Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation

LIU Xiangdong[†], Zhang Junxing[†], Zhang Jinhai[††], He Xiqin[††]

[†] The Research Institute of Nonlinear Information Technology, Dalian Nationalities University, Dalian, Liaoning, P. R. China
[††] Faculty of Science, Liaoning University of Science and Technology, Anshan, Liaoning, P. R. China

Summary
This paper proposed a novel image scrambling scheme based on chaos theory and the sorting transformation. The new algorithm calculates the permuting address codes by sorting the chaotic sequence, not like common method by quantizing the chaotic sequence. Therefore, the new scheme does not require knowing the probability density function of the chaotic orbits in advance, thus not only facilitating the choice of chaotic systems but also reducing the complexity of the scheme. The paper also analyzed the scrambling performance of the new algorithm statistically. The results indicate that the new algorithm can provide a high level security owing to the strong irregularity of sorting transformation.

Key words:
Image scrambling, Chaotic Sequence, Sorting Transformation, Threshold quantization.

1. Introduction

Image scrambling is commonly used in image encryption, and is also used in watermarking to make the image statistically undetectable. It is a field that has drawn much attention in the latest years [1,2]. The main aim of image scrambling is to transform a meaningful image into a meaningless or disordered image in order to enhance the power to resist invalid attack and in turn enhance the security [3]. Now, the mainly used three kind of image scrambling types are scrambling in the space domain, scrambling in the frequency domain, and scrambling in the color or grey domain.

In a great quantity of all kind of image scrambling algorithms, the image scrambling algorithms based on chaos have attracted more and more attention since they have sufficient large secret key space and can provide a high level of security [4,5,6,7].

Most of proposed chaotic image scrambling methods are based on the construction of a chaotic sequence of real numbers that is afterwards somehow threshold quantized in order to provide the permuting address codes. To threshold quantize a chaotic sequence requires knowing a lot about the probability distribution of the chaotic orbits, but this is an unsolved difficult problem yet in chaos theory. Moreover, since the permuting address codes have some peculiarities, the algorithm has to experience a lot of iterations that can not generate the permuting address code in order to ergod all addresses, thus arguments the complexity of the algorithmic.

The proposed image scrambling scheme generates the permuting address codes by sorting the chaotic sequence directly, not by threshold quantizing the chaotic sequence. The new scheme does not require having any knowledge of the distribution of the chaotic orbits in advance, so one can select and use an arbitrary chaotic model to generate chaotic sequences, thus expanding the secret key space of the algorithm tremendously. The new algorithm can also decrease iterations greatly, meanwhile, it can provide a high level security owing to the strong irregularity of sorting transformation.

2. Image Scrambling Algorithm Based On Chaos Theory and Sorting Transformation

For a digital gray image I of size $M \times N$ pixels, we can adopt an arbitrary chaotic iteration

$$x_{n+1} = f(x_n), x_i \in A \quad (1)$$

to generate a chaotic sequence of real numbers. The initial value x_1 is associated to the secret key. Then applied the following scheme to scramble and unscramble I.

2.1 Scrambling Algorithm

step1. Give an initial value x_1 that is associated to the secret key. Let $k = 1$.
step2. Iterate N - 1 times with the chaotic iteration (1), get the sequence of real numbers $\{x_1, x_2, \ldots, x_N\}$.
step3. Sort the sequence $\{x_1, x_2, \ldots, x_N\}$ from small to large, get the sorted sequence $\{x'_1, x'_2, \ldots, x'_N\}$.
step4. Calculate the set of scrambling address codes $\{t_1, t_2, \ldots, t_N\}$, where $t_i \in \{1, 2, ..., N\}$. t_i is the new

Manuscript received January 5, 2008
Manuscript revised January 20, 2008

subscript of x_i in the sorted sequence $\{x'_1, x'_2, \ldots, x'_N\}$.

step5. Permute the kth row of the image I with permuting address code $\{t_1, t_2, \ldots, t_N\}$, namely, replace the t_i th column pixel with the ith column pixel for i from 1 to N.

step6. If $k = M$, that is the end. Otherwise, let $x_1 = x_N$, and $k = k+1$. Repeat from step2 to step5.

2.2 Unscrambling Algorithm

For a given initial value x_1, the procedure for the decryption is similar with scrambling, except that step5 should be changed as: replace the ith column pixel with the t_i th column pixel for i from 1 to N.

3. Properties of the Scrambling Algorithm

In this paper, we adopted 1-dimension Logistic mapping

$$x_{n+1} = 1 - 2x_n^2, x \in [-1, 1] \quad (2)$$

to generate the chaotic sequence of real numbers. And we went on our statistical analyzing by Supposing that the size of image I is 256×256 pixels.

3.1 Complexity of the algorithm

For row scrambling algorithms based on quantization, one must divide the interval of chaotic mapping, namely [-1, 1] into 256 continuous subintervals. In order to speed up the quantization, these 256 subintervals must satisfy that the probability of x_n of the chaotic orbits dropping in each subinterval is equal to each other.

As we know that the probability density function of the orbits of Logistic mapping [8,9] is

$$\rho(x) = \frac{1}{\pi\sqrt{1-x^2}}, x \in [-1, 1]. \quad (3)$$

we can calculate the points of partitions according to (3), and get that

$$L_k = -\cos(k\pi / 256), k = 0, 1, 2, \ldots, 256 \quad (4)$$

Randomly choose 50000 initial values, and generate the permuting address codes by quantizing chaotic sequence. Iterations to ergod whole 256 addresses are given in table 1.

Table 1 Iterations to ergod whole 256 addresses with randomly choosing 50000 initial values

Iterations	Maximum	Minimum	Average
	2294	1252	1660.2

According to table 1, we can get that scrambling scheme based on quantization need much iterations to calculate the permuting address codes, and the iterations relate to initial values closely. Furthermore, we also fond by the experiments that along with the number of address code increasing, iterations required to ergod all addresses increase promptly. Therefore, to scramble a large image by the algorithm based on quantization, one has to partition it to sub-images and scrambles them locally, thus reducing the scrambling effect on the entire image. Since multi-valued quantization also requires large amount of comparisons, the scrambling scheme based on sorting transformation is obviously superior to those based on quantization on the complexity. The iterations of the new scheme are much fewer than that of the scheme based on quantization, and does not relate to initial values.

3.2 Fixed points of scrambling

We call it a fixed point of the scrambling scheme if its pixel coordinate does not change after scrambling. The fewer there the fixed points of the scheme are, the more effective the scheme is, and the higher security the scheme provides.

Table 2 Statistical results of proportions the fixed points account for in whole points of proposed row scrambling algorithm with randomly choosing 50000 initial values

Proportion the Fixed points account for in whole points	Maximum	Minimum	Average
	0.45%	0.38%	0.40%

The statistical results of proportions the fixed points account for in whole pints of proposed row scrambling algorithm with randomly choosing 50000 initial values are given in table 2. It can be observed from the table 2 that the fixed points of proposed row scrambling algorithm account for 0.38% ~ 0.45% in whole points, that is considerable few.

3.3 Average moving distance of scrambling

The average moving distance of scrambling is defined as

$$\|D\|_2 = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\sqrt{(w-i)^2 + (v-j)^2}, \quad (5)$$

where (i, j) represents the pixel coordinate of a point in original image, and (w, v) represents the pixel coordinate of that point in scramble image, respectively. The lager the average moving distance of the scrambling scheme is, then the less relation between the original image and the scramble image there is, and the higher the efficiency of the scheme is.

Table 3 Statistical results of average moving distance of proposed row scrambling algorithm with randomly choosing 50000 initial values

Average moving distance	Maximum	Minimum	Average
	85.5290	85.0698	85.2564

The statistical results of average moving distance of proposed row scrambling algorithm with randomly choosing 50000 initial values are given in table 3. It can be observed from table 3 that the average moving distance of proposed row scrambling scheme stabilizes at 256/3 ≈ 85.3333, which is the universal mean of the average moving distance of the random scrambling algorithm. That illustrates the security of the proposed scramble scheme is as high as the random scramble scheme.

3.4 Natural ordered pairs

It is called a natural ordered pair if two pixels are adjacent in the original image and are adjacent in the scramble image after image scrambling.

The fewer the natural ordered pairs of the scheme there are, the more effective the scheme is, and the higher security the scheme provides.

The statistical results of proportions the natural ordered pairs account for in each 3×3 sub-images of proposed row scrambling scheme with randomly choosing 50000 initial values are given in table4.

Table 4 Statistical results of proportions the natural ordered pairs account for in each 3×3 sub-image of proposed row scrambling scheme with randomly choosing 50000 initial values

Proportion the natural ordered pairs account for in each 3×3 sub-image	Maximum	Minimum	Average
	0.0663	0.05754	0.0610

It can be seen from table 4 that proportions the natural ordered pairs account for in each 3×3 sub-images are considerable small, almost all of the adjacent pixels in original image are not adjacent in the scramble image.

3.5 Hamming correlativity

Since proposed image scrambling algorithm belongs to row scrambling algorithm that scramble image row by row, we have studied the Hamming correlativity between each row's permuting address codes.

Let $\{t_1, t_2, \ldots, t_N\}$ and $\{s_1, s_2, \ldots, s_N\}$ are two row's permuting address codes of length N, their Hamming correlativity H is defined as $H = \sum_{i=1}^{N} \delta(t_i, s_i)$, where $\delta(a, b) = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$.

Hamming correlativity H depicts similarity between two rows' permuting address codes. The larger the H is, the more similar two rows' permuting address codes are, and the less efficient the scheme is.

The statistical results of the Hamming correlativity between one row and other 255 two rows' permuting address codes of proposed row scrambling algorithm with randomly choosing 50000 initial values are given in able 5.

Table 5 The statistical results of the Hamming correlativity between one row and other 255 rows' permuting address codes of proposed row scrambling algorithm with randomly choosing 50000 initial values

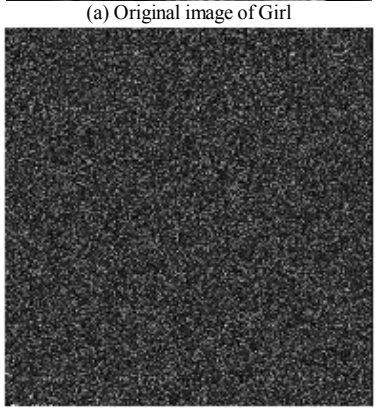
Hamming correlativity	Maximum	Minimum	Average
	254	235	245.8562

It can be seen from table 5 that the Hamming correlativity of different row of proposed row scrambling scheme is very small, numbers of the same address codes of arbitrarily two rows' permuting address codes are less than 1 averagely.

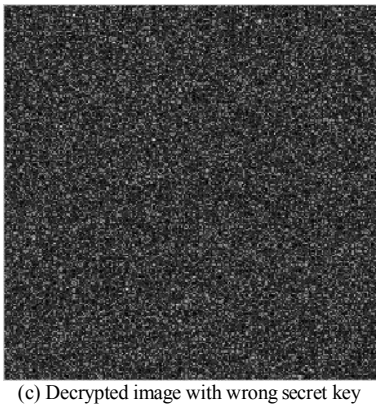
4. Experimental Results

Figure 1 shows the experimental results of proposed row scrambling algorithm for the 256×256 grey image Girl. The initial value $x_1 = 0.7$. Figure 1(a) shows the original image. Figure 1(b) shows the scramble image, which does not contain any features of original image. Figure 1(c) shows the decoded image with the secret key $x_1 = 0.70000001$ which is slight different from the correct secret key. The results indicate that the scramble image can not be decrypted correctly with a wrong secret key, thus being impossible to randomly guess the secret key to decrypt the scramble image.

(a) Original image of Girl



(b) Scramble image



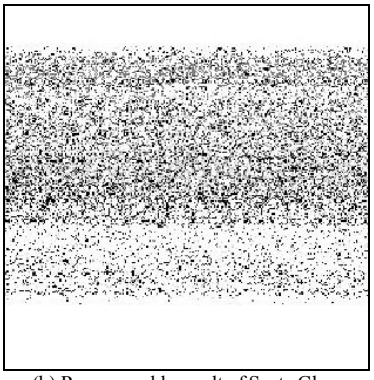
(c) Decrypted image with wrong secret key

Fig. 1 Experimental results of proposed row scrambling algorithm for the 256×256 grey image Lena

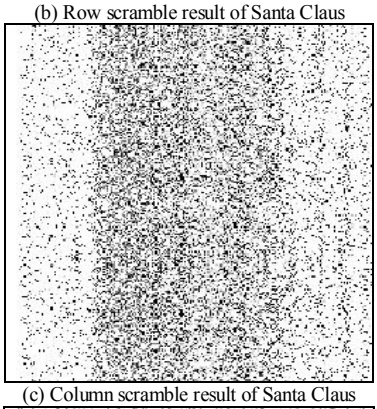
If the original image is relatively simple and has large amount of area with the same grey scale, the scramble image is easy to let an attacker judge the scrambling method, thus reducing security of the scheme. Though the main body of the paper discussed a row scrambling algorithm, it is easy to turn the scheme to a column scrambling algorithm. Compounding the row and the column scrambling scheme can strengthen security of the scheme.

Figure 2(a) shows a simple grey image of 256×256 pixels, Santa Claus. Figure 2(b) and (c) are scramble images of Santa Claus of the row and column scrambling, respectively, which have the obvious streak structure. Figure 2(d) shows the scramble result of Santa Claus of compound scrambling scheme of raw and column scrambling, which is unable to perceive any structure. Moreover, proposed scheme is easy to be generalized to work on color or grey domain in order to improve the security furthermore.

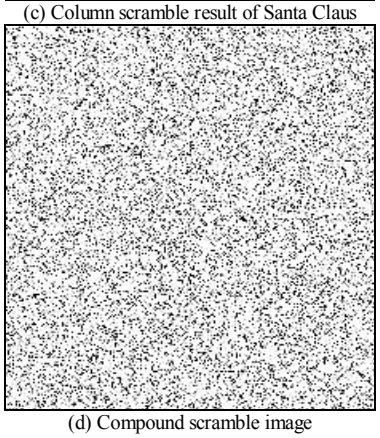
(a) Original image of Santa Claus



(b) Row scramble result of Santa Claus



(c) Column scramble result of Santa Claus



(d) Compound scramble image

Fig. 2 Scramble results of a simple image of the algorithm

5. Conclusions

In this paper, a new image scrambling algorithm based on chaos theory and sorting transformation was put forward. The new algorithm improved the drawbacks of common chaotic quantization image scrambling methods such as having high complexity, requiring the knowledge of the probability distribution to chaotic system orbit in advance, thus being convenient to choose chaotic system and speeding up the scrambling. Owing to the strong

irregularity of the sorting transformation, the initial sensitivity of the chaotic mapping are enhanced, thus improving the effect of the scrambling and making the scheme provide a high level security and a sufficient larger secret key space. The experimental results show that the algorithm is effective to scramble the image and can provide high security.

Acknowledgments

Our research was partially supported by a grant from the Natural Science Foundation of P. R. China (No. 60573124), and by a grant from the Natural Science Foundation of Liaoning, P. R. China (No. 20040948).

References

[1] Bender W, Gruhl D, Morimoto N, *et al. Techniques for data hiding* [J]. IBM Systems Journal, 1996, **35**(3&4):313-335

[2] Petitcolas F A P, Anderson R J, and Kuhn M G. *Information hiding – A Survey* [J]. Proceeding of the IEEE, special issue on protection of multimedia content, 1999, **87**(7): 1062-1078

[3] Chiou Ting Hsu, and Ja Ling Wu, *Hidden digital watermarks in Image* [J]. IEEE Transactions on Image Processing, 1999, **8**(1): 58-68

[4] Yu X Y, Zhang J, Ren H E, Xu G S and Luo X Y. *Chaotic Image Scrambling Algorithm Based ob S-DES* [J]. Journal of Physics: Conference Series, 2006, 48: 349-353

[5] Zhu Liehuang, Li Wenzhuo, Liao Lejian and Li Hong. *A Novel Image Scrambling Algorithm for Digital Watermarking Based on Chaotic Sequences* [J]. International Journal of Computer Science and Network Security, **6**(8B): 125-130, 2006

[6] Matthews R. *On the derivation of a 'chaotic' encryption algorithm* [J]. Cryptogia, 1989, 13:29-42

[7] Scharinger J. *Fast encryption of image data using chaotic Kolmogorov flow* [J]. J. Electronic Imaging, 1998, **7**(2): 318-325

[8] James P. Crutchfield, J Doyne Farmer, Norman H. Packard and Robert S. Shaw. *Chaos* [J]. Scientific American, 1986, **255**(6): 46-57

[9] Jurgen Jost. *Dynamical Systems* [M]. Springer - Verlag, Heidelberg, Berlin, 2005

Liu Xiangdong received the M.S. degree and Ph. D degrees in Computer Software and Science from Northeastern University of P. R. China in 1996 and 2000, respectively. He has also worked as a professor of Computer Science at Dalian Nationalities University from 2002. His research interests are in computer and network security, protocols, communication systems, and wireless access network.