Image Encryption Algorithm Based on DNA Encoding and Hyperchaotic System (Postprint)

Authors: Zhang Xuncai, Liu Yishan, Cui Guangzhao

Date: 2018-05-02T00:00:00+00:00

Abstract

To address issues such as the limited diversity of DNA encoding rules and the low key sensitivity of chaotic encryption algorithms, an image encryption scheme based on DNA encoding and hyperchaotic systems is proposed. The algorithm first employs the SHA-3 algorithm to compute the hash value of the plaintext image, which is used as the initial value for the hyperchaotic system to enhance plaintext sensitivity. Secondly, the image is converted into DNA sequences and undergoes DNA sequence operations with the constructed S-box. Finally, the sequence generated by the hyperchaotic system is utilized to permute the image. Results and theoretical analysis demonstrate that the algorithm not only improves key sensitivity and the security of data transmission, but also exhibits robust resistance against brute-force attacks, statistical attacks, and differential attacks.

Full Text

Image Encryption Algorithm Based on DNA Encoding and Hyper-Chaotic System

Zhang Xuncai, Liu Yishan, Cui Guangzhao
(College of Electrical & Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)

Abstract: To address the issues of single DNA encoding rules and low key sensitivity in chaotic encryption algorithms, this paper proposes an image encryption scheme based on DNA encoding and hyper-chaotic systems. The algorithm first uses the SHA-3 algorithm to compute the hash value of the plaintext image, which serves as the initial value for the hyper-chaotic system to increase plaintext sensitivity. Next, the image is converted into DNA sequences and undergoes DNA sequence operations with constructed S-boxes. Finally, the image is scrambled using sequences generated by the hyper-chaotic system. Results

and theoretical analysis demonstrate that the algorithm not only improves key sensitivity and transmission data security, but also exhibits strong resistance against exhaustive attacks, statistical attacks, and differential attacks.

Key Words: image encryption; DNA encoding; hyper-chaotic system; S-box; SHA-3

0 Introduction

In recent years, image transmission has been widely used in medical imaging, online education, communications, and various other fields. However, the openness and sharing nature of networks pose significant threats to image transmission security. The 2013 "PRISM" incident made people realize that solving information security transmission problems is urgent. Image encryption technology is an effective solution for protecting image security during transmission. Due to characteristics such as high redundancy, large data capacity, and strong correlation between pixels, image encryption requires fast algorithms. Traditional encryption methods such as DES, AES, and RSA can no longer meet current image encryption requirements.

In recent years, scholars have proposed new image encryption algorithms, such as chaos-based image encryption methods and DNA sequence-based image encryption methods. Chaos systems exhibit excellent pseudo-random characteristics, orbit unpredictability, and sensitivity to initial states and control parameters—features that align well with many cryptography requirements. Because of the close relationship between chaos and cryptography, chaotic cryptography has been extensively studied and applied to image encryption. However, low-dimensional chaotic systems produce chaos that is only predictable in the short term, often with poor randomness in chaotic sequences, small key spaces, low security performance, and vulnerability to cryptanalysis. To expand the key space and increase the randomness of chaotic sequences, researchers have designed image encryption algorithms based on hyper-chaos and multi-level chaos. Currently, hyper-chaos has been widely applied in nonlinear circuits, secure communications, lasers, neural networks, and biological systems. However, with the improvement of cryptanalysis technology, hyper-chaotic encryption technology has also revealed issues such as low sensitivity to keys.

The inherent ultra-large-scale parallelism, ultra-low energy consumption, and ultra-high storage density of DNA molecules give DNA computing-based image encryption algorithms unique advantages that traditional cryptographic algorithms do not possess. Because biological experiments are costly, Ning et al. proposed a pseudo-DNA encryption method that simulates information encryption on electronic computers using basic concepts from DNA computing, though this method is not particularly suitable for image encryption. In 2010, Xue et al. proposed an encryption method combining DNA encoding with chaotic sequences, which provided good encryption effects using the sensitivity to initial conditions and high randomness of chaotic systems. However, subsequent research

identified vulnerabilities in DNA chaotic image encryption algorithms that use fixed encoding and single operation rules, making them susceptible to chosen-plaintext attacks. Other researchers have proposed improved image encryption algorithms based on encoding and multi-chaotic maps, using hyper-chaotic systems to scramble pixel positions and values, performing pseudo-DNA operations with DNA encoding rules, and finally obtaining encrypted images through DNA decoding. Recent studies have pointed out that current encryption algorithms for true-color images based on DNA encoding and chaos theory exhibit vulnerabilities to plaintext attacks and have shortcomings such as low sensitivity to plaintext and keys.

Therefore, this paper combines hyper-chaotic systems, DNA computing, and hash functions to perform block encryption on images. The SHA-3 hash function processes the original image to obtain initial values for the hyper-chaotic system and an image matrix for XOR operations with the original image, linking the original image information with key acquisition. The hyper-chaotic system then generates hyper-chaotic sequence values to construct S-boxes, which are used for addition, subtraction, and shift operations on the image. This algorithm can effectively improve key sensitivity and transmission data security, resist known-plaintext and chosen-plaintext attacks, and demonstrate strong resistance against exhaustive attacks, statistical attacks, and differential attacks.

1.2 DNA Encoding and Operations

1) DNA Encoding

DNA is a high-molecular polymer with deoxyribonucleic acid as its basic unit. A deoxynucleotide consists of three components: a phosphate molecule, a deoxyribose sugar molecule, and a nitrogenous base. There are four types of nitrogenous bases: adenine (A), cytosine (C), guanine (G), and thymine (T), where A and T, G and C are complementary pairs. Each pixel in a grayscale image can be represented by an 8-bit binary number, and in binary, 0 and 1 are complementary. Therefore, if the four deoxynucleotides A, T, C, and G represent the binary numbers 00, 11, 01, and 10 respectively, each pixel value can be represented by a DNA sequence of length 4. For example, the decimal value 200, expressed as (11001000) , would be converted to the 4-base DNA sequence TAGA.

There are eight encoding rules that satisfy the complementary relationship between DNA bases, as shown in Table 1 .

2) DNA Sequence Operations

DNA sequence addition and subtraction are similar to traditional algebraic calculations. When using 00-A, 11-T, 01-C, 10-G for encoding, the addition and subtraction operation rules between bases are as shown in Table 2 .

2 Scheme Design

Image encryption is achieved through confusion and scrambling using hyper-chaotic systems, DNA encoding, and hash functions.

In 2005, literature [29] provided a detailed description of the hyper-chaotic Lü system:

$$\begin{cases} \dot{x} = a(y - x) + uy \\ \dot{y} = -xz + cy \\ \dot{z} = xy - bz \\ \dot{u} = xz + du \end{cases}$$

where parameters a, b, c are the Lü system parameters, parameter d is a 待定 control gain parameter, and x, y, z, u are variables. When $a = 36$, $b = 3$, $c = 20$, and $-0.35 < d \leq 1.3$, the system exhibits hyper-chaotic behavior.

For an original grayscale image of size $L \times L$ (here defaulting to square images; if the encrypted image is not square, padding is applied according to rules described later), the main diagonal is defined as diag(0). Lines parallel to the main diagonal above it are sequentially defined as diag(-1), diag(-2), ···, diag(-L+1). Lines below the main diagonal are defined as diag(1), diag(2), ···, diag(L-1). The definition method is shown in Figure 1 [Figure 1: see original paper].

To achieve scrambling effects, this paper recomposes pixel positions. The rule for extracting pixels from the image is as follows:

$$X_i = \text{diag}(i) + \text{diag}(-L + i)$$

where $i = 0, 1, 2, ..., L - 1$.

Example: When $i = 0$, $X_0 = \text{diag}(0) + \text{diag}(-L) = \text{diag}(0)$; when $i = 1$, $X_1 = \text{diag}(1) + \text{diag}(-L + 1)$.

Using this method, the L elements extracted each time are converted into $L \times L$ image submatrices, yielding L image submatrices of size $L \times L$.

2.2 SHA-3 Algorithm

The SHA-3 algorithm is based on the sponge structure and is one of the most fundamental modules in modern cryptography. It takes a message of arbitrary length as input and generates a fixed-length HASH value. A key generated from the hash value will produce a completely different encryption key even if the original image has an extremely tiny change. Therefore, this encryption method can effectively resist brute-force attacks.

After the original image is transformed by SHA-3, it produces a 256-bit hash value: `dbbf374d57de108723c923b41d768d018c8e538a2de7479962c487a0335e1e85`.

The generated hash value is used as input information for the next hash function to produce a new hash value. This cycle repeats eight times, yielding a total of 256×8 bits of hash value. A DNA encoding rule is selected to encode the obtained hash value, with every 8 bits of hash value forming a group for encoding. For example, `db` $\rightarrow$ `11011011` $\rightarrow$ `TCGT`.

2.4 S-box Construction

Setting the control parameters of the hyper-chaotic Lü system as $a = 36$, $b = 3$, $c = 20$, $d = 1$, and using the initial values obtained in Section 2.3, the hyper-chaotic Lü system generates four groups of hyper-chaotic sequences to construct S-boxes. The steps are as follows:

a) Construct an empty sequence M.

b) Divide the interval $[0, 256]$ into 256 sub-intervals $[(0, 1), ..., (j, j + 1), ..., (255, 256)]$, denoted by T_j for $j = (0, 1, 2, ..., 255)$, as shown in Figure 2 [Figure 2: see original paper].

c) Iterate the hyper-chaotic Lü system i times to obtain state values x_i, y_i, z_i, and u_i. Preprocess the generated chaotic sequences using equations (7)-(10) to obtain final values:

$$f(x_i) = \mathrm{mod}(x(i)\times 1000, 255) f(y_i) = \mathrm{mod}(y(i)\times 1000, 255) f(z_i) = \mathrm{mod}(z(i)\times 1000, 255) f(u_i) = \mathrm{mod}(u(i)\times 1000$$

d) If $f(x_i)$ falls in the j-th sub-interval $(j, j + 1)$, and j does not exist in sequence M, then add j to sequence M. The same applies to other sequences.

e) If the number of elements in sequence M is less than 256, continue steps c) and d) until sequence M contains 256 elements.

f) Convert the 256 elements in sequence M into a 16×16 matrix to obtain an S-box. Construct 16 S-boxes of size 16×16 using this method and encode them sequentially. For example, a value 233.6 generated by iterating the hyper-chaotic Lü system with initial values falls in the sub-interval 233-234, belonging to T_{233}. If 233 is not in sequence M, add this value to sequence M and perform DNA encoding.

2.5 Encryption Scheme

The main content of this encryption algorithm is as follows: first, the original image is divided into L sub-image matrices according to the extraction rule shown in Section 2.1. Second, the hash values generated by the SHA-3 algorithm are encoded and undergo DNA encoding operations with the DNA-encoded sub-image matrices. Finally, S-boxes constructed from sequence values generated by the hyper-chaotic Lü system are used to perform substitution and scrambling

operations on the image. The encryption flow is shown in Figure 3 [Figure 3: see original paper]. The specific steps are:

a) Input an 8-bit grayscale image $I(m, n)$. Pad the image according to the following rule to obtain image $I'(L, L)$:

b) Convert the image into L submatrices of size $L \times L$ using the method shown in Section 2.1.

c) Perform DNA encoding on each element of the image submatrices.

d) Using the 16×16 DNA-encoded matrix obtained in Section 2.2, perform DNA sequence operations with the L image submatrices from step c) according to the rules in Table 2 .

e) Perform DNA encoding operations between the 16 S-boxes constructed in Section 2.4 and the L image submatrices from step d) according to the rules in Table 2 . Then apply a left circular shift of 3 bits to each of the L image submatrices (based on extensive experiments, shifting by 3 bits yields the best effect).

f) Extract the odd positions from the first half of hyper-chaotic sequences $f(x_i)$ and $f(y_i)$ and add them together; extract the even positions from the first half of sequences $f(z_i)$ and $f(u_i)$ and add them together to form a new chaotic sequence G. Take this sequence modulo 256, sequentially extract L numbers from this sequence to form L groups $G_1, G_2, ..., G_L$. Convert each group of L numbers into an $L \times L$ matrix, transform the L matrices into binary, select a DNA encoding rule for encoding, and perform DNA encoding operations with the L image submatrices from step e) according to the DNA encoding operation rules in Table 2 .

g) Combine the L image submatrices from step f) into a single image matrix I_1.

h) Generate matrix C using equation (12) and perform DNA sequence operations between matrix I_1 and C according to the rules in Table 2 to obtain image matrix I_2.

$$C = L \times L \times (x(L + j) + 0.5) \times \text{ones}(L, 1)$$

where $j = 1, 2, 3, ..., 256$.

i) Extract the even positions from the first half of hyper-chaotic sequences $f(x_i)$ and $f(y_i)$ and add them together; extract the odd positions from the first half of sequences $f(z_i)$ and $f(u_i)$ and add them together to form a new chaotic sequence G_0. Arrange in ascending order to obtain a new sequence, replace each element in the original sequence with its position value to get the new sequence index, and use this index to scramble image matrix I_2 to obtain image I_3.

j) Perform DNA decoding on image I_3 to obtain the encrypted image I_4.

The decryption algorithm is the inverse process of the encryption algorithm and will not be detailed here.

3 Simulation Experiment

The proposed algorithm was simulated in MATLAB 7.1. The original image used was the standard 256×256 Lena grayscale image. Under the condition $x_0 = 1$, the experimental results are shown in Figure 4 [Figure 4: see original paper].

4 Security Analysis

The security analysis of the algorithm mainly includes key space, sensitivity analysis, and resistance to statistical attacks.

4.1 Exhaustive Attack Analysis

1) Key Space Analysis In this algorithm, the key includes: x_1, y_1, z_1, u_1 and 256 bytes from the SHA-3 function. If the computational precision of x_1, y_1, z_1, u_1 is 10^{14}, the key space of the Lü system is $10^{14} \times 10^{14} \times 10^{14} \times 10^{14} = 10^{56}$. The key space of SHA-3 is 2^{128}. The total key space is $10^{56} \times 2^{128} \approx 3.4 \times 10^{94}$, demonstrating that the algorithm has a sufficiently large key space to resist exhaustive attacks.

2) Key Sensitivity Analysis To test key sensitivity, decryption was performed with slightly different keys. Figure 5 Figure 5: see original paper shows the decrypted image with $x_1 = 3$ while other keys remain unchanged; (b)-(d) show decrypted images with $y_1 = 10$, $z_1 = 30$, and $u_1 = 2$ respectively, with other keys unchanged. Even a small difference in the key prevents correct decryption of the original image, and the incorrectly decrypted image reveals no information about the original image. Therefore, the algorithm exhibits key sensitivity and can effectively resist brute-force attacks.

4.2 Statistical Attack Analysis

1) Histogram Analysis Statistical analysis was performed on the original and encrypted images to analyze their statistical characteristics. Figure 6 Figure 6: see original paper shows the histogram of the original image, and (b) shows the histogram of the encrypted image. The pixel values of the original image are relatively concentrated, while the histogram of the encrypted image is essentially uniform, making it difficult for attackers to restore the original image using statistical characteristics of pixel gray values. This demonstrates that the algorithm has excellent resistance to statistical analysis.

2) Correlation Analysis 2,500 pairs of adjacent pixels were randomly selected from the original and encrypted images in horizontal, vertical, and diagonal directions. The correlation between pixels was calculated using equations (13)-(16):

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))r_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\times D(y)}}$$

where x and y are the gray values of adjacent pixels in the image; $\mathrm{cov}(x,y)$ is the covariance; $D(x)$ is the variance; and $E(x)$ is the mean. The results are shown in Table 3 . Figure 7 [Figure 7: see original paper] shows the correlation of adjacent pixels in the original and encrypted images in horizontal, vertical, and diagonal directions. The correlation coefficient of adjacent pixels in the encrypted image is -0.0005348, indicating that the image encryption algorithm has strong resistance to statistical attacks.

3) Information Entropy Information entropy is defined to describe the degree of uncertainty in a system and can be used to represent the uncertainty of image information. The more uniform the distribution of image gray values, the greater the information entropy. The formula is:

$$H(m) = \sum_{i=0}^{2^t-1} P(m_i)\log_2 \frac{1}{P(m_i)}$$

where $P(m_i)$ is the probability of information m_i occurring. For grayscale images, information m has 256 states ranging from 0 to 255. An ideal random image has an information entropy value of 8. The experimental information entropy is 7.9897, indicating that the encryption algorithm has high security.

4.3 Differential Attack Analysis

Differential attack refers to an attacker making slight changes to the plaintext and comparing the differences in the corresponding ciphertext to find the relationship between the plaintext and ciphertext images. The NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) metrics are typically used to evaluate an image encryption scheme' s resistance to differential attacks. NPCR and UACI are calculated using the following formulas:

$$\mathrm{NPCR} = \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)\times 100\% \mathrm{UACI} = \frac{1}{M\times N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|P_1(i,j) - P_2(i,j)|}{255}\right]\times 100\%$$

where M and N represent the image length and width; $P_1(i,j)$ and $P_2(i,j)$ represent the corresponding ciphertext pixel values before and after plaintext change. An NPCR value closer to 100% indicates higher sensitivity of the image encryption scheme to plaintext and stronger resistance to differential attacks. The ideal UACI value is 33%, and values closer to this ideal indicate stronger resistance to differential attacks.

By changing a single pixel value in the plaintext image—for example, changing the pixel value at position (7,8) from 128 to 30—the calculated values are NPCR = 99.5956% and UACI = 33.39%. The NPCR is close to 100%, and the UACI value is also close to 33%, verifying that the image encryption scheme can resist differential attacks.

5 Conclusion

This paper proposes an image encryption algorithm based on the combination of DNA encoding and hyper-chaos. The algorithm adopts DNA encoding rules and uses the SHA-3 algorithm to increase the key space. The hyper-chaotic sequence increases the complexity and unpredictability of the ciphertext. Finally, the use of S-boxes provides dual security for the algorithm. Experimental analysis shows that the algorithm not only achieves good encryption effects and high key sensitivity, but can also effectively resist exhaustive attacks, statistical attacks, and differential attacks.

References

[1] Zhu Shuqin, Li Junqing, Wang Wenhong. Security analysis of improved image encryption algorithm based on DNA encoding and chaos [J]. Computer Applications Research, 2017, 34(10): 3090-3093.

[2] Van Droogenbroeck M. Partial encryption of images for real-time applications [C]// Proc of the 4th IEEE Signal Processing Symposium. 2004.

[3] Seripeariu L, Frunza M D. A new image encryption algorithm based on invertible functions defined on galois fields [C]// Proc of IEEE International Symposium on Signals, Circuits and Systems. 2005: 243-246.

[4] Chen R J, Lai Y T, Lai J L. Architecture design of the re-configurable 2-D von neumann cellular automata for image encryption application [C]// Proc of IEEE International Symposium on Circuits and Systems. 2005: 3059-3062.

[5] Zhen W, Xia H, Yuxia L, et al. A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system [J]. Chinese Physics B, 2013, 22(1).

[6] Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos [J]. Signal Processing, 2012, 92(4): 1101-1108.

[7] Guesmi R, Farah M A B, Kachouri A, et al. A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2 [J]. Nonlinear Dynamics, 2016, 83(3): 1123-1136.

[8] Wang X, Wang X, Zhao J. Chaotic encryption algorithm based on alternant of stream cipher and block cipher [J]. Nonlinear Dynamics, 2011, 63: 587-597.

[9] Wei X, Guo L, Zhang Q, et al. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system [J]. Journal of Systems and Software, 2012, 85(2): 290-299.

[10] Zhang Y, Tang Y. A plaintext-related image encryption algorithm based on chaos [J]. Multimedia Tools and Applications, 2017: 1-23.

[11] Akhavan A, Samsudin A, Akhshani A. Cryptanalysis of an image encryption algorithm based on DNA encoding [J]. Optics & Laser Technology, 2017, 95: 94-99.

[12] Alvarez G, Montoya F, Romera M, et al. Cryptanalysis of an ergodic chaotic cipher [J]. Physics Letters A, 2003, 311(2): 172-179.

[13] Elnashaie S, Abashar M E. On the chaotic behaviour of forced fluidized bed catalytic reactors [J]. Chaos, Solitons & Fractals, 1995, 5(5): 797-831.

[14] Liu W, Sun K, Zhu C. A fast image encryption algorithm based on chaotic map [J]. Optics & Lasers in Engineering, 2016, 84: 26-36.

[15] Zhu Congxu, Hu Yuping, Sun Kehui. A new image encryption algorithm based on hyper-chaotic system and ciphertext interleaved diffusion [J]. Journal of Electronics & Information Technology, 2012, 34(7): 1735-1743.

[16] Gao Tiegang, Chen Zengqiang. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372(4): 394-400.

[17] Kumar M, Iqbal A, Kumar P. A new RGB image encryption algorithm based on DNA encoding and elliptic curve diffie–Hellman cryptography [J]. Signal Processing, 2016, 125: 187-202.

[18] Zhou C, Wei X, Zhang Q, et al. DNA sequence splicing with chaotic maps for image encryption [J]. Journal of Computational and Theoretical Nanoscience, 2010, 7(10): 1904-1910.

[19] Wang Q, Zhang Q, Wei X. Image encryption algorithm based on DNA biological properties and chaotic systems [C]// Proc of the 15th International Conference on Bio-Inspired Computing: Theories and Applications (BIC-TA). 2010: 132-136.

[20] Adleman L. Molecular computation of solutions to combinatorial problems [J]. Science, 1994, 266(5187): 1020-1024.

[21] Tian Haibing, Lei Peng, Wang Yong. Image encryption algorithm based on chaos and DNA dynamic encoding [J]. Journal of Jilin University: Engineering and Technology Edition, 2014, 44(3): 801-806.

[22] Tu Zhengwu, Jin Cong. Color image encryption algorithm based on DNA sequence [J]. Computer Engineering and Science, 2015, 37(10): 1933-1939.

[23] Özkaynak F, Yavuz S. Analysis and improvement of a novel image encryption algorithm based on DNA sequence operation and hyper-chaotic system [J]. Nonlinear Dynamics, 2014, 78(2): 1311-1320.

[24] Özkaynak F, Özer A B, Yavuz S. Security analysis of an image encryption algorithm based on chaos and DNA encoding [C]// Proc of the 21st Signal Processing and Communications Applications Conference. 2013: 1-4.

[25] Zhang Q, Liu L, Wei X. Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps [J]. AEU-International Journal of Electronics and Communications, 2014, 68(3): 186-192.

[26] Kong L, Li L. A new image encryption algorithm based on chaos [C]// Proc of the 35th Chinese Control Conference. 2016: 4932-4937.

[27] Liu Y, Tang J, Xie T. Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map [J]. Optics & Laser Technology, 2014, 60: 111-115.

[28] Liu Jinmei, Qiu Shuisheng, Liu Weiping. Security analysis of image encryption algorithm based on hyper-chaotic system [J]. Computer Applications Research, 2010, 27(3): 1042-1044.

[29] Chen A, Lu J, Lu J, et al. Generating hyperchaotic Lü attractor via state feedback control [J]. Physica A-statistical Mechanics and Its Applications, 2006, 364: 103-110.

[30] Shiu H, Ng K, Fang J, et al. Data hiding methods based upon DNA sequences [J]. Information Sciences, 2010, 180(11): 2196-2208.

[31] Enayatifar R, Sadaei H J, Abdullah A H, et al. A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata [J]. Optics and Lasers in Engineering, 2015, 71: 33-41.

Note: Figure translations are in progress. See original paper for figures.