A Scrambled Image Blind Evaluation Method Based on Space and Frequency Domain

Congli Wang a, Xiong Li
Noncommissioned Officer Academy of PAP, Hangzhou, China
a tzhang@clsg.edu.cn

Abstract. Most of the image scrambling degree evaluation algorithms rely on the statistical features of the original image, which cannot achieve blind evaluation. Based on the uniform distribution model of the statistical characteristics of ideal scrambled images, a blind evaluation algorithm of image scrambling degree combining space and frequency domain is proposed in this paper. In the space domain, the uniform distribution characteristics of the gray histogram of the ideal scrambled image are used, and the uniform distribution characteristics of the Discrete Fourier Transform (DFT) spectrogram in the frequency domain are combined with the gray correlation analysis theory. The two are weighted to realize the space and frequency domain evaluation of the scrambled image performance. The experimental results indicate that the evaluation algorithm in this paper can consider the performance evaluation of both pixel value and pixel position dislocation, avoiding the disadvantage of ineffective spatial domain evaluation when only the pixel position scrambling is performed. It has very sensitive to the histogram distribution and frequency domain features of encrypted images, and has good agreement with Human Visual System (HVS). The original image is completely independent, and it enables blind evaluation objectively.

Keywords: Image scrambling degree, Uniform distribution, Space domain, frequency domain, Blind evaluation.

1. Introduction
Image scrambling, as the main means of image encryption technology, has achieved rapid development in recent years [1]. How to scientifically evaluate the effect of scrambling algorithm is the main problem currently faced. Currently, the commonly used objective evaluation method is the scrambling evaluation. The scientific scrambling evaluation algorithm should be able to achieve the following objectives: first, it can measure the performance of encryption algorithms for both pixel position and pixel value transformations; second, it should be able to reflect some relationship between the scrambled image and the scrambling algorithm used, such as the relationship between the scrambling degree and the number of scrambles; the third is that the calculation process should be as independent as possible from the original image data. The third point is particularly important, and the solution to the problem is to establish a scientific statistical model for the ideal scrambled images and further study the blind evaluation indexes, so that accurate and objective blind evaluation can be achieved without the...
participation of the original images in the scrambling evaluation. In recent years, most of the commonly used metrics for scrambling evaluation rely on the original images, and no more scientific mathematical models have been established. The paper[2] uses the space-domain differential second-order statistics of images to evaluate the scrambling degree and to establish a scientific model. In the literature[3], a method based on discrete cosine transform is proposed to evaluate the effect of frequency domain image encryption but no model is established. In this paper, from the statistical characteristics of uniform distribution of statistical features related to the image space and frequency domain, an ideal scrambled image uniform distribution model is established, and a blind evaluation algorithm is presented in the space and frequency domains based on the mode. The two methods are combined to achieve objective evaluation.

2. The ideal uniform distribution of scrambled images in the space domain.

After the image is scrambled, the more random the probability of taking the gray value for each coordinate position, the better the noise-like characteristics of the scrambled image. In the limit condition, the probability of taking each gray value is equal, and the scrambling image can achieve the ideal scrambling. The grayscale distribution of the scrambled image should be similar to the uniform noise distribution. The histogram distribution of the secret image should be a straight line when the probability of each gray value is equal, which is called ideal scrambling.

The ideal uniform noise model is shown in equation (1):

\[ p_z(z) = \frac{1}{b-a}, a \leq z \leq b \]  

The mean is \( m = (a + b) / 2 \) and the variance is \( \sigma^2 = (b - a)^2 / 12 \).

For an ideal scrambled image, \( a = 0, b = 255 \), the grayscale histogram distribution is modeled by equation (2):

\[ p_z(z) = \frac{1}{256} \]  

For a visible image of size \( m \times n \) and 256 gray levels, the histogram distribution should conform to the uniform noise distribution after ideal scrambling, and the distribution function model is rewritten and expressed in terms of the number of gray values as equation (3):

\[ h(k) = \frac{m \times n}{256}, k = 0, 1, \ldots, 255 \]  

Equation (3) shows that the number of pixels at each gray level should be equal when the image is ideally scrambled.

The definition is now improved according to the ideal uniform noise model (3).

Definition 1: The grayscale image \( A \) is the original image with 256 gray levels, which is transformed into a scrambled image \( B \) by the scrambling transformation \( T \). Taking any region \( D \) of \( B \), \( f_{BD}(v) \) represents the number of pixels with grayscale value \( v \) for region \( D \) of image \( B \), \( v = 0, 1, 2, \ldots, 255 \). If for each \( v \), equation (4) holds, then \( T \) is called the ideal scrambling transformation.

\[ \frac{f_{BD}(v)}{\|D\|} = \frac{1}{256} \]  

where \( \|D\| \) denotes the number of pixels in \( D \).

Definition 1 indicates that for any region \( D \), \( T \) is an ideal scrambling transformation if its pixel distribution probability is equal to the probability of an ideal uniform noise distribution.

From Definition 1, it is known that the ideal pixel distribution of the scrambled image should conform to the uniform noise distribution and does not depend on the grayscale statistical characteristics of original image, so this definition has more important application value and is more general.
Gray Relation Analysis (GRA) is a part of gray system theory [4], which is mainly used to analyze the relationships between objects with incomplete information and unclear inherent connotations. The basic idea of gray correlation analysis is to determine the reference and comparison series, and find the difference between the two series, and calculate the gray correlation coefficient and gray correlation degree for the difference sequence.

3. Basic principles of GRA
Compared with traditional mathematical analysis, GRA is unique in that it constructs a brief framework that can analyze the relationship or behavior of series, even if there is little information about the sequence. Let $X$ be the set of sequences: $X = \{x_i | i \in I, i = 0, 1, 2, \ldots, m \}$, $x_i, y_j \in X$, The symbol $\gamma (x_i, y_j)$ represents the adjacent measure between $x_i$ and $y_j$, or the gray correlation measure. $\Delta_{0j}(k)$ is the absolute difference between $x_0(k)$ and $x_j(k)$, $x_0$ is the reference sequence, $x_j$ is the comparison sequence, and the specific calculation steps of gray correlation are as follows:

**Step1:** Grey relational number is $\gamma (x_0(k), x_j(k))$

The equation for the number of gray relations is expressed as equation (5):

$$\gamma (x_0(k), x_j(k)) = \frac{x(\min) + \zeta x(\max)}{\Delta_{0j}(k) + \zeta x(\max)}$$

$x(\min) = \min_k \Delta_{0j}(k)$ is the lower environment parameter of $L_{Y_{gr}}$. $x(\max) = \max_k \Delta_{0j}(k)$ is the upper environment parameter of $dd$, $\zeta \in [0, 1]$ is the resolution factor, which is generally taken as 0.5.

**Step2:** Grey relational degree

The values of the grey relational coefficients at each point are summed to obtain the gray relational degree calculation equation (6):

$$\gamma (x_0, x_j) = \frac{1}{n} \sum_{k=1}^{n} \gamma (x_0(k), x_j(k))$$

Gray relational degree is a comparative measure between sequences and sequences, and can be used directly as an evaluation index of scrambling degree.

4. Blind Evaluation Algorithm of space domain Scrambling Degree Based on Ideal Uniform Distribution

The Equation (4) in Definition 1 shows that the probability of the pixel distribution is equal to the probability of the ideal uniform noise distribution for any region $D$ after the ideal scrambling transformation of the image. According to Definition 1, the degree of image scrambling is defined as follows.

**Definition 2:** $f_A(v)$ represents the number of pixels with gray value $v$ in image $A$, $f_{BD}(v)$ denotes the number of pixels with gray value $v$ in region $D$ of image $B$, $v = 0, 1, 2, \ldots, 255$. The scrambling degree is defined as Equation (7):

$$s = \min_D \left[1 - \sum_{v=0}^{255} \frac{f_{BD}(v)}{|D|} - \frac{1}{256}\right]$$

Features 1: $0 \leq s \leq 1$;
Features 2: When $s = 1$, it is ideal scrambling.

The physical meaning of equation (7) is to find a sub-block after dividing the scrambled image into sub-blocks such that it has the highest similarity to the uniform noise model distribution. However,
Definition 2 is not easy to compute because it involves the problem of selecting the location and size of arbitrary region D. We need to design a new and easily calculable evaluation index for the degree of image scrambling based on the ideal uniform noise model.

Let $p_i(j)$ is the probability of distribution of pixel values with gray value $j$ in the scrambled image $B$, and $p(j)$ is the pixel value distribution probability of the gray value $j$ in the ideal uniform noise model, so $p(j) = 1/256$, $j = 0, 1, \cdots, 255$.

According to Definition 1 and Definition 2, the index $\alpha$ to measure the degree of image scrambling is constructed as shown in equation (8):

$$
\alpha = 1 - \frac{\sum_{j=0}^{255} h(j) \times |p_i(j) - p(j)|}{\sum_{j=1}^{255} h(j) \times \max(p_i(j), p(j))}
$$

It is easy to verify that $0 \leq \alpha \leq 1$.

5. Blind Evaluation Algorithm of Scrambling Degree in Frequency Domain Based on GRA

In order to find out the characteristic changes of the image before and after the scrambling in the frequency domain, the original image lena.bmp and its scrambled image are DFT transformed. The DFT spectrograms of the original image and the scrambled image are given in Figures 1 and 2, including the plane and Three-Dimensional(3D) images, respectively. The scrambled image is the image scrambled 5 times by 3D Arnold Transformation (AT)[5].

(a) plane image

(b) 3D image

Fig. 1 The spectrum of original image by DFT
Comparing with the spectrum of DFT, the spectrum distribution of the scrambled image is more uniform than that of the original image, and the distribution of high-frequency components is dispersed, breaking the characteristic that the distribution of high-frequency components is more concentrated in the original image. In order to measure the uniformity of the FFT transform results of the scrambled images, the GRA method is used.

Analyzing the spectrum before and after DFT transformation, the high-frequency components of the original image are concentrated in the peak, and the mean value of this region should be significantly higher than other regions. The mean value of each sub-block should be approximately equal for the disordered image. Therefore, using the theory of GRA, the average value of sub-blocks is selected as the reference and comparison series. After chunking the scrambled image spectrogram, the mean values of the sub-blocks are calculated and a comparison sequence is formed. The sub-block means should converge to the same value at the ideal scrambling, and after normalization, a reference sequence with all values of 1 is formed:

\[ x_0 = (1, 1, \ldots, 1) \]

The specific operations of gray relation and scrambling are as follows:

**Step1:** The DFT transform is performed on the read-in scrambled image, and the transform result is chunked. This procedure takes the size of the sub-block as 32×32.

**Step2:** By calculating the mean value of each sub-block, a sequence of means of length 1 with the number of sub-blocks is obtained: \( x_i = (m_1, m_2, \ldots, m_N) \). Where \( m_i \) represents the mean value of the \( i \)-th image sub-block and \( N \) denotes the total number of sub-blocks.

**Step3:** After normalizing the series of mean values according to (9), it is used as a comparison sequence:

\[ x_i = \frac{x_i}{\max(x_i)}, \quad (9) \]

**Step4:** Calculation of the gray relation between \( x_0 \) and \( x_i \):

\[ r_k = \frac{1}{1 + \varepsilon}, \quad (10) \]
\[ \xi_k = |x_0(k) - x_1(k)| \]  

Step5: The overall correlation of the sequences is \( \beta = \frac{1}{N} \sum_k r_k \), which is the image scrambling degree in the frequency domain.

In order to evaluate the degree of image scrambling more objectively, the two evaluation indexes in the space and frequency domain are weighted to obtain the overall scrambling factor, as shown in equation (12):

\[ \eta = \frac{\alpha + \beta}{2} \]  

6. Analysis of experimental results

In order to examine the scrambling performance of the two scrambling evaluation methods and the consistency with HVS, a grayscale image lena.bmp with a size of 256×256 and a gray level of 256 was used for the experiment. The 3D AT method in the paper[5] is used to scramble it with a transformation count of 100.

We calculate and compare the scrambling degree evaluation algorithm that combines the space and frequency domain proposed in this paper. The comparison result of 3D AT scrambling degree change curve is shown in Figure 3:

![Distribution plot of scrambling degree by 3D Arnold transform](image-url)
The 3D AT disorder curve (Fig. 3) shows that most of the space scrambling degree varies around 0.9. However, the scrambling degree is below 0.8 when the number of transformations is a multiple of 6. In particular, it is below 0.5 at the 24th, 48th, 72nd, and 96th times. This property shows that the scrambling degree of 3D AT does not simply increase with scrambling times, but even decreases drastically after a certain number of scrambling. For the scrambling degree of frequency domain, 3D AT has a higher scrambling degree (above 0.9), indicating that the scrambling algorithm has a high frequency domain scrambling degree. The integrated scrambling degree is mainly concentrated between 0.8 and 1, except for the minimum points mentioned above.

For the 3D AT transform results, the evaluation algorithms in the literatures[6, 7] were used for comparison, respectively. The results are shown in Figure 4. In terms of consistency with the HVS, the algorithm in this paper is the best, followed by the algorithm of gray block analysis, and the algorithm of image surface area is the worst.

Based on the above discussion, the scrambling evaluation algorithm based on the uniform noise model combining the space and frequency domain has the following advantages:

Firstly, by combining the space and frequency domain, the performance evaluation considering both pixel value and pixel position scrambling is realized. It avoids the disadvantage that the effect of space domain evaluation is ineffective when only pixel position scrambling is performed. The scrambling degree converges to 1 when the ideal scrambling is achieved.

Secondly, the degree of scrambling changes regularly with the number of scrambling times, and has very sensitive to the histogram distribution and frequency domain features of encrypted images, which has good agreement with HVS.

Thirdly, the evaluation algorithm only needs the gray histogram information and frequency domain information of the encrypted image, without any data of the original image. It is completely independent from the original image, so they can achieve blind evaluation objectively.

7. Conclusions

The blind evaluation study of image scrambling degree can objectively evaluate the scrambling degree, make up for the shortcomings of subjective evaluation, and provide guidance for the development of high-security scrambling algorithms. Based on the analysis of the grayscale uniform distribution model of the ideal scrambled image, combined with the theory of GRA, this paper proposes a scrambled image blind evaluation method based on space and frequency domain. The experimental results show that the model and evaluation algorithm of this paper are applicable to natural images, avoiding the disadvantage of ineffective space domain evaluation when only pixel position scrambling is performed, and they have good agreement with HVS. It provides a unified standard for the objective evaluation of image scrambling degree without relying on the statistical features of the original image for blind evaluation. The research has important theoretical significance and practical value for the evaluation of image scrambling degree.
References

[1] Y. Gou, W. Jingshi, and Y. Zhouyan, “Image encryption algorithm based on scrambled bits between adjacent pixels,” Computer Engineering and Design, no. 7, pp. 1829–1835, 2020.

[2] L. Wangcong, B. Chenzhi, X. Xueming, and C. Zhang, “Linear model for blind evaluation of image scrambling degree based on difference statistic distribution,” Journal of Computer Applications, vol. 32, no. 12, pp. 3470–3473, 2012.

[3] S. Lishan, T. Zhouyi, L. Zhanghong, and Y. Sunwei, “A novel image encryption performance evaluation based on discrete cosine transform,” Computer Technology and Development, vol. 30, no. 5, pp. 99–102, 2020.

[4] L. Dengju, The Primary Methods of Grey System Theory. Wuhan, HB, CHINA, 2005.

[5] M. Wucheng and P. Tianxiao, “3-Dimensional non-equilateral Arnold transformation and its application in image scrambling,” Journal of Computer-Aided Design and Computer Graphics, vol. 22, no. 10, pp. 1831–1840, 2010.

[6] X. Wangxin, and T. Bu, “An evaluation algorithm of image scrambling degree based on the image area,” Journal of Anhui University (Natural Science Edition), vol. 35, no. 4, pp. 48–52, 2011.

[7] P. Tianhong, “Image scrambling performance blind evaluation based on grey block analysis,” Computer Engineering and Applications, vol. 45, no. 34, pp. 171–173, 2009.