Arnold Transform Based Image Scrambling Method

Min Li[1] Ting Liang[2] Yu-jie He[3]

Abstract. With the development of information security, the traditional image encryption algorithm has been far from to ensuring the security of images in the transmission process. This paper presents a new image encryption algorithm, which can improve the security of image during transmission more effectively. The traditional scrambling algorithm based on Arnold transformation only applies to the square area, which is a big limitation. Focus on this, a multi-region algorithm for image scrambling encryption model is proposed, which splits the non-square image to multiple square regions, and scrambles each region. Experimental results show that the new algorithm improves the image security effectively to avoid deciphering, and it also can restore the image as same as the original image almost, which reaches to the purposes of image safe and reliable transmission.

Keywords: Arnold transform. image encryption • image scrambling • multi-regional • scrambling degree.

1 Introduction

Digital image scrambling can make an image into a completely different meaningless image during transformation, and it is a preprocessing during hiding information of the digital image, which also known as information disguise. Image scrambling technology depends on data hiding technology which provides non-password security algorithm for information hiding. Data hiding technology led to a revolution in the warfare of network information, because it brought a series of new combat algorithms, and a lot of countries pay a lot of attentions on this area. Network information warfare is an important part of information warfare, and its core idea is to use public network for confidential data transmission. The image after scrambling encryption algorithms is chaotic, so attacker cannot decipher it.

Some improved digital watermarking technology can apply scrambling method to change the distribution of the error bit in the image to improve the robustness of digital watermarking technology. Arnold scrambling algorithm has the feature of simplicity and periodicity, so it is used widely in the digital watermarking technology[1] (Arnold transform is proposed by V. I. Arnold in the research of ergodic theory, it is also called catmapping, and then it is applied to digital image). According to the periodicity of Arnold scrambling, the original image can be restored after several cycles. Because the periodicity of Arnold scrambling depends on the image size, it has to wait for a long time to restore an image. Generally, the cycle of Arnold transformation is not directly proportional to the image degree[2].

Currently, Arnold scrambling algorithm is base on square digital image in most literature, and these images are mostly $N\times N$ pixels of the digital image. However, most of the digital images are non-square in the real world, so that we cannot use Arnold scrambling algorithm widely[3]. To improve the Arnold scrambling algorithm, we will improve the original Arnold scrambling algorithm, so that we can apply Arnold scrambling algorithm to $M\times N$ non-square pixel digital image, it means the length and width of the image is not equal[4] .

[1]Min Li(✉)
Xi’an Research Inst.of Hi-Tech, 710025, Shaanxi Province, P. R. C
e-mail: clwn@163.com

[2]Ting Liang
Xi’an Research Inst.of Hi-Tech, 710025, Shaanxi Province, P. R. C

[3]Yu-jie He
Xi’an Research Inst.of Hi-Tech, 710025, Shaanxi Province, P. R. C

This work was supported by the National Natural Science Foundation of China under Grant No. 61102170.

2 Image Scrambling Based Arnold Transformation

2.1 Arnold Scrambling Algorithm

As shown in Fig.1 [5], the transformation of point (x, y) in the unit square change to another point (X ', Y ') is:

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} (\mathrm{mod}\ 1) \tag{1}$$

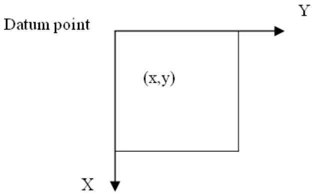


Fig. 1. Distribution of image coordinates.

Table 1. Arnold scrambling algorithm cycle

Size of image(N)	Cycle of scramblin(T)	Size of image(N)	Cycle of scrambling (T)
3	4	25	50
4	3	32	24
5	10	64	49
6	12	100	150
7	8	120	60

This transformation is called two-dimensional Arnold scrambling. To be specific to the digital image, we need to change the two-dimensional Arnold scrambling of mod 1 to:

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} (\mathrm{mod}\, N) \tag{2}$$

It is mod2 which is Arnold scrambling. For $x, y \in \{0,1,2,3,\cdots,N-1\}$, N is the order of digital image matrix. The transformation of mod2 is matrix A. $(x, y)^{\mathrm{T}}$ in the right is the input, $(x', y')^{\mathrm{T}}$ in the left is the output, considering the feedback, iterative process which can do as the following:

$$\begin{aligned} P_{xy}^{n+1} &= AP_{xy}^{n} (\mathrm{mod}\, N) \\ P_{xy}^{n} &= \quad (x, y)^{T} \end{aligned} \tag{3}$$

where: n representative of the time of iterations, n = 0, 1, 2.... Image information (such as the gray value) with the replacement of the discrete lattice for transplantation, they generated a new image after all of the points of the original image have been traversed. In addition to simple, easy to come true, Arnold scrambling also has the character of cycle, brief description is given below[6, 7].

2.2 Arnold Transform Based Digital Image Scrambling

The digital image can be seen as a two-dimensional matrix. When the size of the image is N, then I have $N \times N$ elements, the subscript x, y stand for the position of pixel, x, $y \in \{0, 1, 2..., N\text{-}1\}$. Let x, y corresponds to the x, y of Arnold scrambling, for each pair x, y, after all do Arnold scrambling, become x' and y', which equivalent to the original image of the point from (x, y) move to the = (x ', y'), so realized the movement of pixels in the image, the image with Arnold scrambling traverse all the points to complete a picture of Arnold scrambling.

The cycle of Arnold scrambling is relate to the size of the image, but not directly proportional. If size is 128 × 128 pixel image of Arnold scrambling cycle is 96, size 240 × 240 pixel image of Arnold scrambling for 60 cycles. Table 1 shows the relationship between different *N* values and the cycle *T* of Arnold scrambling.

2.3 Scrambling Recovery in Arnold Scrambling Algorithm

Arnold scrambling recovery has two ways: one is the application of its periodicity, and the other is the pursuit of its inverse matrix to the inverse transformation [8]. It is very natural to leverage the periodicity of Arnold scrambling method. By research of it before, we can come to this conclusion: For the digital image of *N* × *N* pixels, as long as meet non-1 positive integer *N*, The Arnold scrambling has periodicity. Extend to an arbitrary Scrambling time of n, you need to proceed (m^{N-n} mod m^{N}) times Arnold scrambling transformation. However, the times of scrambling are relate to the order of *N*, in general, if *N* is the number of higher-order cases, the cycle is relatively long.

3 Improved Arnold Algorithm Model

3.1 Basic Principle to Improve the Arnold Scrambling Algorithm

Select a non-square *L* × *L* pixels area in a digital image, doing the Arnold transformation, in order to achieve parts of the region scrambling. Fig. 2 shows the idea of using improved Arnold scrambling algorithm for image scrambling in the single region:

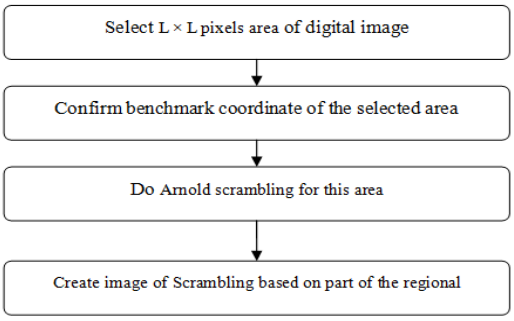

Select L × L pixels area of digital image
Confirm benchmark coordinate of the selected area
Do Arnold scrambling for this area
Create image of Scrambling based on part of the regional

Fig. 2. Flow of digital image scrambling based on part of the regional.

The idea of parts of region scrambling: the selection of the most upper left pixel coordinates (x_1, y_1) is set to (1, 1), after this period of transformation coordinates (X-(x_1-1), Y - (y_1-1)), then the original formula (1), (2) change to formula (4), (5):

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X-(x_1-1) \\ Y-(y_1-1) \end{bmatrix} (\bmod 1) \tag{4}$$

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X-(x_1-1) \\ Y-(y_1-1) \end{bmatrix} (\bmod N) \tag{5}$$

The (x_1, y_1) of above formulas is an arbitrary choice of the square image in the upper left corner coordinates of the region, $x, y \in \{0,1,2,\cdots,N-1\}$, and *N* is the order of digital image matrix.

Compare a few selected areas in the non-square of the same size, the only change is the coordinates of reference point, and the operation principle is as same as Arnold algorithm. So, Arnold scrambling algorithm is still available.

3.2 Scrambling Degree Theory

According to the concept of the scrambling transformation, the scrambling of position space is the original image pixel position has been moved essentially, If the pixel has been moved farther away comparing to the original image pixels, the degree of scrambling is higher. While scrambling does not change the original image pixel gray level, but can change the image of the visual effects. Scrambling the image compare to the original image more "chaos ", indicating that the scrambling algorithm is more effective. A more "chaos" image should be intuitive visual was "chaotic", and the overall distribution of relatively uniform gray image. According to the analysis above, the degree of image scrambling is not only considering the distance to move the image pixels, but also considering the intuitive visual effect of image. Using the formula of Ds below can objectively shows the image scrambling degree [9].

$$Ds = DSF \times GSF \tag{6}$$

DSF (distance scrambling factor) is determined by the distance of the pixel movement, GSF (gray scrambling factor) is calculated by quantifying the intuitive visual data.

In general, the image pixel position to move the more further away, the greater the degree of scrambling is, so it can be used to represent the scrambling degree by moving distance. Move away from here by pixel to calculate the mean and variance of DSF.

Definition 1: Assumes that the image $A_{M\times N}$ scrambled into the image $A'_{M\times N}$, a pixel position (x, y) is mapped to scrambled images $(x ', y')$ position, then the move distance of pixels is:

$$d(x,y) = \sqrt{(x-x')^2 + (y-y')^2} \tag{7}$$

The mean moves distance of whole image is:

$$E(d) = \frac{1}{M\times N}\sum_{x=1}^{M}\sum_{y=1}^{N} d(x,y) \tag{8}$$

Obviously, when each pixel in the image does not move, it means when the image does not scrambling, E (d) is the minimum value $E_{\min}$ (d) = 0; when the image of each pixel move diagonal distance, E (d) is Max.

$$E_{\max}(d) = \sqrt{(M-1)^2 + (N-1)^2} \tag{9}$$

The distance of pixel scrambled moved higher means that the degree of movement is greater. Therefore, DSF can be calculated by

$$DSF(A, A') = E(d) / E_{\max}(d) \tag{10}$$

According to the previous analysis that if the image is divided into the same size and do not re-place sub-block, then scrambling the image average gray level of each sub-block closer to the image "chaos " the greater the degree. As a result, the following method can be used to calculate GSF.

Divied Scrambling image and original image into $k \times k$ pixels in size and do not overlap sub-block, set sub-image $B_{m\times n}(i, j)$ stand for the image of the (m, n) sub-blocks, then the sub-image $B_{m\times n}(i, j)$ of gray level $E(B_{m\times n})$ is:

$$E(B_{m\times n}) = \frac{1}{k\times k}\sum_{i=1}^{k}\sum_{j=1}^{k} B_{m\times n}(i,j) \tag{11}$$

There are $(M/k)\times(N/k)$ sub-block after block of the image, such as mean and variance of equation gray showed below by formula (12) (13).

$$E(E(B'_{m\times n})) = \frac{1}{(M/k)\times(N\times k)}\sum_{m=1}^{M/k}\sum_{n=1}^{N/k} E(B'_{m\times n}) \tag{12}$$

$$\sigma^2 = \frac{1}{(M/k)\times(N/k)}\sum_{m=1}^{M/k}\sum_{n=1}^{N/k}(E(B'_{m\times n}) - E(E(B'_{m\times n})))^2 \tag{13}$$

Described as a random variable variance relative to the mean wave, if the variance is smaller, the wave degree is smaller, the variance is larger, and the wave degree is larger. Therefore, the gray level sub-image can be used to describe the variance of degree of image scrambling. If the variance is smaller, the difference between the average gray code between is smaller, is means the degree of "chaos" is higher.

If the sub-scrambling image means gray level variance is σ_{new}^2, the original image of the sub-image intensity mean and variance is σ_{org}^2, then the value of intuitive visual GSF is:

$$GSF = \frac{\sigma_{org}^2}{\sigma_{new}^2} \tag{14}$$

According to the equation above, the more GSF larger, the image more "chaos" , which compare to the original image, and the scrambling better.

The value of scrambling degree Ds is also related to the image block. Image sub-block can not be too small or too large, for example, when sub-block size is 4 × 4 pixels, a few values as about 10^{-2}, sub-block is 8 × 8 pixels for the 10^{-1} of magnitude, Because the degree of image scrambling only related to the size of Ds value, it does not depend on the number of class of Ds value. As long as the specific application image of sub-blocks in the same size, we can always use the Ds value to stand for the chaos of image, which used for evaluating the scrambling method.

4 Experiment and Analysis

In Matlab 7.1, on a single image of the different areas doing the Arnold scrambling, as shown in Fig.3. The two regions or more regions of the replacement are similar to the replacement of a region.

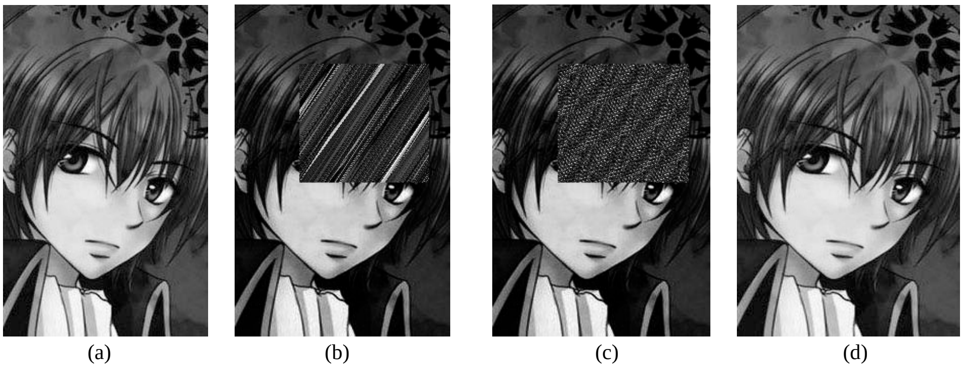


Fig. 3. Image scrambling effect of different times in single region: (a) Single area of the original image, (b) scrambling 2 times of the original image, (c) Scrambling 68 times of single region, and (d) scrambling 96 times of single region.

After the scrambling of a region above, all images will be scrambling if a number of different areas of the image part of the regional scrambling, so that this image has a higher degree of scrambling, and a higher security. Scrambling process is the physical location of pixel changes in selected regions can overlap.

Image scrambling: the image is segmented into equal number of non-square regions, each region do different times of Arnold scrambling.

This picture shows the 564 × 642 pixel image, for the maximum square area 564 × 564 pixels, the first maximize area is to the left which is 564 × 564 pixel region, the second maximize area is to the right-hand which is the 564 × 564 pixel region . This totally was divided into six regions, as shown in Fig. 4.

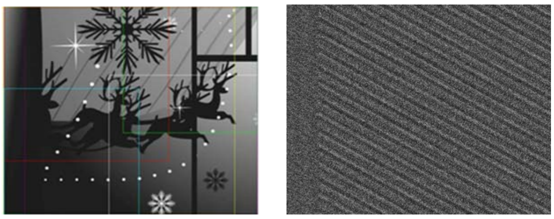


Fig. 4. Adds two maximize regions of the regional distribution: (a) 564×642 pixel non-square image into six different regions and (b) multi-region scrambling effects. (The size of divided image: Red line: 396*396; Green line: 342*342;

Blue line: 342*342; White line: 360*360; Yellow line: 564*564; Brown line: 564*564)

By scrambling a single image multiple regions, from the subjective point of view, there is no boundary in the image, we also cannot find the boundary inside. This reached the purpose to get rid of attacker.

5 Attacking Experiment and Analysis

In order to verify if there was data loss during transmission of the encrypted image when attacked, make the following two attacking experiment.

5.1 Part of the Regional Shear Experiment

Shear processing for part of the scrambling images regional by Photoshop CS4.0, as shown in Fig. 5. The images restored through a recovery process as shown in Fig. 6.

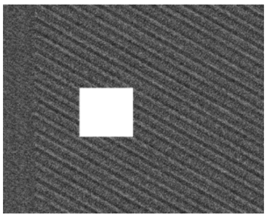
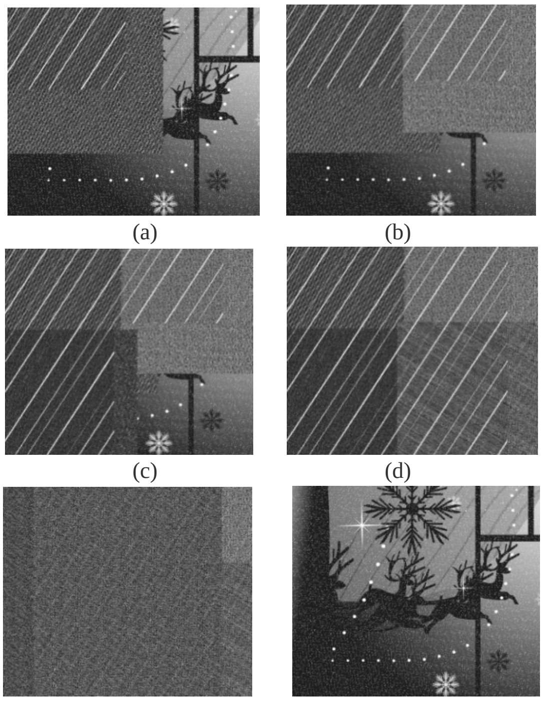


Fig. 5. Part of the shear image areas after scrambling



(a) (b)

(c) (d)

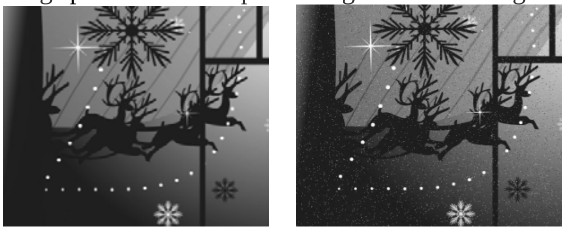
(e) (f)

Fig. 6. the restore image after shear of Part of the region: (a) restore a region of the image, (b) restore two regions of the image, (c) restore three regions of the image, (d) restore four regions of the image, (e) restore five regions of the image, and (f) restore all regions of the image.

Through the attacking experiment of Part of the shear image area, although the image through some of the processing area shear, after image restoration, the resulting image similar to the original image.

5.2 Adding Noise Experiment

The original image adding spiced salt noise processing is shown in Fig. 7.



(a) (b)

Fig.7. the original image and the image of adding noise:
(a) the original image and (b) the image of adding noise.

Using Matlab7.1 software processing adding salt and pepper noise on the image after the scrambling, and restore as the following image.

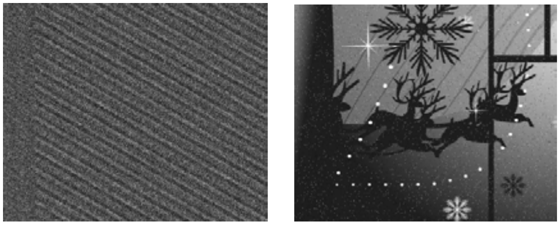


Fig. 8. Adding noise and restore to the image after scrambling:
(a) the image of adding noise and (b) the restore image.

Conclusion of the noise attacking experiment: when the digital scrambling image attacked by the noise, the restore image, compared to the original image, they are almost the same. Illustrate this scrambling algorithm is relatively weak in anti-noise attack.

Conclusion of the two attacking experiments above: Arnold scrambling algorithm in some areas shear of image scrambling, after the recovery, can basically restore the initial image. When scrambling image attacked by noise, the restore image is almost the same as the original image after the noise attack, indicating Arnold scrambling algorithm and the noise attack did not influence each other, even if image was attacked, still could use the algorithm for image restoration processing.

6 Conclusions

This paper gives a new image scrambling algorithm, by using image scrambling to encrypt the image to improve the security of image. Compared with the traditional Arnold scrambling algorithm, the proposed multi-area scrambling method in this paper not only can be used for a square image, but for any non-square images. By using multi-region scrambling, it can more effectively improve the security of image, lead decipher even more difficult. It simulates scrambling under Matlab 7.1 to confirm it. Experimental result shows that the improved algorithm is feasible.

References

1. Delaigl E J F, Vleeschouwer C D, Macq B.: Watermarking Algorithm Based On A Human Visual Model. J. Signal Processing. 66(5), 319--336(1998).
2. SWANSON M D, ZU B, TEWF IKA H.: Robust Data Hiding For Images. J. Proc IEEE 7th Digital Signal Processing Workshop (DSP 96). 9, 37--40(1996).
3. Gu-song Hao, Yang Cai, Zhang Haiyu, Liu Xiaoxia.: One Iimproved Arnold Transformation. J. Henan University (Natural Science). 2, (2009).

4. Qi Dongxu, Zou Jianchun, Han Xiaoyou.: A New Class of Scrambling Transformation And Its Application In The Image Information Covering. J. Science In China Scrics., 43 (3), 304--312 (2000).
5. Baraff D, Witk A, Kass M.: Untangling Cloth. J. ACM Transactions On Graphics. 22(3), 862--870(2003).
6. Wang Lulu, Zhang Chong.: Arnold Scrambling Based On Digital Image EncryptionTechnique. J. National Defense Technology Base. 10, (2010).
7. Huang Fangyuan.: Arnold Scrambling Based On Image Scrambling Algorithm And Implementation. J. Gui Zhou University (Natural Science). 25(3), (2008).
8. Wu Lingling, Zhang Jianwei, Ge qi.: Arnold Transformation And Its Inverse Transformation. J. Micro Computer. 14, (2010).
9. Huang Liangyong, Xiao Degui.: The Best Scrambling Degree of Arnold Transformation On Binary Images. J. Computer Applications. 2 (2009)