Arnold transform can be calculated as:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ N) \quad (1)$$

(x', y') is the transformed position.

ART has been proved to be periodic. The original image can be restored by a number of encryption processing. The period of Arnold transform is determined according to the following formula:

$$T = \min\left\{n \mid \{ART[I(x, y), N\}^n = f(x, y)\right\} \quad (2)$$

$\{ART[I(x, y), N\}^n$ means n times encryption of image I. n is the number of encryption iterations. $N > 2$, and $T \le N^2 / 2$. $f(x, y)$ is pixel value.

The decryption of ART is to use its periodicity. If the number of iterations in encryption is n_e, we need to calculate the remaining number of transformation to satisfy the following formula:

$$n_d = rT - n_e \quad (3)$$

r is an integer and $r \ge 1$, n_d is the number of decryption iterations. Usually, we set $r = 1$.

2.2. Image Gray Level Scrambling Based on Gravitational Model

Gray level transform method has many advantages, such as large key space and strong anti-attack ability. In [9], a gravitation model was proposed based on the gray level transform.

Let us consider a gray-scale image $K = \{0 \le f(i, j) \le 255; i = 0,1,2,\cdots, M-1; j = 0,1,2,\cdots N-1\}$ as $M \times N$ particles located in the same plane of a space. For a unit particle outside the plane, it has gravitational force upon all $M \times N$ particles according to the theory of gravitation. Therefore, with the gravitational force, each particle pixel value will be shifted.

The transformation based on gravitational model is defined as:

$$B'_{ij} = [k \frac{mm_{ij}}{(x-i)^2 + (y-j)^2 + z^2}] \bmod 256 \oplus B_{ij} \quad (4)$$

k is the gravity coefficient. m is the quality of a unit particle, so $m=1$. x, y, z are coordinates, where z≠0, so no matter what value of x, y, the distance (denominator) $r^2=(x-i)^2+(y-j)^2+z^2>0$ can be guaranteed. In coordinates (i, j), m_{ij} is pixel quality and B_{ij} is pixel gray value. B'_{ij} is pixel gray value in transformed coordinates (i, j).

3. Proposed Hybrid Encryption Algorithm

In this paper, we propose to a hybrid encryption algorithm. It first uses gravitation model to scramble image gray value, then uses an improved Arnold transform to scramble pixels' position. The Arnold transform is amended to fit to image sized $M*N$. Hybrid algorithm integrates the two features of position and gray information to achieve effective encryption effect. Its steps are set as follows:

(1) Set original image as I, its size is $M*N$, then decompose it to a matrix. The corresponding coordinate value is equal to the pixel value.

(2) From point (0, 0), one time gravitation transform is done for each pixel. If the original image is a color image, gravitation transform is done in each channel of R, G and B [13,14]. This step is executed to the point $(M-1, N-1)$.

(3) Set image obtained from the second step as a source image. Choose iteration number n_e. For each point of image, Arnold transforms of n_e times are done. Then positions of all the points are changed.

(4) Hybrid encryption image is obtained from the third step.

The decryption process is the inverse of the encryption process. To encryption image, ART is done first, then gravitation transform is done.

4. Experimental Results

4.1. anti-clipping performance

Figure 1, Figure 2 and Figure 3 are anti-clipping experiments. (a) is original image, (b) is encryption image, (c) is clipping image of (b), (d) is decryption image of (c). In addition, in order to make comparison, we set clipping position and size in Figure 1 the same as in Figure 2 and Figure 3.

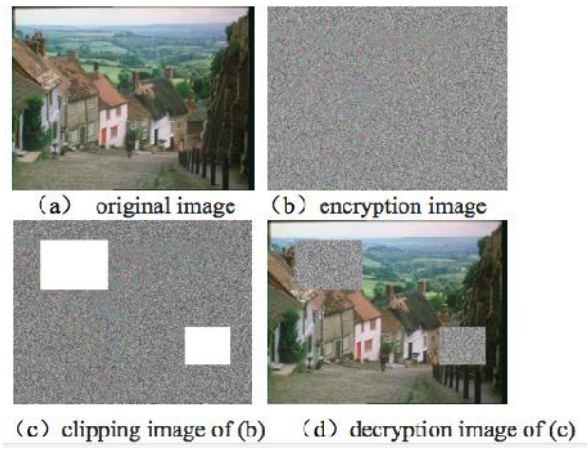

Figure 1. Anti-clipping performances based on gravitation model [9]

Figure 1 shows anti-clipping performances based on gravitation model. In this experiment, we set scrambling key as follows: $m_{ij}=g(i, j)=25i^2+j^3+186$, $k=12.9\times10^{14}$, $x=436$, $y=275$, $z=388$.

Position and size of the two clippings are set as:

(1) From (79 62) to (284 218), the clipping size is 205×156.

(2) From (517 335) to (655 454), the clipping size is 138×119.

Figure 2 shows anti-clipping performances based on Arnold transform. In this experiment, we set $n_e = 55$.

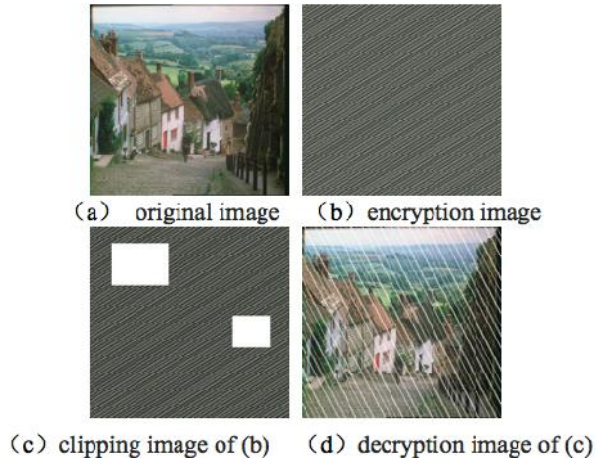

Figure 2. Anti-clipping performances based on Arnold transform [4]

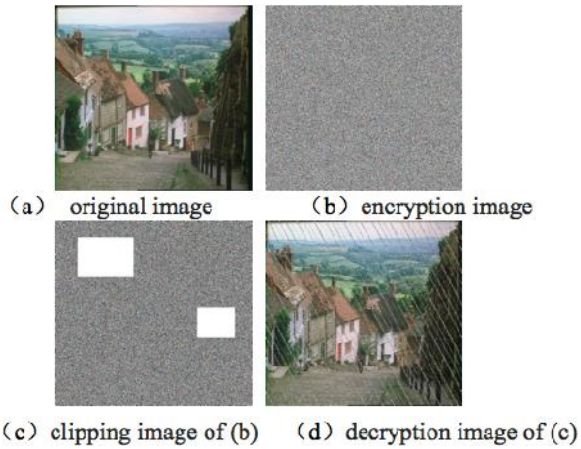

Figure 3. Anti-clipping performances based on proposed hybrid encryption scheme

Figure 3 shows anti-clipping performances based on our proposed hybrid encryption scheme. Scrambling key is set the same as in Figure 1.

From the above three experiments, we can find that:

(1) To scrambling algorithm based on gravitation model, if clipping is done on encryption image, we will find that only the clipping zone cannot be restored in the process of decryption. The main reason of the phenomenon is that gravitation model can only scramble image gray value. Therefore, other parts of the image will not be affected by the clipping.

(2) To scrambling algorithm based on Arnold transform, if clipping is done on encryption image, we will find that its decryption image is different from gravitation model. It seems that the decryption image is a noised original image. The main reason of the phenomenon is that Arnold transform belongs to pixel position scrambling method. Original pixels are dispersed to different positions. Then if one part is clipped, it is similar to every pixel position of the whole image is

clipped in the process of. When scrambling is sufficiently uniform, noise in the decryption image is also uniform.

(3) To scrambling algorithm based on hybrid encryption, it mainly absorbs the advantages of the ART, so that its decryption image is different from gravitation model. The latter wholly loses the clipping parts information.

From the above analysis, we may draw a conclusion that the advantage of hybrid scrambling algorithm is it can maintain the overall information of image even its locally clipped.

4.2. Anti-compression Performance

Figure 4 is a group of experiments. First, the original image is encrypted by using the above three kinds of encryption algorithms, then anti-compression experiments are done (decrypting after compression the encryption image) [15]. (a) is a fruits.png for the original image. (b), (c) and (d) are encryption images by using gravitation model [9], ART algorithm [4] and our proposed hybrid scheme. (b1), (c1) and (d1) are decryption images of (b), (c) and (d) compressed by quality 10. (b2), (c2) and (d2) are decryption images of (b), (c) and (d) compressed by quality 60.

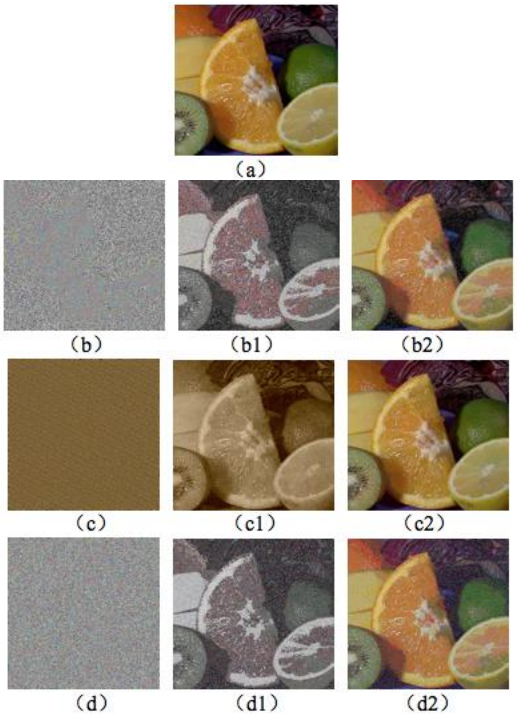

Figure 4. Anti-compression performances of three different encryption algorithms for color image

Figure 5(a) is gray image of Figure 4(a). Other experimental steps are same as Figure 4. From Figure 4 and Figure 5, we can see that to color images if the compression degree is very high (such as compression quality of 10), much color is lost by ART decryption algorithm. Moreover, as the compression quality improvement, decryption image of ART algorithm is more similar to the original image. Its effects are better than the other two compared algorithms. But to gray image, there seems no obvious difference of decryption images of these three algorithms. The reason is that there is only brightness information instead of color information. Therefore, the difference is not as obvious as color images.

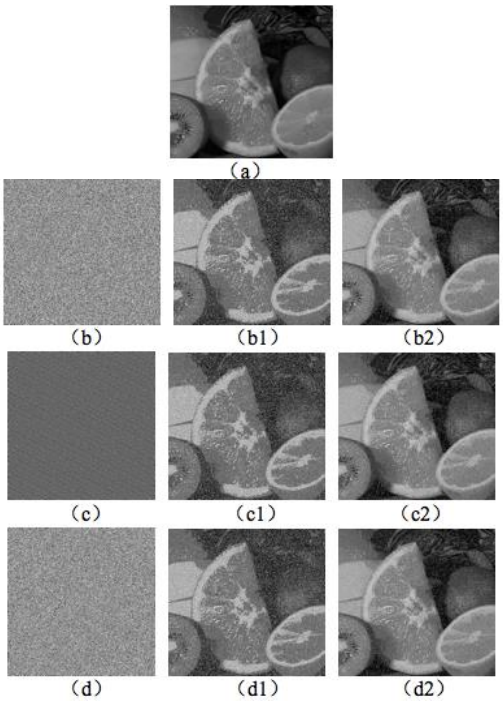

Figure 5. Anti-compression performances of three different encryption algorithms for gray image

The following table presents data comparison results between original image and decryption images of these three algorithms shown in Figure 4 and Figure 5.

Table 1. Comparison of the three algorithms difference ratio

Comparison			Number of same pixels	Number of slight different pixels	Number of great different pixels	Numbers of all pixels	Differenc ratio
Color image (Figure 4)	Gravitation model [9]	b1	2	34634	211124	245760	85.9065%
		b2	8	130267	115485	245760	46.9909%
	ART[4]	c1	1	66772	178987	245760	72.8299%
		c2	16	205003	40741	245760	16.5775%
	Proposed scheme	d1	0	23533	222227	245760	90.4243%
		d2	14	117935	127811	245760	52.0064%
Gray image (Figure 5)	Gravitation model [9]	b1	6200	91559	148001	245760	60.2217%
		b2	20411	165679	59670	245760	24.2797%
	ART[4]	c1	5469	103914	136377	245760	55.4919%
		c2	19248	213384	13128	245760	5.3417%
	Proposed scheme	d1	6206	91700	147854	245760	60.1619%
		d2	20247	165556	59957	245760	24.3965%

From Table 1 we can clearly see that the anti-compression recovery capability of the three algorithms. Compared to gray images, our proposed scheme shows more obvious effect on color images. To high level compression of 60, ratio of slight different pixels was improved by 9.47% to Gravitation model, and 42.47% to ART. At the same time, ratio of great different pixels was changed from 9.64% to 68.12%. Furthermore, we may draw the following two conclusions. Anti-compression performance of encryption algorithm based on pure position information will be better than algorithm based on gray level information and anti-compression performance for gray image will be better than color image of the proposed hybrid encryption scheme.

5. Conclusion

In this paper, we proposed an image encryption and decryption algorithm based on Arnold transform and gravitation model transformation. Arnold transform is improved to process image with size M*N, and its encryption and decryption iterations are also improved to gain good security. Hybrid encryption scheme mainly uses image's spatial and gray level information. Experiments show that the proposed method's characteristics are better as compared to some single encryption algorithms.

Acknowledgements

This work was supported by Jiangsu Provincial Department of Education and the National Nature Science Foundation of China (No. 61375001).

References

[1] Shi Liu, Changliang Guo, John T Sheridan. A review of optical image encryption techniques. *Optics & Laser Technology*. 2013: 327-342.
[2] Y Zhong. Plaintext related image encryption scheme using chaotic map. *Telkomnika indonesian journal of electrical engineering*. 2014; 12 (1): 635-643.
[3] Y Zhong, J Xia, P Cai, et al. Plaintext related two-level secret key image encryption scheme. *Telkomnika Indonesian journal of electrical engineering*. 2012; 10 (6): 1254-1262.
[4] VI Arnold, A Avez. Ergodic Problems in Classical Mechanics. New York: Benjamin. 1968.
[5] N Jiang, W Wu, L Wang. The quantum realization of Arnold and Fibonacci image scrambling. *Quantum Inf Process*. 2014; 3: 1223-1236.
[6] M Deng, Q Zeng, X Zhou. *Robust Image Watermarking Against Shearing Based on Hilbert-Huang Transformation*. 2010, 2nd International Conference of Information Engineering and Computer Science (ICIECS). WuHan, China. 2010.
[7] He Li M, Qiang SL. Novel image scrambling algorithm based on changing pixel values. *Application research of computers*. 2012; 29(12): 4635-4650.
[8] Chuan-Kuei Huang, Hsiau-Hsian Nien, Shih-Kuen Changchien, Hong-Wei Shieh. Image encryption with chaotic random codes by grey relational grade and Taguchi method. *Optics Communications*. 2007; 280(2): 300-310.
[9] Sun Yufeng, Chen Jianhua. A new image scrambling method based on gravitation model. *Journal of Fuzhou University*. 2006; 34(1): 47-50.
[10] Osama AK, Abdullah MZ. An efficient adaptive of transparent spatial digital image encryption. *Procedia technology*. 2013; 47: 152-158.
[11] Mazleena S, Subariah L, Ismail FI. Image encryption algorithm based on chaotic mapping. *Jurnal Teknologi*. 2003: 1-12.
[12] Muhammad RA. Securing color information using Arnold transform in gyrator transform domain. *Optics and Lasers in engineering*. 2012; 50: 772-779.
[13] Wang Qingsong, Fan Tiesheng. Chaotic image scrambling algorithm based on location and gray transformation. *Journal of chinese computer systems*. 2012; 33(6) 1284-1287.
[14] Seyed MS, Benyamin N, Sattar M. RGB color image encryption based on hoquet fuzzy integral. *Journal of Systems and Software*. 2014; 97: 128-139.
[15] Zhou NR, Zhang AD, Zheng F, Gong LH. Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing. *Optic& Laser Technology*. 2014; 62: 152-160.