Design and Implementation of Image Encryption System Based on Random Grids and Mscan Patterns

Guangming Yang*, Jingying Ma* and Zhenhua Tan**

University of Northeastern, Faculty of Software, room Information Building B432, H010 Mailbox School of Software, Northeastern University, Hunnan Campus, No. 195, Innovation Road, Hunnan District, Shenyang. Email: *yanggm@mail.neu.edu.cn, **383913734@qq.com, **tanzh@mail.neu.edu.cn

Abstract. In the field of information security and the rapid development of network technology and the era of Internet+, the concept of cyberspace security has risen, and related algorithms and related works for image encryption have emerged. This paper studies the image encryption based on the random grid encryption algorithm and the modified SCAN encryption algorithm. A hybrid image encryption system is proposed and designed by combining these two algorithms. This also considered the distortion, compressibility and encryption strength of the image. Using the defects of the MSCAN algorithm, a simulation attack was performed on the traditional MSCAN encryption algorithm. Finally, statistical analysis and diffusivity tests are used to evaluate the design of the encryption system.

1. Introduction

With the rapid development of information security and network technology and the advent of the Internet+ era, people’s demand for data transmission has greatly improved. At the same time, the transmitted text on the Internet is not just monotonous text, but related files such as images, audio, video, etc. have begun to spread more and more on the Internet. Therefore, the confidentiality and security of image files in the transmission process has become an important issue that cannot be ignored.

At the same time, image encryption has become an indispensable part of information security. There are many encryption algorithms, of which the more influential is the chaotic encryption method[6]. Discrete chaos encryption is one of the most representative ones. Chaotic stream ciphers are mainly used in Logistic mapping [1]. The advantages of this algorithm are simple, fast encryption, and high security. The disadvantage is that it does not consider the characteristics of the image. Based on the characteristics of the image, this paper proposes a random grid2 encryption algorithm and a modified SCAN mode encryption algorithm, integrates the two algorithms, and uses the modified SCAN mode to encrypt the pixel attributes of the image, the gray value of the image uses a random grid algorithm for encryption, and the two algorithms form a complete system.

The test results show that the algorithm designed in this paper has excellent performance in resisting known plaintext attacks, and also has excellent resistance to aggressive statistical attacks such as aggressive attacks.

2. Random Grid and Modified Scan Image Encryption Algorithm

The algorithm proposed in this paper is to combine the random grid [9][10]and the modified SCAN algorithm to encrypt the image. The modified scan algorithm can obtain complex image scrambling by combining multiple sets of basic scanning methods, and the operation is simple and the efficiency is...
high. However, in the experiment, it is found that the MS-CAN algorithm has the disadvantage of being insecure, that is, it does not completely confuse the pixels of the image, and is vulnerable to plaintext analysis. According to this defect, based on the random lattice algorithm, the two-dimensional sequence of the pixels of the image is completely scrambled and rearranged to ensure that the algorithm has strong resistance. The two algorithms are respectively used to encrypt the pixel attributes and gray value attributes of the image. The combination of the two algorithms compensates for the lack of a single encryption algorithm in the encryption process.

2.1. Random Grid Encryption Algorithm
Kafri and Keren [2] introduced the concept of a random grid for the first time in 1987 and used it for the encryption of images and graphics. Kafri and Keren define that the random grid is a transparency composed of a two-dimensional sequence of grayscales. Each pixel is completely transparent or completely opaque, and transparent or opaque is achieved by a random rule like a “toss in”, so in a two-dimensional sequence of random cells, there is no correlation between the values of different pixels. Transparent pixels allow light to pass through and opaque pixels prevent light from passing through.

The probability of the number of transparent pixels in the random grid is equal to the number of opaque pixels, so the average optical transmission of a random grid is equal to 1/2, that is, the probability of transparency and opacity of each pixel is 1/2. The generalized OR operation is expressed by $\otimes$, which describes the overlapping relationship between two random grid pixels multiplied by pixels. is exactly the same as $R$, so for every pixel $r$ in $R$, there is

$$T(R \otimes R) = 1/2 \quad T(r \otimes r) = 1/2$$

(1)

Assuming that $R_1$ and $R_2$ are two independent random cells of the same size, the probability that each pixel in the two random cells is overlapped (transparent or opaque) is equal, set the transparency to 0, the opacity to 1, According to permutations and combinations, there are four overlapping results for pixels in two random grids. Only if the two are transparent, the overlapping result is transparent, so the probability of transparency is 1/4.

In this paper, three different random grid algorithms are designed to implement image encryption, a image of $w \times h$ is input. Two random grids $R_1$ and $R_2$ are output according to the algorithm, so that they do not give away any information about image $B$, When they overlap, the image $B$ can be displayed.

Input: an image $B$ of size $w \times h$, $B[i, j] \in \{0, 1\}$ (white or black)($1 \leq i \leq w, 1 \leq j \leq h$).
Output: two random grid $R_1$ and $R_2$, $B[i, j] \in \{0, 1\}$ (transparent or opaque)($1 \leq i \leq w, 1 \leq j \leq h$) $k \in \{0, 1\}$.

(1)Algorithm 1
Step 1: Generate a random grid $R_1$, $T(R_1) = 1/2$
Step 2: Encryption process:
for ($B[i, j]$($1 \leq i \leq w, 1 \leq j \leq h$)) do

{}  
if ($B[i, j]$) = 0, $R_2[i, j]$ = $R_1[i, j]$
else $R_2[i, j]$ = $R_1[i, j]$

Step 3: Output ($R_1$, $R_2$)
(2)Algorithm 2
Step 1: Generate a random grid $R_1$, $T(R_1) = 1/2$
Step 2: Encryption process:
for ($B[i, j]$($1 \leq i \leq w, 1 \leq j \leq h$)) do

{}
if(B[i,j])=0, R_2[i,j]= R_1[i,j]
else R_2[i,j]= random_pixel(0,1)
}
Step 3: Output (R_1, R_2)

(3) Algorithm 3
Step 1: Generate a random grid R_1, T(R_1)=1/2
Step 2: Encryption process:
for (B[i,j](1≤ i≤ w,1≤ j≤ h)) do
{
  if (B[i,j])=0, R_2[i,j]= random_pixel(0,1)
  else R_2[i,j]= R_1[i,j]
}
Step 3: Output (R_1, R_2)

In the above algorithm steps, random_pixel(0,1) is a function that uses a tossing rule to implement a binary value, that is 0 or 1, respectively, representing transparent and opaque, while R_1[i,j] represents R_1[i,j] is reversed 0(1) represents a white (black) pixel in a binary image and a transparent (opaque) pixel in an encrypted map, both being interchangeable.

The area of all transparent and opaque pixels in B is denoted by B(0) or B(1) respectively, pixel b belongs to B(0) or B(1), so b=0 or b=1, where B = B(0)∩B(1) and B(0)UB(1)=∅. Let R[B(0)] and R[B(1)] respectively represent the pixel areas corresponding to B(0) and B(1) in the random grid R, that is, the pixel r belongs to R[B(0)] or R[B(1)], if and only if the corresponding pixel b of r belongs to B(0) or B(1). Here R= R[B(0)] U R[B(1)] and R[B(0)]∩R[B(1)]=∅.

2.2. MSCAN Image Encryption Algorithm
The modified SCAN, also known as MSCAN, is a SCAN encryption algorithm for binary images based on the SCAN mode. Its encryption process consists of encryption and 2DRE compression algorithms[5][7].

2.2.1. SCAN Mode Encryption Algorithm. the basic idea of SCAN algorithm encryption is to rearrange image pixels[4]. The rearrangement is done by the scan mode (key) that occurs in the encryption dedicated SCAN language.

The Scan language can be expressed in terms of syntax as:

\[ G = (Γ, Σ, A, ∩) \]  
(2)

Γ is a non-end symbol.
\[ Γ = \{A, S, P, U, V, T\} \]  
(3)

Σ is the ending symbol.
\[ Σ = \{c, d, o, s, r, a, e, m, y, B, Z, X, (, )\} \]  
(4)

A is the starting symbol and ∩ is the product rule, given by:
\[ A → S\]P  
(5)
\[ S → UT \]  
(6)
\[ P → VT (AAAA) \]  
(7)
The definition of the above encryption-specific SCAN language is as follows:
(1) A→S|P indicates processing of scan S or division of P.
(2) S→UT indicates that the scan area U and transform T scan the area.
(3) P→VT (AAAA) indicates the use of differentiation mode V and transformation of T-differentiated regions, and the application of A to process 4 sub-regions in a differentiation order.
(4) U→c|d|o|r|a|e|m|y|w|b|z|x with raster (r), continuous raster (c), diagonal (d), continuous vertical (o), right orthogonal (a), outward spiral (s), horizontal symmetry (m), diagonal parallel (e), diagonal symmetry (y), second diagonal (w), z (Z, zeta), block (b, block), or x-type (x, xi) scans, see figure 1.
(5) V→B|Z|X is to use B-type, Z-type or X-type patterns for differentiation, respectively, as shown in figure 2.
(6) T→0|1|2|3|4|5|6|7 indicates scanning or differentiation with one of 8 transformation.

For differentiation, these transformations are represented by figure 2, for scans, these transformations are defined for all scan modes, with 0 representing an identity transformation and 2 representing a clockwise rotation of 90°. For scanning modes c, o, s, a, e, m, y, w, b, and x, 4 indicates clockwise rotation by 180°, and 6 indicates clockwise rotation by 270°. For scanning modes r and z, 4 represents vertical reflection, and 6 represents vertical reflection after 90° clockwise rotation. For scanning mode d, 4 indicates horizontal reflection and 90° clockwise rotation, and 6 means that the vertical reflection and 180° clockwise rotates. For all scan modes, 1, 3, 5 and 7 are the opposite of the scan path 0, 2, 4 respectively.

Figure 1. Basic scan mode.

Figure 2. Differentiation modes and transformations.

For example, for a 16x16 pixel image, if the scan key B5 is considered (S2 Z0 (c5 b0 o0 s5) c4 d1), the key scan path is as shown in figure 3. According to the outermost layer of the key, it is known that B5 differentiation is used, and then the B5 differentiation order is divided into four sub-regions: S2,
Z0 (c5 b0 o0 s5), c4, and d1, and the second subregion is divided by Z0 and the four subregions are scanned by c5, b0, o0, and s5 respectively. The explanation is as follows:

(1) s2, s denotes the outer spiral (figure 1), 2 denotes the clockwise rotation of $90^\circ$, the result of which is shown in figure 4.

(2) c4, c denotes continuous grating (figure 1), 4 denotes clockwise rotation $180^\circ$, the result of which is shown in figure 5.

(3) c5, for all modes, 5 represents the opposite path from 4 and reverses c4 to get c5. The result is shown in figure 5.

(4) The paths of s4 and s5 are similar to those of c4 and c5. The results are shown in figure 6.

(5) d1, d represents the diagonal figure 1, d1 is the reverse scan of d0, and d0 is d, the result is shown in figure 7.

**Figure 3.** Scan key B5 (s2 Z0 (c5 b0 o0 s5) c4 d1) Path diagram.

**Figure 4.** From s to s2.

**Figure 5.** From c to c4 to c5.

**Figure 6.** From s to s4 to s5.
2.2.2. **DRE Compression Algorithm.** The 2DRE compression algorithm compresses the binary image with the segmented black or white pixel string according to the scanning order. First record the pixel values encountered by the scan, and the lengths of consecutive black or black pixel strings are stored in scan order.

In this algorithm, the largest element in the scan array is calculated, the first scan value of the scan array is stored, check if two consecutive pixels are equal and find the maximum length of the pixel string.

Assuming that a fixed-length binary is represented by L bits, the total number of bits required is equal to \((1+s)\times L\), where s represents the number of divided pixel strings. Thus, the compression ratio can be defined as:

\[
\text{compression} = \frac{R_0}{R_c}
\]  

(11)

In the formula, R0 is the total number of bits used before the image is compressed, and Rc is the total number of bits used after the image is compressed.

2.3. **Mscan Mode Encryption**

This article uses the modified SCAN mode encryption in the encryption process. Unlike the traditional encryption process, this encryption is mainly an encryption method for binary images[3].

2.3.1. **Quadtree representation of binary images.** When the entire image is black or white, the image is represented by the root node, and each cell is represented as 0 or 1, according to the gray or white of the image. The image is divided into 4 equal-sized sub-graphs, each of which All sizes are 4×4, which are labeled as nw (north-west), ne (north-east), sw (south-west), and se (south-east), respectively representing the northwest subgraph, the northeast subgraph, and the southwest subgraph and Southeast Subgraph. If there is only 0 or 1 in the subgraph, represent the leaf node with a black box or a white box and stop dividing. If it is not, continue to divide each subgraph according to the method until the subgraph is all 0 or all 1, which means that the leaf node of the quadtree is an outer node or a leaf node, and its gray node is called an inner node. Figure 8 shows the original image, and figure 9 shows the corresponding quadtree.

2.3.2. **Mscan Language.** This paper uses the quad \((V_N, V_T, P, S)\) to represent the MSCAN language for 2n x2n binary images. In the quad, S is the starting symbol, P is the generating rule set, VN is non-terminal symbol set, VT is a set of terminal symbol set, where \(V_N = \{S, U_{i=1}^{n} L_i\}, V_T = \{U_{i=1}^{n} R_j | 1 \leq j \leq 4^i\}\).
This dissertation uses Li to represent different scan pattern sets in the i-th layer of the quadtree, and \( R_j^i \) is one of the 24 scan patterns defined in figure 10. Each mode \( SP_k (0 \leq K \leq 23) \) is the kth scan mode of the 2x2 mode window.

![Figure 10. 24 scan modes.](image)

3. Encryption Algorithm Implementation

![Figure 11. Encryption system flow chart.](image)

(1) Assign the gray value of the specified position picture to the two-dimensional array \( P \).

(2) The two-dimensional matrix is encrypted to obtain an encryption matrix and assigned to the matrix \( E \). Generate a 256x256 image, display and save the image.

The pseudo code for the entire encryption system is as follows:

BEGIN:
(1) int[,] P = comm. get Pixel; Input an image and get the image matrix and image size
(2) comm. rand Pixel(N, rnd); Generate random grid 1
(3) comm. rand Pixel(N, rnd); Generate random grid 2
(4) Random Grids. RGen; Random grid encryption
(5) MSCAN. get key (); Get key k, random seed p, number of iterations m
(6) MSCAN.2dre (); 2DRE compression
(7) MSCAN. Enc(enIm, img, M); MSCAN encryption
(8) comm. show Image EE(); Process the encryption matrix and display the encrypted image
END

4. Image Encryption Test
In this paper, two methods of statistical analysis and diffusive test are used to test the performance of the algorithm. The statistical analysis methods are mainly histogram and variance.

The diffusivity test involves pixel change rate (NPCR) and uniform mean change intensity (UACI).

4.1. Statistical Analysis Methods
The variance indicates the degree of dispersion between the histogram and its average value. The degree of consistent distribution of the histogram can be measured by the variance. The smaller the variance value is, the more consistent the distribution of the histogram of the image to be detected is, the more resistance it can be to such a class plaintext attack.

Use hist(i=0,1,...,255) to represent the gray value of a pixel in a certain colour direction (that is, one of the three directions of RGB, the direction of the red component in this experiment), and the average value of all pixel gray values is represented by aver, equation 12 is used to calculate the variance of the gray value of the image.

$$s = \frac{1}{25} \sum_{i=0}^{255} (\text{hist}_i - \text{aver})^2$$

Among them, aver can be calculated by formula 13:

$$\text{aver} = \frac{1}{256} \sum_{i=0}^{255} \text{hist}_i$$

The histogram analysis of the original image and the corresponding histogram analysis of the encrypted graph are shown in figure.12 and figure.13.

![Figure 12. Original image and histogram](image1)
![Figure 13. Encryption map and histogram](image2)

It can be seen from the figure that the consistency of the original variance distribution is poor.

Compared with the original image, the consistency of the encrypted image has been improved to some extent.

4.2. Diffusion Test
The pixel change rate is used as an index of the diffusivity[8] test. The two encrypted images are represented by C1 and C2. The original image of the two pictures has only one pixel with different gray values. Let C1 and C2 have gray values at (i, j) as C1(i, j) and C2(i, j), which have the following definitions:

$$D(i, j) = \begin{cases} 0, & C_1(i, j) = C_2(i, j) \\ 1, & C_1(i, j) \neq C_2(i, j) \end{cases}$$
The pixel change rate (NPCR) is defined as:

\[
\text{NPCR} = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\%
\]  

(15)

In the equation, the width and height of \( C_1 \) and \( C_2 \) are denoted by \( M \) and \( N \) respectively, while NPCR represents the percentage of different pixels in the two encrypted images. In this test, the original image is encrypted to obtain the image \( C_1 \), and the value of the \([0, 0]\) position of the original image is reduced by 5 and then encrypted to get image \( C_2 \). After testing NPCR = 0.01220703125.

Consistent average change in intensity can be used as another indicator of a diffusivity test and is defined as follows:

\[
\text{UACI} = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C_1(i,j) - C_2(i,j)|}{255 \times M \times N} \times 100\%
\]  

(16)

In this test, the acquisition of images \( C_1, C_2 \) is the same as when calculating the pixel change rate. After testing, UACI = 6.58222273284314 \times 10^{-5} \%

After the diffusion test, the performance of this hybrid image encryption system is excellent. This article compares the NPCR and UACI of the other two encryption systems, as shown in table 1:

| Encryption system list                        | NPCR            | UACI            |
|----------------------------------------------|-----------------|-----------------|
| Cryptosystem based on random grid algorithm  | 1.53 e^{-5}     | 2.99e^{-4}      |
| MSCAN-based encryption system                | 4.58 e^{-5}     | 1.79e^{-7}      |
| Hybrid Encryption System in this article     | 1.22 e^{-4}     | 6.58 e^{-7}     |

As can be seen from the table, compared with the other two encryption methods, the NPCR and UACI of the encryption system in this article are at a relatively high level, and even an order of magnitude higher for NPCR, so the diffusion of this encryption system is stronger. When it comes to attacking poorly classified plaintext attacks, the encryption system of this article will show superior features.

5. Conclusion

This article is about the two encryption algorithms, namely the random lattice encryption algorithm and the modified SCAN encryption algorithm. On this basis, the two algorithms are implemented, modified and integrated with C# code to form a complete image encryption system. An encrypted image encryption system is evaluated and tested. According to the test results, the performance of the hybrid encryption system is significantly better than the other two encryption systems, and it has good resistance to plaintext attacks. At the same time, the 2DRE compression algorithm is used to improve the encryption effectiveness.

6. Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grants No. 61772125 and No. 61402097; and the Fundamental Research Funds for the Central Universities under Grant No. N151708005.

7. Reference

[1] Zhu Congxu, Hu Yuping, Sun Kehui J 2012 A New Image Encryption Algorithm Based on Hyperchaotic System and Ciphertext Diffusion in Crisscross Pattern Electronic and Information Institute, vol 34 pp 1735–1743.

[2] Kafri O, Keren E J 1987 Encryption of pictures and shapes by random grids Optics Letters vol 12 p 377.
[3] Chang C C and Yu T X J 2002 Cryptanalysis of an encryption scheme for binary images Pattern Recognition Letters vol 23 pp 1847–1852.

[4] Zhu Congxu, Liao Chunlong and Deng Xiaoheng J 2013 Breaking and improving an image encryption scheme based on total shuffling scheme Nonlinear Dynamics vol 71 pp 25–34.

[5] TAQUET J and LAB IT C J 2012 Hierarchical oriented predictions for resolution scalable lossless and near lossless compression of CT and MRI biomedical images IEEE Transactions on Image Processing vol 21 pp 2641 – 2652.

[6] Wang Yuanmei and Li Tan C 2010 Study on Image Encryption Algorithm Based on Arnold Transformation and Chaotic System Proc of 2010 Int. Conf. on Intelligent System Design and Engineering Application pp 449–451.

[7] DENGH, DENGJ and DENG X J 2013Joint compression and tree structure encryption algorithm based on EZW Acta Physica Sinica vol 62 p 110701.

[8] Benyamin Norouzi J 2014 A novel image encryption based on hash function with only two-round diffusion process Multimedia Systems vol 20 pp 45–64.

[9] C.N. Yang, C.C. Wu, and D. Wang 2014 "A Discussion on the Relationship between Probabilistic Visual Cryptography and Random Grid," Information Sciences vol 278 pp 141–173.

[10] X. Yan, X. Liu, and C.N. Yang 2018 "An enhanced threshold visual secret sharing based on random grids," Journal Real-Time Image Processing vol 14 pp 61–73.