Compression-aware and Hyperchaotic Dynamic Bit-level Image Encryption Algorithm

Cong Ma[1,a,*], Guodong Li[2]

[1]College of Transportation Management, Xinjiang Institute of Transportation Technology, Urumqi, Xinjiang, China

[2]School of Mathematical and Computational Sciences,Guilin University of Electronic Science and Technology, Guilin, Guangxi, China

[a]571849657@qq.com

*Corresponding author

Keywords: Bit-level Encryption, Compression-awareness, Rabinovich Hyperchaos, Ring Diffusion

Abstract: To address the problems of low real-time transmission and limited accuracy of traditional encryption algorithms, a compression-aware combined with Rabinovich hyperchaotic encryption algorithm is proposed. Firstly, the plaintext image is DWT transformed to obtain the sparse basis matrix, which makes the encryption and compression simultaneously; secondly, the double-disorder mechanism of the bit plane is designed with the help of the improved hyperchaotic sequence, and the encryption engine function is introduced to perform the circular diffusion operation on the image; finally, the joint random Gaussian measurement matrix is used to compressively perceive the encrypted image sampled to form the ciphertext image. Simulation experiments show that the algorithm achieves 99.57% and 33.41% NPCR and UACI, with large key space and high sensitivity, and is able to resist exhaustive attacks with high security.

1. Introduction

The rapid development of the information age has made the issue of security in electronic communication technology extremely important, and has also brought new challenges to confidential communication. Compression-awareness uses an observation matrix to project a high-dimensional signal onto a low-dimensional space, and reconstructs the original signal by solving an optimization problem[1,2]. Chaotic systems are characterized by high initial value sensitivity, high randomness, and the generated pseudo-random sequences are not easy to be broken, etc. Using chaos for confidential communication is now a very popular research topic[3]. xiong Li et al. proposed a chaos mapping-based remote authentication scheme for environmental security, which is applicable to telecare medicine and contributes to the development of clinical medicine[4]. usman Arshad et al. based on modern chaos science, proposed a fast computational and quantum encryption image encryption algorithm, which uses quantum rotation and rotation operators to encrypt compressed data[5]. In order to overcome the problems of low real-time and security of traditional encryption algorithm transmission, this paper proposes an encryption algorithm based on the combination of compression-awareness and hyperchaos to achieve simultaneous compression encryption, and designs a bit-level encryption algorithm to improve the degree of pixel dislocation, and verifies the security and effectiveness of the algorithm through simulation experiments.

2. Four-dimensional Rabinovich hyperchaotic system

A controlled four-dimensional hyperchaotic Rabinovich system is used, with the following kinetic equations[6].

Copyright © (2023) Francis Academic Press, UK DOI: 10.25236/icceme.2023.035

$$\begin{cases} \dot{x} = hy - ax + y \\ \dot{y} = hx - by - xz + w \\ \dot{z} = -dz + xy \\ \dot{w} = -ky - lw \end{cases} \tag{1}$$

where the system exhibits a chaotic state when the condition $a = 4, b = 1, d = 1, k = 1, l = 0$, $h \geq 2.05$ is satisfied.To further expand the key space and increase the pseudo-randomness of the chaotic sequence, the initial value of the Rabinovich hyperchaotic mapping is selected using a specific method.The one-dimensional logistic mapping with initial value k_1 and control parameter k_2 is iterated 100 times, and the four values x_1, x_2, x_3, x_4 corresponding to the k_3, k_4, k_5, k_6 position are selected within 100 times, and the Rabinovich hyperchaotic initial values are selected according to the rule of equation (2).

$$\begin{cases} x_0 = \mathrm{mod}(abs(x_1 \times 10^4), 2^8) / k_3 \\ y_0 = \mathrm{mod}(abs(x_2 \times 10^4), 2^8) / k_4 \\ z_0 = \mathrm{mod}(abs(x_3 \times 10^4), 2^8) / k_5 \\ w_0 = \mathrm{mod}(abs(x_4 \times 10^4), 2^8) / k_6 \end{cases} \tag{2}$$

Using x_0, y_0, z_0, w_0 as the initial value of the Rabinovich hyperchaotic mapping, the sequence values of its 1000 iterations were tested for randomness. According to the SP800-22 Revla test standard,The test results were 0.5714, 0.6211 and 0.6029 for TFMT, FTB and TRT, respectively, indicating that the chaotic sequences generated by the Rabinovich hyperchaotic system have strong randomness.

3. Design of the encryption algorithm

The specific steps of the encryption algorithm are as follows:

(1) Conversion: firstly, the color plaintext image is converted into a grayscale image, and the grayscale image of size $M \times N$ is sparse using the discrete wavelet transform DWT to obtain a coefficient matrix of $m \times n$.

(2) Bit plane decomposition: the 8 bit planes obtained by bit plane decomposition contain 0.39%, 0.78%, 1.57%, 3.14%, 6.28%, 12.55%, 25.1%, 50.2% of image information, the higher the bit level contains more image information, and the 8 bit planes are divided into 4 groups on average, which are recorded as $pic1$, $pic2$, $pic3$, $pic4$.

(3) Chaotic sequence generation: Given the initial key and the initial value of Rabinovich hyperchaos, the Runge-Kutta method is used to solve the equations and obtain four sets of random sequences. Four chaotic sequences of length s are intercepted and the first k_7 times are discarded respectively to eliminate the transient effect to obtain a new chaotic sequence l_1, l_2, l_3, l_4.

(4) Disorder: $pic1, pic2, pic3, pic4$ is divided into four blocks, the rules of blocking is uniform blocking, $pic1$ is represented by $A_1 - A_4$, $pic2$ is represented by $B_1 - B_4$, $pic3$ is represented by $C_1 - C_4$, $pic4$ is represented by $D_1 - D_4$, if it is not a square matrix, it is transformed into a square matrix by adding zero to the left or down, and the block is disordered according to the dislocation mechanism of formula (3), and the four bit planes obtained are noted as $pic1'', pic2'', pic3'', pic4''$.

$$
\begin{aligned}
&A_1 \to B_2 \to C_3 \to D_4 \to A_1 \\
&A_2 \to B_3 \to C_4 \to D_1 \to A_2 \\
&A_3 \to B_4 \to C_1 \to D_2 \to A_3 \\
&A_4 \to B_1 \to C_2 \to D_3 \to A_4
\end{aligned} \tag{3}
$$

In order to improve the dependence of the encryption algorithm on the plaintext image, the Zig-Zag transform is used to quadratically dislocate the four bit planes. The standard Zig-Zag dislocation rules are shown in Figure 1, and if the plaintext image is not a square matrix, the same way of adding 0 is used to transform it into a square matrix, and the final dislocation matrix obtained is $pic1', pic2', pic3', pic4'$ respectively.

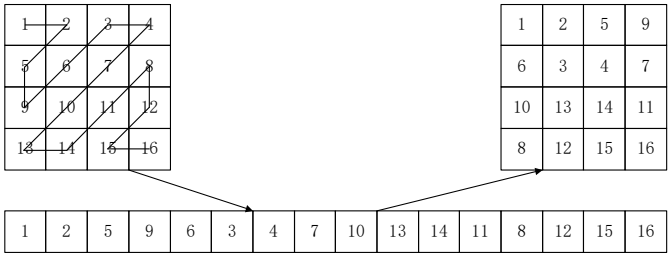

Figure 1 Zig-Zag disruption rules.

(5) Diffusion: construct two encryption engine functions kl_1, kl_2, based on the plaintext pixel values and the key stream l_1, l_2, l_3, l_4,

$$
\begin{aligned}
kl_1 &= \mathrm{mod}(I_{pic3}, 2) \\
kl_2 &= ceil\left(\frac{\mathrm{mod}(I_{pic4}, 256)}{m \times n}\right) + 1
\end{aligned} \tag{4}
$$

where I_{pic3} I_{pic4} is the sum of the pixel values of the permutation matrix $pic3'$ $pic4'$, respectively, and the permuted four ciphertext images are converted into a one-dimensional vector $L_i = \{L_1, L_2, \cdots, L_{m \times n}\}$. The circular diffusion function is designed according to the encryption engine kl_1, kl_2,Taking L_1 as an example.

$$
\begin{aligned}
L_a^{'} &= L_a \oplus L_{a+1} \oplus kl_1 \\
L_a^{''} &= L_a^{'} \oplus L_{a-1} \oplus kl_2
\end{aligned} \tag{5}
$$

where, $a = m \times n, m \times n\text{-}1, \cdots, 1$, the ciphertext function $L_a^{''}$ is converted into a $m \times n$ matrix noted as $L_1^{'}$. The same operation is performed on L_2, L_3, L_4 to finally obtain the diffusion matrix, i.e., the ciphertext image C'.

(6) Compression perception: the ciphertext matrix C' is sampled by compression perception using the random Gaussian measurement matrix Φ, $C = \Phi C'$ to obtain the final ciphertext image C.

(7) In order to achieve the purpose of fully confusing the encrypted image, the above steps (3) and (4) are repeated T times, and T is saved as the key to complete the encryption process.

4. Simulation experiments

The classical image of cryptography "Thinker" is selected as the experimental object, and the image resolution is 256*256, and MATLAB 2018b is used to simulate the algorithm of this paper, in which the system parameters of Rabinovich hyperchaos are set to $a = 4, b = 1, d = 1, k = 1, l = 0, h = 3$, the initial value is $x_0 = 1.51, y_0 = 2.37, z_0 = 3.45, w_0 = 3.7$, and the rest of the keys are $k_1 = 0.75, k_2 = 3$, $k_3 = 9, k_4 = 29, k_5 = 29$,

$k_6 = 29, k_7 = 500, T = 3, s = 100000$ except for the above key.The results of the simulation experiments are shown in Figure 2,They are plaintext image, ciphertext image and decrypted image respectively.

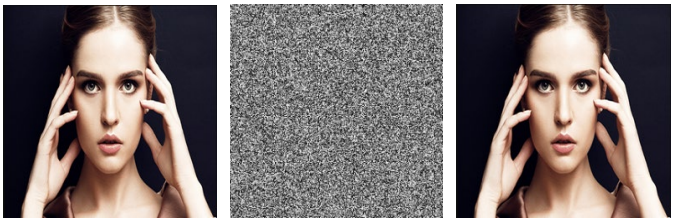

Figure 2 "Thinker" encryption effect.

5. Security Analysis

5.1. Histogram analysis

The histogram can visually show the resistance of the image to attack, the probability distribution of pixel values appearing in the plaintext image is uneven and easy to be attacked, while the probability distribution of pixel values in the ciphertext image is more uniform and it is difficult to find out the pattern of the original image, indicating that the encrypted ciphertext image has good resistance to exhaustive attack, and the results of the histogram analysis are shown in Figure 3.

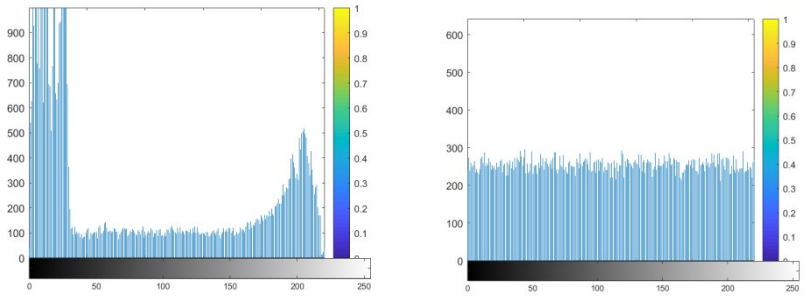

Figure 3 Histogram of plaintext and ciphertext images.

5.2. Key sensitivity analysis

The detection indicators of key sensitivity analysis are pixel change rate $NPCR$ and pixel normalized average change intensity $UACI$. When any pixel value in the plaintext changes slightly or the key makes a small change, it will drastically change the information of the ciphertext image. $NPCR$ shows the ratio of the number of different pixel points to all pixel points, when one pixel value in the plaintext changes the ratio of pixel value change in the ciphertext image, $NPCR$ the closer to 100%, $UACI$ shows the average of the ratio of the difference and the maximum difference between all the pixel points in the corresponding positions of the two images, and the ideal value of $UACI$ is close to 33.4635%. The calculation formula is as (6).

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\%$$
$$UACI = \frac{1}{M \times N} \times [\sum_{i}\sum_{j} \frac{D_1(i,j) - D_2(i,j)}{256}] \times 100\% \quad (6)$$

Where D_1 denotes ciphertext and D_2 denotes plaintext.The pixel value (101,100) of any point in the plaintext image is changed slightly to (101,101), at which time $NPCR$ and $UACI$ are 99.57% and 33.41%, respectively, both very close to the ideal value, comparing literature 8 and literature 9[8,9], the results are shown in Table 1.

Table 1 *NPCR* and *UACI* values.

	Algorithm of this paper	References[7]	References[8]
NPCR	0.9957	0.9946	0.9974
UACI	0.3341	0.3331	0.3356

5.3. Information entropy analysis

The information entropy responds to the degree of randomness of the sequence; the greater the information entropy, the greater the randomness and the more uniform the distribution of grayscale values, and vice versa, calculated as in (7)[9].

$$H(m) = -\sum_{i=1}^{255} p(m_i) \log_2 p(m_i) \tag{7}$$

The information entropy of an image is maximum when the probability of occurrence of each gray value in the image is equal, and the ideal value of information entropy of a gray image with 256 gray levels is 8. The information entropy of the algorithm in this paper is calculated to be 7.9987, which indicates that the probability of occurrence of each pixel value is very close and the gray values are evenly distributed, and also indicates that the algorithm has good resistance to attack and can resist exhaustive attacks, and the encryption effect is very good.

6. Conclusion

In this paper, we combine compression-aware and hyperchaotic systems for image encryption. The main features of the algorithm are: the plaintext image is first compressed and sampled to obtain the compressed matrix, a bit-plane decomposition and merging mechanism is designed, the four bit-planes are doubly dislocated using Rabinovich hyperchaotic operation to change the position of each pixel value, and further, the cryptographic engine function is added to perform circular diffusion to fully confuse the pixel values, and the resulting transition ciphertext matrix is combined with a random Gaussian matrix for compressed-aware sampling to obtain the final ciphertext image. The simulation experimental results show that the algorithm can well resist violent exhaustive attacks, has a large key space, high security of the encryption algorithm, solves the singularity of chaotic system encryption, improves the real-time encryption, and has a strong anti-cracking ability, which has a broad application prospect in network security.

Acknowledgements

This paper is one of the stage achievements of the project of Xinjiang Communications Vocational and Technical College "Research on Digital Image Encryption Algorithm Based on Compressed sensing and Chaotic System" (project number: J-21-12).

References

[1] Tiejun Li, Yue Sun, Weiren Shi, Guifang Shao, Jianjun Liu. Terahertz pulse imaging: A novel denoising method by combing the ant colony algorithm with the compressive sensing[J]. Open Physics, 2018,16(1).

[2] Shuyu Yao, Linfei Chen, Yuan Zhong. An encryption system for color image based on compressive sensing[J]. Optics and Laser Technology, 2019,120.

[3] Samar M. Ismail, Lobna A. Said, Ahmed G. Radwan, Ahmed H. Madian, Mohamed F. Abu-ElYazeed. A Novel Image Encryption System Merging Fractional-Order Edge Detection and Generalized Chaotic Maps[J]. Signal Processing, 2019.

[4] Xiong Li, Fan Wu, Muhammad Khurram Khan, Lili Xu, Jian Shen, Minho Jo. A secure chaotic map-based remote authentication scheme for telecare medicine information systems[J]. Future

Generation Computer Systems, 2018, 84.

[5] Usman Arshad, Syeda Iram Batool, Muhammad Amin. A Novel Image Encryption Scheme Based on Walsh Compressed Quantum Spinning Chaotic Lorenz System[J]. International Journal of Theoretical Physics, 2019, 58(10).

[6] Yongjian Liu. Hyperchaotic Systems of Controlled Rabinovich Systems[J]. Control Theory and Application, 2011, 28(11):1671-1678.

[7] Yicong Zhou, Weijia Cao. Image encryption using binary bitplane[J]. Signal Processing, 2014, 100(7): 197-207.

[8] Keya Hu. Image encryption based on block Compressed sensing and improved magic square transform[J]. Laser Technology, 2019,43(04):96-102.

[9] Kulkarni K, Lohit S, Turaga P, Kerviche R, Ashok A. ReconNet: Non-Iterative Reconstruction of Images from Compressively Sensed Measurements. 2016 IEEE Conference on Computer Vision and Pattern Recognition Las Vegas, USA, June 26–30, 2016 p449.