RESEARCH ON COLOUR IMAGE ENCRYPTION EFFICIENCY

PENG Jing-yu

Department of Electronic Information, College of Applied Technique, Soochow University, Suzhou, Jiangsu 215325, China
kymiao@163.com

Keywords: colour image, encryption efficiency, Arnold transform, scrambling degree, encryption effect

Abstract

In order to improve the efficiency of color image encryption, the encryption scheme based on Arnold transformation is analyzed about the encryption effect and encryption efficiency. The shortage of traditional method is pointed out, and the improved encryption scheme is proposed in this paper. The physical locations of pixels are scrambled and mapped to different colour spaces during the encryption process. A kind of inverter conversion algorithm for colour image is put forward in decryption process. Decryption time only depend on the encryption key instead of relying on the conversion cycle. Simulation results show that the algorithm could not only improve encryption efficiency, but also make a very good encryption effect. Furthermore, this algorithm is a simple, feasible colour image encryption method.

1 Introduction

As for colour image is one of the main components of multimedia data, it is necessary to encrypt reliably in order to ensure the security during transmission. Thus, colour image encryption technology has become an important research direction in the field of information security nowadays. Recently, there are many methods of colour image encryption. In literatures [1] and [2], an image encryption technology is proposed based on chaos theory. And an encryption technology based on linear transformation is presented in reference [3]. In their way, the essence is to scramble the positions or the grey levels of the image pixels, so the original image can not be identified in the visual and statistical characteristics. The colour image data is three-dimensional.

In comparison with other text data, it has not only large data information, but also high correlation. Therefore, in the encryption process, it must be considered to change the subjective visual effect and correlation between objective data. Moreover, there are computationally expensive task of recalculating and much time-consuming. To encrypt the transmission colour image requires a real-time, so it is particularly important to research encryption efficiency. A parallel encryption model to improve encryption efficiency is presented in [4]. In [5], an efficient adaptive colour image encryption algorithm is proposed. Unfortunately, the above algorithms are not a detailed theoretical and experimental analysis of the encryption efficiency. In this paper, encryption efficiency for colour image is analyzed detailedly, and a simple, efficient colour image encryption and decryption scheme based on Arnold transform is proposed. Then the experiments were analyzed on the subjective visual effect, the objective statistical effect and the time of encryption and decryption.

The structure of the paper is organized as follows. Encryption efficiency based on the Arnold transform is described in section 2. Section 3 introduces the proposed algorithm. Experiments are given in section 4. Finally, the conclusions are summarized in section 5.

2 Encryption efficiency and effect based on the Arnold transform

2.1 First encryption algorithm

Applying the formula of Arnold transformation into color image encryption, the pixels' gray levels of the RGB components at the coordinates (x, y) can be mapped to the coordinates (x', y') as equation (1)(2).

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

$$w_{xy}(r,g,b) = w_{x'y'}(r,g,b) \qquad (2)$$

Where (x, y) $\in$ {0,1, 2, …, N } are coordinate values of the pixels before transformation, and (x', y') $\in$ {0,1, 2, …, N } are the new coordinate values after transformation. N is the order of a digital image matrix. $w_{xy}(r, g, b) \in \{0,1,2,\ldots,255\}$ are gray levels of pixels in coordinate (x, y) before transformation, and $w_{x'y'}(r, g, b) \in \{0,1,2,\ldots,255\}$ are the ones after transformation. The essence of this encryption is to moving the pixels' locations so that the pixels in the original image are scrambled and encrypted.

Each pixel will return to its original position after a certain period T based on the periodicity of Arnold transformation. Thus, the iterative times could be as a key. Assuming that the image is encrypted after t transformation times by equation (1), the decryption process is to transform T - t times by equation (1).It can be proved that the period has a relationship with image size.

Figure 1 shows the relationship between period and image size.

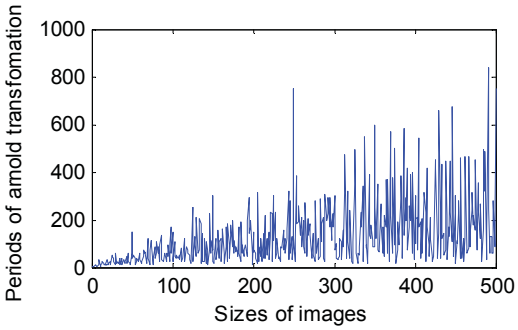

Figure 1. Relationship between period and image size

As shown in Figure 1, the trend of the transformation periods is larger with the increasing of the image size, but it is not a linear change. There are some different transformation periods for images with different size in Table 1. It shows that there is no linear relationship between the size of image and the period of transformation. Therefore, the total time of encryption and decryption is related to the size of images and not concerned in the encryption effect. So the encryption efficiency is dependent on the image size and can not be improved.

N	period	N	period	N	period
2	3	80	60	325	350
19	9	90	60	444	228
53	54	130	210	478	357
70	120	189	72	495	60

Table 1. Different size of image correspond to transformation period

2.2 Second encryption algorithm

For color image, there is another method to scramble the color by changing the gray level of each pixel's RGB components. According to the 3D equal-length Arnold transformation, the three color components (r, g, b) can be mapped to another components (r', g', b') as equation (3):

$$\begin{bmatrix} r' \\ g' \\ b' \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} r \\ g \\ b \end{bmatrix} (\mathrm{mod}\ 256) \qquad (3)$$

In equation (3), we assume the max value of RGB pixels is 255, and the transformation period is 448.

Then the pixels' gray levels in image W can be changed as equation (4):

$$\begin{cases} W(r) = W(r') \\ W(g) = W(g') \\ W(b) = W(b') \end{cases} \qquad (4)$$

In equation (4), W is color image whose sampled data is a 3D matrix. W(R),W(g),W(b) stand for the RGB components of matrix W. They are 2D matrixes.

In the experiments, we find that the method for a relatively small number of images, such as the watermark image, is computationally expensive task of recalculating, and low efficiency.

2.3 Analysis of the encryption effect and efficiency

An image with the size of 80 by 80 is encrypted with the same iterative times by the first method and the second method. Figure 2 shows the result of the above algorithm.

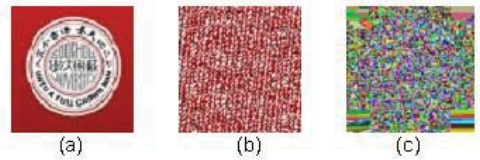

Figure 2. Result of the above algorithm

(a)Original image; (b) Image encrypted by first algorithm; (c) Image encrypted by second algorithm

As shown in Figure 2 (b), encryption effect in visual subjective evaluation is comparatively good because of directly altering the physical location of each pixel. In Figure 2 (c), if the color in an area is same, the contour is still visible after scrambling, because the gray levels of pixels are changed by second algorithm. So the encryption effect in subjective visual evaluation is not ideal.

However, by analysis the encrypted statistical effect, we find the first algorithm is unable to change the image statistical characteristics. As Figure 3 shows, the histogram of red component before and after encryption is the same. On the contrary, the second algorithm can change the image statistical characteristics, and make the image pixel values uniform distribution in the entire value space. In Figure 3, X axis stands for the red component gray value, Y axis is the number of pixel points of the image.

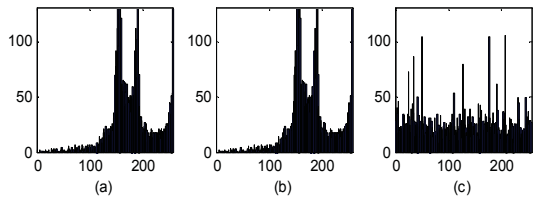

Figure 3. Statistical effect before and after encryption

(a)Statistical characteristic of original image; (b) Statistical characteristic of the image encrypted by first algorithm; (c) Statistical characteristic of the image encrypted by second algorithm

Scrambling degree presented in literature [6] will be used to evaluate the encryption effect objectively. Moreover, scrambling time will be measured. Table 2 shows the result. When the iteration time is the same, the encryption time is substantially equal. However, the second encryption algorithm encryption effect is better than the first one at the same time. If using the Arnold transformation periodicity to decrypt, when N is 80 in Table 1, the transform period is 60, and the consumptions of encryption and decryption are required for 60 iterations. According to equation (3), the transform period is 448, and about 7 times iterations time will be waster.

Iteration time	First algorithm		Second algorithm	
	time(s)	scrambling degree	time(s)	scrambling degree
7	0.0780	0.1090	0.0780	0.1311
21	0.1560	0.1100	0.1400	0.1290
42	0.3130	0.1061	0.3130	0.1280
56	0.4060	0.1070	0.4060	0.1255

Table 2. Relationship between the time of encryption and scrambling degree

Experiments show that the above two methods in encryption effect cannot balance the subjective evaluation and objective statistical effect. And the encryption efficiency is determined by the image itself, and cannot to achieve the purpose of increasing efficiency.

In fact, the research indicates that the Arnold scrambling time and effect is not a linear relationship. In experiment, three images with the resolutions of 90 by 90, 130 by 130 and 280 by 280 are choose to be scrambled using different number of iterations. As Table 1 shows, the period of three images is 60, 210, and 120.

Figure 4 depicts the relationship between the scrambling degree and the time of iterations. We can find that the relationship between the time of iterations and the scrambling effect have a certain periodicity, but not have a linear relationship. Moreover, even in a period, it is untenable that when the time of scrambling is long, the scrambling degree is large. Thus, avoid to use the time when scrambling degree is low, the better effect could be reach. If the time of decryption don't rely on period, it is possible to speed up decryption and improve encryption efficiency.

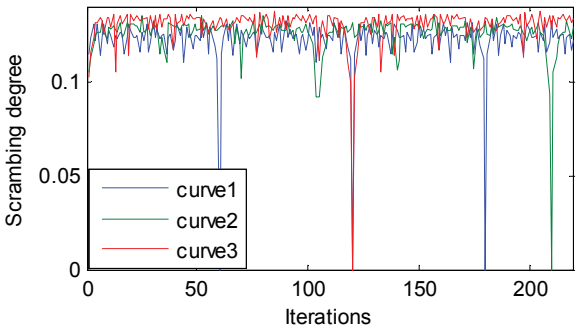

Figure 4. Scrambling degree with iterations

Curve 1 is for the image with 90×90 pixels; Curve 2 is for the image with 130×130 pixels; Curve 3 is for the image with 280×280 pixels.

A new encryption and decryption algorithm is proposed based on Arnold transformation. It do not rely on the transformation period, and improve the encryption efficiency while meliorate the encryption effect.

3 Proposed encryption algorithm

3.1 Encryption method

W is a 3D matrix of color image. $W_r(x, y)$, $w_g(x, y)$, and $w_b(x, y)$ stand for RGB values of coordinate (x, y) respectively. While coordinate (x, y) changes, the gray level of this pixel's primary color (r, g, b) will be mapped to another color space(r', g', b'). The $w_r(x, y)$, $w_g(x, y)$, and $w_b(x, y)$ are represented as equation (5).

$$\begin{cases} w_r(x,y) = w_{r'}(x',y') \\ w_g(x,y) = w_{g'}(x',y') \\ w_b(x,y) = w_{b'}(x',y') \end{cases} \quad (5)$$

In equation (5), coordinate (x, y) and coordinate (x', y') will be calculated as equation (1). Gray level (r, g, b) will be mapped to another color space (r', g', b') as equation (3).

In equation (1), the transform period is related to the size of image, and marked T1. According to formula (3), the transform period is related to color quantization level, marked T2. When using the transform period to decrypt, the consumption time will be (T1-t)*(T2-t). The proposed method will decrypt not depend on the transform period. And the time of decryption is decided by encryption time.

3.2 Decryption method

Decryption process uses inverse Arnold transform. Theoretically, the inverse formula of equation (1) is as equation (6):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ N) \quad (6)$$

Considering image pixels coordinates can not be negative value, the improved formula is calculated by equation (7) to return the pixels to original coordinate positions:

$$\begin{cases} x' = |2x - y| \bmod N \\ y' = |y - x| \bmod N \end{cases} \quad (7)$$

Similarly, the inverse formula of equation (3) is as equation (8):

$$\begin{bmatrix} r' \\ g' \\ b' \end{bmatrix} = \begin{bmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{bmatrix} \begin{bmatrix} r \\ g \\ b \end{bmatrix} (\mathrm{mod}\, 256) \quad (8)$$

Considering image pixels gray levels can not be negative, the color is recovery by equation (9):

$$\begin{cases} r' = |2r - g| \bmod 256 \\ g' = |-r + 2g - b| \bmod 256 \\ b' = |b - g| \bmod 256 \end{cases} \quad (9)$$

When t times transform is carried out by equation (5) to encrypt an image, the decrypted image will be obtained also after t times transform by equation (5). Note that (x, y) and (x', y') should be exchanged by using formula (7), and (r, g, b) should be mapped to (r', g', b') by using formula (9).

4 Simulation and analysis

In the experiments, some different sizes of JPG images are used to evaluate the algorithms. The proposed algorithm is compared with the above two methods. These algorithms

are simulated using Matlab 7.0, and experiments are carried out on a computer with 2.8-GHz Intel Celeron D Processor Unit and 1-GB random access memory.

4.1 Encrypted effect

4.1.1 The subjective effect of encryption

After iterating same times by three algorithms, the subjective effect of encryption can be obtained as Figure 5. Although many experiments have been done to different images, the results are same. Figure 5 only shows the results of images whose resolution is 130 by 130. They are iterated 8 times by three algorithms. The experiments show that the subjective encryption effect of proposed algorithm is better than other two methods.

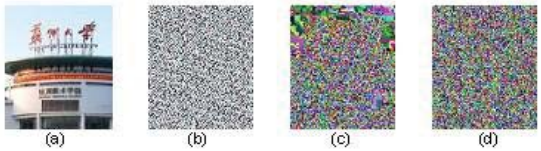

Figure 5. Images before and after encryption

(a)Original image; (b) Image encrypted by first algorithm; (c) Image encrypted by second algorithm; (d) Image encrypted by third algorithm;

4.1.2 Statistical characteristics

Figure 3 shows the result of the above two algorithms. The statistical characteristics of the images encrypted by proposed method will be calculated in this experiment. As the red component histogram shows in Figure 6, the new method can completely change the original image's statistical characteristics, and make the image pixel values uniform distribute in the entire value space.

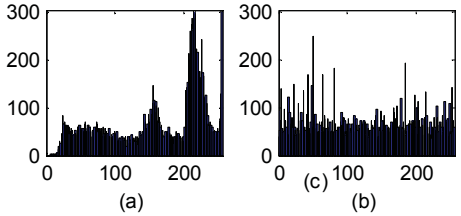

Figure 6. Statistical characteristic of original image and encrypted image

(a) Statistical characteristic of original image; (b) Statistical characteristic of the image encrypted by third algorithm;

4.2 Encryption efficiency and effect

4.2.1 Encryption time and encryption effect

Scrambling degree is used to evaluate the effect of encryption image. Figure 7 shows the relationship between encryption time and scrambling degree. It can be see that the scrambling degree of proposed method is far greater than other methods. Moreover, the proposed method uses the minimum time to reach larger scrambling degree and maintains a stable scrambling state. Other methods could not only make a small scrambling degree, but also show different volatility with encryption time.

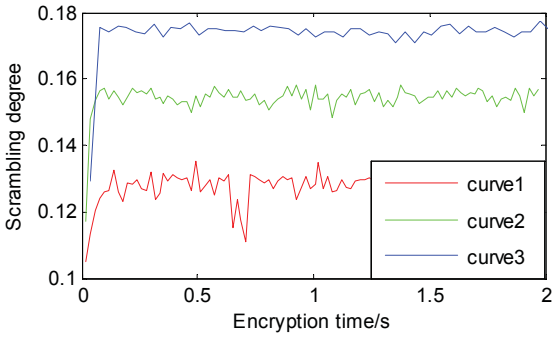

Figure 7. Relation between encryption time and scrambling degree

Curve 1 is the relation between encryption time and scrambling degree which is encrypted by first algorithm; Curve 2 is by the second algorithm and curve 3 is by the proposed algorithm.

4.2.2 Consumption time of encryption and decryption

In the experiments, consumption times of encryption and decryption for four different sizes of images are calculated. Table 3 shows the result.

Size of images	First algorithm(s)	Second algorithm(s)	Proposed algorithm(s)
80*80	0.4070	3.7340	0.3750
90*90	0.5000	4.8440	0.3280
130*130	1.0470	10.1710	0.7030
280*280	5.2340	48.5470	4.0780

Table 3. Consumption times of encryption and decryption in four different sizes of images

The results show, for different images, the proposed method consumes minimum time encrypting and decrypting. The advantages of new algorithm will be more conspicuous when the size of image is bigger.

5 Conclusions

The encryption effects whether it is judged by subjective visual or objective statistical characteristics show that the proposed encryption method for color image is better than the other two methods. The other two decryption processes depended on the period of transformation .So it can not improve the efficiency of operation. The advanced decryption process uses an inverse transformation for color image and overcomes above-mentioned weakness. Moreover, the simulation results also show, when the size of images is bigger, there is an obviously advantage to reduce the time of encryption and decryption by using our method.

References

[1] LI Shanshan, ZHAO Yinghai, "Image Scrambling Based on Chaos Theory and Vigenère Cipher", USA, IEEE Computer Society, 2011, pp. 555-558.

[2] Linhua Zhang, Xiaofeng Liao, Xuebing Wang , "An image encryption approach based on chaotic maps", Chaos,Solitons and Fractals, 2005, 24, pp.759- 765.

[3] A.A. RAVANKAR, S.G.SEDUKHIN, “Image Scrambling based on a New Linear Transform”, USA, IEEE, 2011, pp.3105-3108.
[4] Zhou Qing, Wong Kwok-wo, Liao Xiaofeng, et al, “Parallel Image Encryption Algorithm Based on Discretized Chaotic Map”, Chaos,Solitons and Fractals, 2008, 38, (4), pp.1081-1092.
[5] LI Li, LIAO Xiao-feng, ZHOU Qing, et al, “Efficient Self-adaptive Color Image Encryption Algorithm”, Computer Engineering, 2010, 36, (14), pp. 120-121.
[6] ZHANG Jian, YU Xiao-yang, REN Hong-e, et al, “Evaluation method of image scrambling degree”. Computer Engineering and Applications, 2007, 43, (8), pp. 134-136.