

Blind Evaluation of Image Scrambling Degree based on the Correlation of Adjacent Pixels

Congli Wang^{*1,3}, Zhibin Chen¹, Ting Li²

¹Mechanical Institute of Technology, Mechanical Engineering College
Shi Jia Zhuang, 050003, He Bei, P.R.China

²Information Engineering Department, Mechanical Engineering College
Shi Jia Zhuang 050003, He Bei, P.R.China

³Three department of Communication, Shijiazhuang Non-commissioned Officer Academy of CAPF,
Shijiazhuang, 050061, He Bei, P.R.China

*Corresponding author, e-mail: cong7592@126.com

Abstract

The correlation of adjacent pixels is one of the important parameters for measuring the distribution of adjacent pixels' gray value. And it is widely used to evaluate the scrambling degree of digital image. Distribution figures are always plotted to show the relation of adjacent pixels' gray value, but only subjective and qualitative analysis has been applied to explain the uniformity of dots in these figures so far. In order to evaluate their uniformity quantitatively and objectively, two approaches are advanced: average gray difference method and block uniformity method. And, two blind evaluating methods on the image scrambling degree are presented further according to the former. Simulation results show that both of the two approaches can describe the uniformity of distribution figures of adjacent pixels' gray value quantitatively and objectively. They can be operated with just a little data of a cipher image and without using any data of plain image. These two evaluation methods on image scrambling degree are in a good agreement with the Human Vision System, and they can achieve the goal of objective and fast blind evaluation.

Keywords: correlation of adjacent pixels, average gray difference, block uniformity, image scrambling degree, blind evaluation

Copyright © 2013 Universitas Ahmad Dahlan. All rights reserved.

1. Introduction

The image scrambling technology is studied intensively in recent years. A great number of research results which could achieve a good encrypting performance have been reported. But the study on how to evaluate the scrambling degree objectively is lagging behind comparatively. Most evaluating methods depend on plain image, and this lead to the lack of criteria or successful models. Some serious challenges to the evaluation system should be considered: first, both of the pixel value and position should be considered at the same time; second, the evaluation degree should reflect the relationship between a cipher image and the scrambling scheme applied to the former one effectively, such as the relationship between a cipher image and the iterative time; third, the evaluation approach should be independent of the plain image as much as possible; last, the proposed evaluation scheme should obtain the most approximate evaluation with the least data of an image.

Correlation analysis of adjacent pixels is an important way to test the gray value relationship between adjacent pixels in cipher image. The strong correlation existing in adjacent pixels of a natural image would be broken when the image is scrambled. The correlation distributions are plotted and analyzed to explain its distribution range and uniformity in [1-4] qualitatively, but the difference between two plots is not calculated quantitatively and exactly.

In order to achieve better measure of the distribution of adjacent pixels' gray value, two proposals-average gray difference and block uniformity-are advanced in this paper, and two evaluating ways on the image scrambling degree are put forward to further.

2. Correlation Analysis of Adjacent Pixels

4000 pixels are chosen randomly from the test image, and their correlation distribution of gray value is plotted. Figure 2(a) and (d) show the correlation of the plain image (lena.bmp shown in Figure 1(a)) and its encrypted image scrambled by the approach in [1]. The abscissa and ordinate represent the gray value of pixels and their adjacency respectively. Dots are located along the diagonal in Figure 2(a), because the gray values of the adjacent pixels are close to each other for a meaningful image. Dots in Figure 2(d) are scattered over the entire plane with good regularity, and that means the gray value of the adjacency is random for the cipher image. Therefore, a conclusion could be drawn that the correlation of adjacent pixels is greatly reduced for the cipher-image. To describe the regularity of dots in the plain objectively, two methods are given in the next section.

3. Average Gray Difference Analysis

N represents the number of pixels chosen randomly from the image. $count[i, j]$ is the number of dots in position (i, j) in Figure 2. For pixels with gray value $x = i$, the absolute difference of adjacent pixels is defined by Equation (1):

$$sumdif[i] = \sum_{j=0}^{255} count[i, j] * |j - i| \quad (1)$$

So the total gray difference is calculated by Equation (2):

$$sumgray = \sum_{i=0}^{255} sumdif[i] = \sum_{i=0}^{255} \sum_{j=0}^{255} count[i, j] * |j - i| \quad (2)$$

And the average gray difference is given by Equation (3):

$$averdif = sumgray / N \quad (3)$$

Where $averdif$ represents the average gray difference between any pixel and its adjacency.

In order to evaluate scrambling degree by $averdif$, the average gray difference in an ideal scrambled image is analyzed as follows.

N pixels are chosen randomly from an ideal scrambled image. The correlation distribution of the adjacent pixels is uniform in the entire plain. The probability of each dot's appearing in plain is defined by Equation (4).

$$P = N / (256 * 256) \quad (4)$$

The value of adjacent pixels with value $x = i$ is also random from 0 to 255. Therefore, the total difference of gray value is:

$$isumgray = \sum_{i, j=0}^{255} |j - i| * P \quad (5)$$

The ideal average difference is:

$$iaverdif = isumgray / N = 85.33 \quad (6)$$

It is clear that the average difference is independent of pixel number N when ideal scrambled.

The image scrambling degree is defined by Equation (7).

$$\alpha = 1 - \frac{|averdif - iaverdif|}{iaverdif} \quad (7)$$

It is not true that higher $averdif$ means better regularity. For ultimate distribution, such as all of the adjacent pixels' value is $y = 0$ and $y = 255$, $averdif$ is higher but the scrambling degree becomes lower. Therefore, the closer $averdif$ to $iaverdif$ is, the more uniform the distribution of gray value of the adjacent becomes.

4. Block Uniformity Analysis

A block B with size $W \times H$ is chosen randomly from the correlation distribution plot of the ideal scrambled image. The uniformity of dots in B should be equal to that in the entire plain theoretically. And it is denoted by the ratio of dot number to area: N_B is the dot number in block B . The ratio R_B is defined as Equation (8).

$$R_B = \frac{N_B}{W * N} \quad (8)$$

The ratio of entire plain is:

$$R_0 = \frac{N}{256 * 256} \quad (9)$$

And Equation (10) should be true when ideal scrambled.

$$R = \frac{R_B}{R_0} = 1 \quad (10)$$

In order to constitute a parameter to evaluate scrambling degree by Equation (8)~(10), Gray Relation Analysis (GRA) theory is used. The gray system theory, which was established by Professor Deng Julong, focuses on the uncertain system with small samples and inadequate information. The image scrambling effect evaluation can be seen as a gray process, so it is feasible to calculate the characteristic sequence of ideal cipher image by GRA. The main idea of GRA is described as follows: first, to constitute the referential sequence and comparing sequence; then, to calculate the difference sequence; at last, to compute the gray relation coefficient and gray relation degree of the difference sequence.

To form the gray sequence, the entire plain of correlation distribution (such as Figure 2(d)) is divided into 256 sub blocks with size 16×16 , and the ratio R_i ($i = 0, 1, \dots, 255$) is computed by Equation (8). So can be taken as the gray sequence and the referential sequence is $(1, 1, \dots, 1)$ whose length is equal to 256. The mean square deviation between the two sequences is computed by Equation (11).

$$D = \frac{\sum_{i=1}^{255} (R_i - R)^2}{256} \quad (11)$$

The degree of gray relation is derived from the formula in [5].

$$\beta = \frac{1}{1 + D} \quad (12)$$

And β can be taken as the scrambling degree.

5. Results and Analysis

The testing image, lena.bmp, which is with the dimension of 256×256 and 256 gray scales, is shown in Figure 1(a). The so called Arnold transform is chosen in our experiment because of its wide acceptance. The image is encrypted by two-dimension [6] and three-dimension [7] Arnold transforms, and bit-level permutation in [1] (2D AT, 3D AT and BLP for

short, respectively). The iterative times are 192 (a complete period of two-dimension Arnold cat map), 100, and 1, respectively. The cipher image is shown in Figure 1 from (b) to (d).

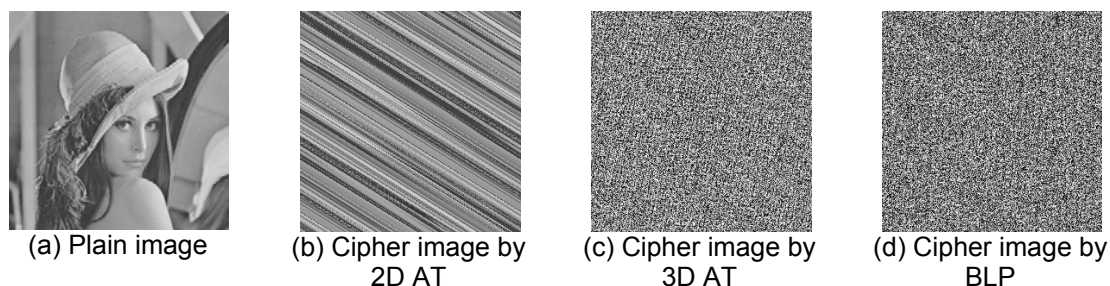


Figure 1. Plain image and cipher image

Figure 2 shows the correlation distribution of adjacent pixels in horizontal direction for each image in Figure 1. Pixel number $N=4000$. Figure 2(b) shows that the uniformity of dots is better than that in Figure 2(a) because the cipher image looks disordered compared to the plain image. And the dots in Figure 2(c) and (d) scatter all over the entire plain, as a result, the distribution rule in Figure 2(a) is broken. But it is difficult to observe the difference between (c) and (d) subjectively. Therefore, Table 1 shows the average gray difference and the mean square deviation of block uniformity. From it, it can be concluded that the uniformity of Figure 2 (c) is better than that of (d), and the difference is imperceptible to human eyes. Table 2 shows the image scrambling degree in Figure 1. The result in both tables indicates that the cipher image Figure 1(c) can achieve better encrypted effect than Figure 1(d).

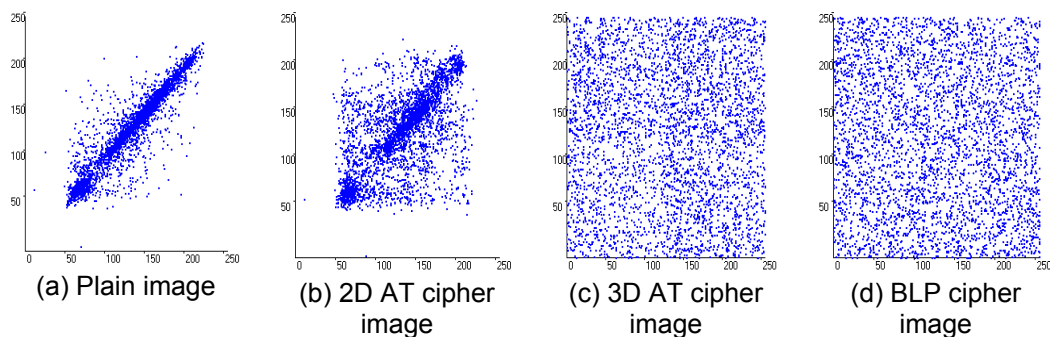


Figure 2. Correlation Plot of Two Adjacent Pixels (horizontal direction)

Table 1. Average Gray Difference and Mean Square Deviation of Block Uniformity in Figure 2

Proposed parameters	Plain image	2D AT	3D AT	BLP
averdif	5.498	23.367	84.793	84.754
D	12.393	5.736	0.062	0.101

Table 2. Scrambling Degree in Figure 1

Scrambling degree	Plain image	2D AT	3D AT	BLP
A	0.064	0.274	0.994	0.993
B	0.075	0.148	0.942	0.908

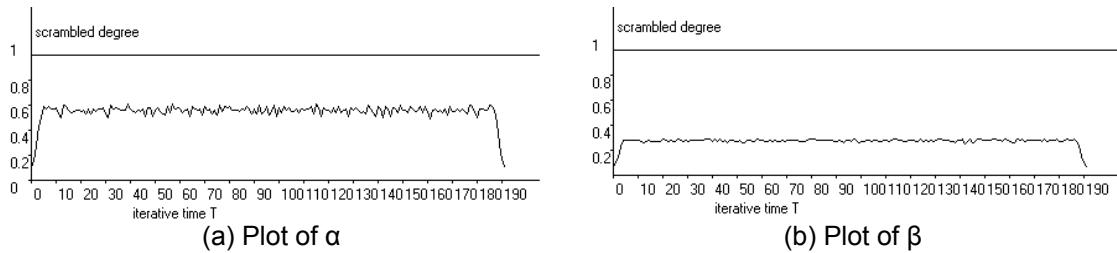


Figure 3. Distribution Plot of Scrambling Degree by 2D AT, $T=192$

The plots in Figure 3 indicate that the scrambling degree encrypted by 2D AT is low. Because 2D AT only changes the position of pixels, and the gray histogram of cipher images is not changed. As a result, the gray value of adjacent pixels is limited in some range which is decided by the maximum and minimum gray value of plain image. This lead to a result that the dots in correlation plot cannot scatter all over the entire plain. Therefore, 2D AT cannot achieve a good scrambling effect.

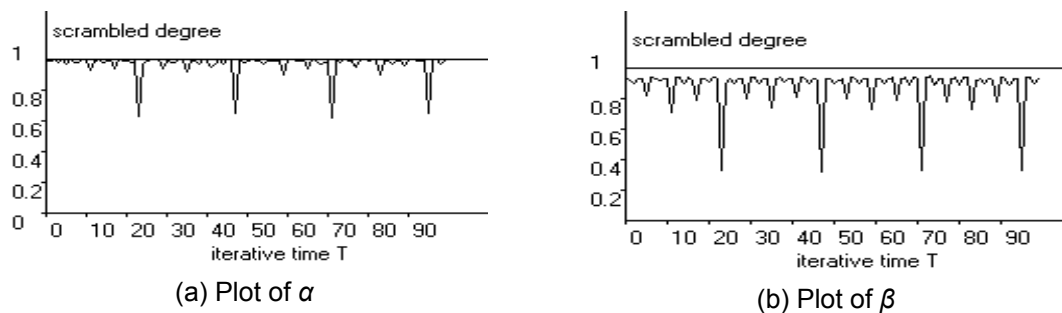


Figure 4. Distribution Plot of Scrambling Degree by 3D AT, $T=100$

The same analysis is made on 3D AT (Figure 4). Figure 4 shows that most of the data is close to 1. But the scrambling degree doesn't always increase along with the transform time. Instead, it even drops acutely by some transform time. The value will be lower when the iterative time T is multiple of six, and the minimum scrambling degrees occur when $T = 24, 48, 72, 96$. The cipher images with those iterative times which mentioned above are shown in Figure 5 and possess an obvious regularity. Therefore, it is not as what [7] has mentioned: the scrambling effect does not change obviously after 10 times scrambled. It indicates that the measure methods have a high sensitivity to the distribution characteristics of adjacent pixels' gray value, and they are in a good agreement with the Human Vision System (HVS). It can be seen that the 3D AT can gain a good scrambling degree in Figure 4 except some special iterative time ($T = 24, 48, 72, 96$).

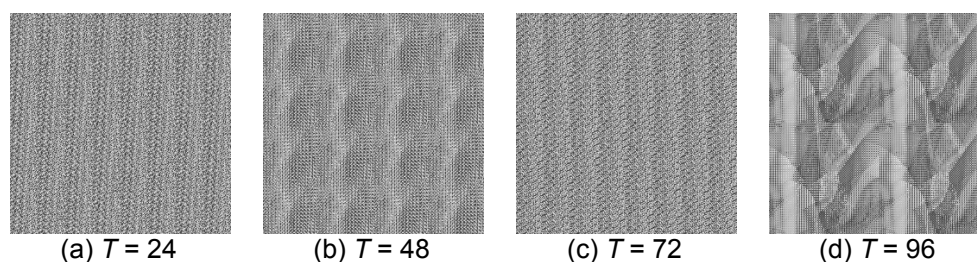


Figure 5. Cipher Images with Iterative Time ($T = 24, 48, 72, 96$) by 3D AT

The reason of low scrambling degree (when $T=24, 48, 72, 96$) is the parameters used in 3D AT, which is given in [7]. This can lead to the scrambling effect like 2D AT after certain times scrambled. For example, the cipher images encrypted by 3D AT and 2D AT with $T=192$ are same. That is to say, they come back to the plain image again. By analyzing the correlation plots in Fig.6, it is found that there are dense and sparse blocks obviously. Therefore they have a low scrambling degree. This problem could be solved by changing scrambling parameters in 3D AT process.

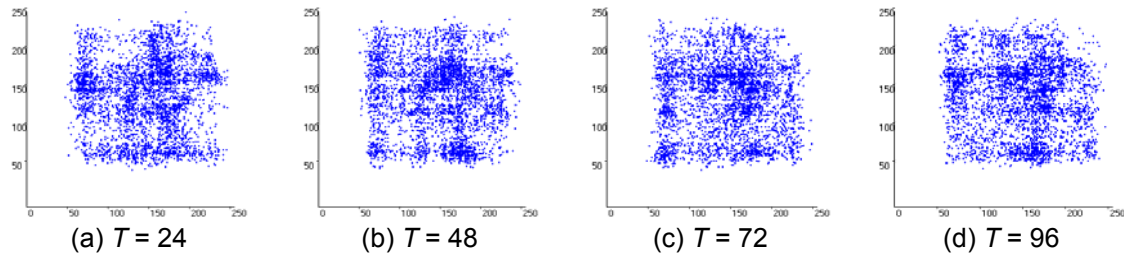
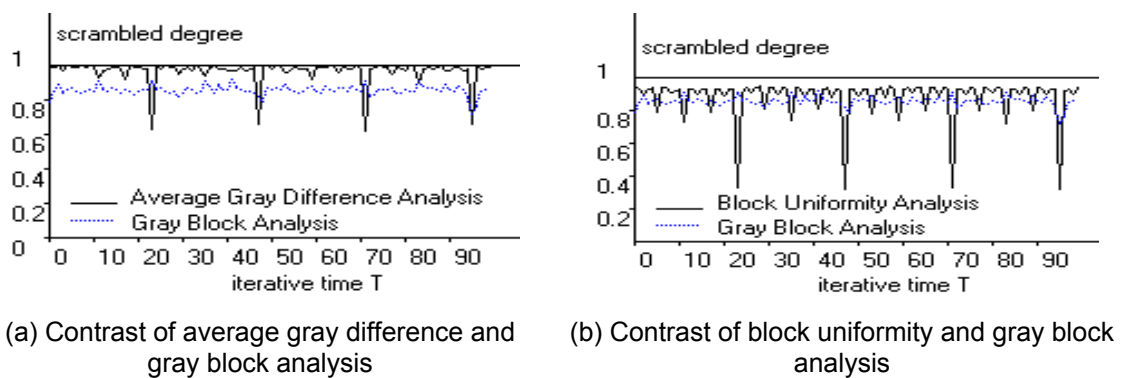


Figure 6. Correlation Plots of Two Adjacent Pixels with Iterative Time ($T= 24, 48, 72, 96$) by 3D AT



(a) Contrast of average gray difference and gray block analysis

(b) Contrast of block uniformity and gray block analysis

Figure 7. Distribution Plot of Scrambling Degree with Different Evaluation Methods by 3D AT

The evaluation approaches mentioned in this paper are contrasted with that in [5], which are about the cipher image by 3D AT, and the results are shown in Figure 7. As to the agreement with HVS, the method of block uniformity analysis offers the best. The second one is an average gray difference analysis, and the last one is a gray block analysis.

The following information is extracted from above analysis:

1) Both the methods, average gray difference and block uniformity, can measure the uniformity of correlation distribution of adjacent pixels.

2) It is easy to prove that $0 \leq \alpha, \beta \leq 1$, and we can get $\alpha = 1, \beta = 1$ under the condition of ideal scrambled.

The next conclusions, which can meet the challenges mentioned in section 1, can also be achieved:

1) Both pixel value and position scrambling can be considered by analyzing the average gray difference and block uniformity of the gray correlation distribution plot of adjacent pixels in cipher image.

2) The scrambling degree changes regularly with the iterating time. This can be seen in Figure 3 and Figure 4.

3) The evaluation approach can be performed without any data of plain image. That is to say, it is independent of the plain image absolutely and can achieve blind evaluation.

4) Although only 4000 pixels, about 6 percentage of the total pixel number, are used to compute scrambling degree, good and subjective evaluating effect can be achieved.

6. Conclusion

In conclusion, two novel evaluation approaches, which are based on the correlation plot of adjacent pixels, have been advanced in this paper to evaluate the uniformity of gray value's distribution. And two approaches have been advanced further to prove the scrambling effect of images scrambled by taking 2D AT, 3D AT and BLP as examples. From the simulation and experimental results, one of the major advantages of these new methods is that it can be carried out by only using a small part of cipher image's data without any information about plain image. Besides, a good agreement with HVS is another advantage. In a word, this method can achieve blind and fast evaluation of the scrambling degree. It is objective and practical.

On the research by evaluating the effect of an image encryption scheme, a further research, which can solve the problem of criteria lack, is planned to explore the scientific models based on natural image or ideal scrambled image. And continuing studies will yield further insight into the fast and blind evaluation scheme.

References

- [1] Zhiliang Zhu, Wei Zhang, Wong, Kwok-wo, Hai Y. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences*. 2011; 181: 1171-1186.
- [2] Xingyuan Wang, Lei Yang, Rong Liu, Abdurahman Kadir. A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dyn*. 2010; 62: 615–621.
- [3] Guoji Zhang, Qing Liu. A novel image encryption method based on total shuffling scheme. *Optics Communications*. 2011; 284: 2775–2780.
- [4] Xiaoxia Ren, Xiaofeng Liao, Yonghong Xiong. New image encryption algorithm based on cellular neural network. *Journal of Computer Applications*. 2011; 31(6):1528-1530.
- [5] Hongpeng Tian. Image scrambling performance blind evaluation based on grey block analysis. *Computer Engineering and Applications*. 2009; 45(34):171-173.
- [6] Yongkui LI, Qiaosheng Feng, Fen Zhou, Qiang Li. 2-D Arnold transformation and non-equilateral image scrambling transformation. *Computer Engineering and Design*. 2009; 13: 3133-3135.
- [7] Chengmao Wu, Xiaoping Tian. 3-Dimensional Non-equilateral Arnold Transformation and its application in image Scrambling. *Journal of Computer-aided Design & Computer Graphics*. 2010; 22(10): 1831-1840.