Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 14, no. 8, August 2018, pp. 1804-1814
DOI: 10.23940/ijpe.18.08.p17.18041814

Image Encryption Method based on Hill Matrix and Dynamic DNA Encoding

Xuncai Zhang, Zheng Zhou, Yishan Liu, Guangzhao Cui, Ying Niu*, and Yanfeng Wang

School of Electrical and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou, 450002, China

Abstract

Based on Hill matrix and dynamic DNA encoding, an image encryption method is proposed. First, this method combines an elliptic curve with a hyper-chaos sequence to fabricate the Hill cipher matrix, and the plaintext image is permuted and encrypted. Second, the dynamic DNA encoding technique is applied to diffuse the gray values of this plaintext image. Finally, hyper-chaos sequences are employed to complete the confusion and diffusion of the image. The experimental results show that the presented method can not only defend against brute-force attacks and statistical attacks but also resist plaintext attacks; in addition, the method has the merits of fast encryption speed, good encryption effects, and easy implementation.

Keywords: encryption method; DNA coding; hHill matrix; hyper-chaos system; elliptic curve

(Submitted on May 6, 2018; Revised on June 19, 2018; Accepted on July 21, 2018)

1. Introduction

Digital images are a common information communication method because of their features, including intuitiveness, ease of recognition, vividness, high redundancy, and ability to convey a large amount of data. Digital images are vulnerable to attacks from unauthorized network transmissions, so encryption technology is utilized to guarantee the reliability of information transmissions. Some conventional encryption algorithms such as RC4 and Blowfish do not take into account the strong correlation between pixels in the digital image itself. Therefore, these image encryption methods have many problems such as low encryption intensity or excessively long encryption time. Therefore, finding new image encryption methods is currently a popular research topic.

A hyper-chaos system has a multitude of properties, such as unpredictable orbit and sensitivity to initial state and control parameters. Hyper-chaotic sequences have a series of advantages, such as a long prediction period, good randomness, large key space, high-security performance, and difficulty with cracking [1-2]. DNA molecules have advantages of ultra-large parallelism and ultra-high storage space. The combination of hyper-chaotic sequences and DNA encoding can solve the shortcomings of the singleness of DNA encoding and make up for the low sensitivity of the hyper-chaos sequence to the key. In literature [3], an encryption scheme based on hyper-chaotic and dynamic DNA coding is introduced that adds DNA coding rules. However, this algorithm has only one kind of DNA operation in the encryption process and has a single calculation rule. Literature [4] demonstrates that the hyper-chaos encryption algorithm using fixed coding and single-operation rules is likely to crack by a plaintext attack. Other research [5-6] put forward an encryption method based on DNA encoding and multiple chaos maps, where a hyper-chaos system is introduced to confuse the pixel values, and the DNA encoding rules are exploited to conduct the pseudo-DNA manipulation; in addition, the ciphered image is finally gained by DNA decoding. Although DNA encoding and hyper-chaotic Chen system provide good encryption, they do not fully show forward-secrecy because of their symmetric properties. To address these problems, some scholars have proposed using public key cryptography to make up for the lack of effective key management for symmetric cryptography.

* Corresponding author.
E-mail address: niuying@zzuli.edu.cn

At present, there exist two kinds of encryption technologies: symmetric encryption and asymmetric encryption. Asymmetric encryption is suitable for multiple users to communicate securely in public networks. Applications of public key cryptography mainly include RSA cryptosystem, ElGamal cryptosystem, and elliptic curve cryptosystem. Because the elliptic curve cryptosystem (ECC) [7] is under the same security intensity, it has the advantages of a short key, flexible parameter selection, high-security, and fast encryption, and it is widely used in security authentication, digital signature, and data security transmission systems [8]. One study proposed an algorithm to embed image data into an elliptical curve with the features of an image. After processing, the image can still be restored according to the elliptic curve point group operation. Another study [9] proposed to encrypt the pixel values of digital images; the disadvantage is that the encryption and decryption processes take more time. A third study [10] proposed a block-image method based on ECC that divides the scrambled matrix into the image elements and then performs the elliptic encryption transformation; however, the pixel quality of block pixels in the process of sending is higher, and the encryption and decryption processes are complicated. Another analysis [11] used the characteristics of the image itself and combined the encryption algorithm of the elliptic curve to apply the elliptic curve public key cryptography to digital image encryption. However, the algorithm will take a long time to encrypt and decrypt. In an article [12], DNA computing and ECC were used to encrypt the RGB images. However, the sensitivity of the algorithm to the parameters was not high. Bibhudendra et al. proposed to construct a self-inverse matrix [13-14] to encrypt the information to overcome the weakness of the inverses of the encrypt matrix. Since the construction of the inverse matrix adopts pseudo-random numbers and the elements are strongly correlated, it is easy to crack. In literature [15], chaotic sequences are used to construct the encryption matrix, but the encryption method is relatively simple. Other research [16] suggests constructing the Hill encryption matrix by an elliptic curve, but the algorithm is too complex.

As described in this method, the technology of a hyper-chaos system and an elliptic curve is utilized to construct the encryption matrix to permute and encrypt the plaintext, avoiding the strong correlation between elements and the complexity and difficulty of elliptic curve encryption. Then, the encoding rules are randomly selected according to the different position of the pixels, and the pixels are encoded by DNA. Finally, the hyper-chaos sequence is used to scramble the plaintext. The merit of the method is that it raises the sensitivity of the key, effectively resisting known and chosen plaintext attacks and having a preferable capacity to anti-brute force attacks and defend against differential attacks.

2. Hyper-Chaotic System and DNA Encoding Rules

2.1. Hyper-Chaos Lorenz System

In 1963, Lorenz obtained a series of basic features of chaotic motion by observing a large number of atmospheric phenomena and conducting numerical experiments and theoretical analysis. The first singular attractor-Lorenz attractor was proposed. Lorenz simulated a fourth-order differential equation by computer. The weather model described found that under certain conditions, the same system can exhibit acyclic irregular behaviour. Lorenz revealed the basic characteristics of a series of chaotic motions, which became the cornerstone and starting point of future generations of chaos theory. It is of great significance in secret communication. The mathematical expression of the hyper-chaos Lorenz system [17] is described as follows:

$$\begin{cases} \dot{x} = \alpha(y - x) + u \\ \dot{y} = \gamma x - y - xz \\ \dot{z} = xy - \beta z \\ \dot{w} = -yz + \delta u \end{cases} \tag{1}$$

Where α, β, γ, and δ are system parameters and x, y, z, and u are state variables, When α=10, β=8/3, γ=28 and δ=-1, the system is in hyper-chaos state, and four chaotic sequences are generated. The four Lyapunov exponents of the formula (1) are: λ_1=-15.1752, λ_2=0, λ_3=0.1586, λ_4=0.3381. Because the hyper-chaotic system has two positive Lyapunov exponents, the computational speed of the hyper-chaos system is faster than that of the normal chaotic system. Therefore, it is more secure to design cryptographic algorithms.

2.2. DNA Encoding and Sequence Operations

2.2.1. Dynamic DNA Encoding

A DNA sequence is made up of four nitrogenous bases [18], that is to say, adenine (A), cytosine (C), guanine (G) and thymine (T) [19]. The well-known Watson-Crick base pairing rule states that A complements with T, and G complements with C [20]. When 0 and 1 are two mutually complementary relationships, 00 and 11, 01 and 10 are two mutually

complementary relationships, respectively. The pixel value is expressed by an 8-bit binary digit. Under the circumstance, there are eight coding rules that meet the base pairing rules, as shown in Table 1. The pixel value of a grayscale image is between 0 and 255, so it is described as an 8-bit binary digit or a 4-bit DNA encoding. For example, the decimal number 133 as an 8-bit binary number is 10000101, with rule 3 encoding as ACTT and rule 8 decoding as 11100000. The information can be encrypted only by the difference of encoding and decoding methods.

Table 1. 8 Encoding rules

Rule	1	2	3	4	5	6	7	8
00	A	C	C	A	T	G	G	T
01	G	A	T	C	C	A	T	G
11	T	G	G	T	A	C	C	A
10	C	T	A	G	G	T	A	C

For the given image $I(m, n)$, the DNA encoding rule is chosen as shown in formulas (2) or (3):

$$r_{i,j} = \left(round\left(mod\left((i+j), 8\right)\right) + 1\right) \tag{2}$$

$$r'_{i,j} = \left(round\left(mod(i \times j, 8)\right) + 1\right) \tag{3}$$

Where i and j represent the row and column of the pixel, $i \in \{1, 2, \cdots, m\}$, and $j \in \{1, 2, \cdots, n\}$, $P(i, j)$ in the matrix, respectively. The encoding rules are selected according to the pixel position, which increases the diversity of coding rules.

2.2.2. DNA Encoding Operations

The DNA subtraction and addition operation rules are similar to a conventional algebraic computation. The definition of rules between bases is defined as shown in Table 2.

Table 2. DNA subtraction and addition operation rules

-	A	G	C	T	+	A	G	C	T
A	A	T	C	G	A	A	G	C	T
G	G	A	T	C	G	G	C	T	A
C	C	G	A	T	C	C	T	A	G
T	T	C	G	A	T	T	A	G	C

3. Scheme Design

The Hill encryption matrix is constructed by combining a hyper-chaos system and elliptic curve, and the image is replaced and encrypted. Next, the dynamic DNA encoding and hyper-chaotic sequence operations are utilized to realize the confusion and scrambling of the image.

3.1. The Key Generation of Hyper-Chaos System

The SHA-3 function is also called the hash function [21], which is the most basic components in modern cryptosystem, and the input data is variable length and the output is fixed length. Messages can be generated with hash functions to generate a message digest that is appended to a message or stored with a message to prevent the message from being tampered with in transit and storage. The hash value of two images is completely different even if only one bit is different. Using this feature, a new sequence is generated with a set key and a summary of the image, the appropriate hash function is selected to generate the hash value of the new sequence, and then the security of encryption is improved by handling the initial values and system parameters of the modified chaotic system accordingly. By combining the plaintext with the key, the computational complexity is 2^{512}, so the encryption method can effectively resist known plaintext and brute force attacks.

After the plaintext is operated with SHA-3 (256), a block of 256-bit values are obtained, and the hash value is converted to binary as the key a. The key a is further processed with Hamming distance to produce the key of the hyper-chaos Lorenz system. The keys of this generation have the advantages of randomness and periodicity.

The Hamming distance represents the number of different characters of two equal-length strings at their corresponding position [22]. From another perspective, it measures the minimum character of substitutions required to convert the string x to a y by replacing the character. Assuming: $x=\{x_1, x_2, \cdots, x_i\}$, $y=\{y_1, y_2, \cdots, y_i\}$, the Hamming distance formula for

calculating these two sequences is as follows:

$$\begin{cases} H(x,y) = \sum_{i=1}^{n} h(x_i, y_i) \\ h(x_i, y_i) = \begin{cases} 0, & x_i = y_i \\ 1, & x_i \neq y_i \end{cases} \end{cases} \tag{4}$$

The key a is divided by bytes and can be divided into 32 bytes, expressed as follows: a_1, a_2, ⋯, a_{32}. For example, b_1=11011101, b_2=11001001, so the Hamming distance $H(b_1, b_2)$ of the two sequences is 2. If $C_1=a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_8$, $C_2=a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus a_{13} \oplus a_{14} \oplus a_{15} \oplus a_{16}$, $C_3=a_{17} \oplus a_{18} \oplus a_{19} \oplus a_{20} \oplus a_{21} \oplus a_{22} \oplus a_{23} \oplus a_{24}$, $C_4=a_{25} \oplus a_{26} \oplus a_{27} \oplus a_{28} \oplus a_{29} \oplus a_{30} \oplus a_{31} \oplus a_{32}$. The key of the hyper-chaos Lorenz system is calculated by the formula (5), where x_1, y_1, z_1, and u_1 are given values.

$$\begin{cases} x_0 = x_1 + H(C_1, C_2) + C_1/4 \\ y_0 = y_1 + H(C_2, C_3) + C_2/4 \\ z_0 = z_1 + H(C_3, C_4) + C_3/4 \\ u_0 = u_1 + H(C_4, C_1) + C_4/4 \end{cases} \tag{5}$$

3.2. The Construction of M Sequence

Given the grayscale image $I(m, n)$, set $L=\lceil m \times n/8 \rceil$, the chaotic sequence generated by the hyper-chaos Lorenz system is applied to construct $L/16$ new sequences -M sequence. The specific construction process is shown below:

Step 1 Fabricate $L/16$ empty sequence M_1, M_2, ⋯, $M_{L/16}$, and each sequence length is 256.

Step 2 The interval [0, 256) is separated into 256 sub-intervals T_j= [j, j + 1), where j =0, 1, ⋯, 255.

Step 3 According to the keys x_0, y_0, z_0, and u_0, the hyper-chaos Lorenz system is iterated s (s>m×n) times by using formula (1). Four sets of hyper-chaotic sequences are obtained: Q_1= $\{q_{11}, q_{12}, \cdots, q_{1s}\}$, Q_2= $\{q_{21}, q_{22}, \cdots, q_{2s}\}$, Q_3= $\{q_{31}, q_{32}, \cdots, q_{3s}\}$, and Q_4= $\{q_{41}, q_{42}, \cdots, q_{4s}\}$. Each element in the hyper-chaotic sequence is pre-processed by formula (6), and the sequences Q_1', Q_2', Q_3', and Q_4' are obtained.

$$f(x) = mod(x \times 1000, 256) \tag{6}$$

Step 4 Followed by the elements in sequences Q_1', Q_2', Q_3', and Q_4' to judge whether it falls into a sub-interval of T, assuming that the value of an element falls into the sub-interval [j, j+1) and j isn't in the M_1, then j is appended to the M_1 until the number of elements in the M_1 reaches 256.

Step 5 Continue to judge the remaining elements in the sequences Q_1', Q_2', Q_3', and Q_4', and fill the sequence M_2, ⋯, $M_{L/16}$. Ensure that each sequence contains 256 elements.

The M sequence constructed in this way has randomness and can effectively resist plaintext attacks.

3.3. Elliptic Curve

Elliptic curve cryptography (ECC), an algorithm for establishing public key encryption. The main advantage of ECC is that in some cases it uses smaller keys, such as RSA encryption algorithms, to provide equivalent or higher security levels than other methods. Another advantage of ECC is that it is possible to define bilinear mappings between groups, based on Weil pairs or Tate pairs; bilinear mappings have found a large number of applications in cryptography, such as identity-based encryption. The disadvantage is that the implementation of encryption and decryption operations is more time-consuming than other mechanisms. In 2005, the NSA announced its decision to adopt a strategy of elliptic curve ciphers as part of the U.S. government's standards to protect sensitive information. Many forms of ECC are slightly different, and all depend on the widely recognized difficulty in solving discrete logarithm problems, corresponding to the group of elliptic curves on finite fields.

The elliptic curve refers to the plane curve determined by the Weierstrass equation:

$$y_2 + a_1 xy + a_3 y = x_3 + a_2 x_2 + a_4 x + a_6 \tag{7}$$

If F is a domain, where $a_i \in F(i=1, 2, 3, 4, 6)$, the number (x, y) that satisfies the Weierstrass equation is called the point of the elliptic curve in the F domain. The F domain is a rational domain or a complex domain. All points of the elliptic curve, plus a special infinite point O, are defined as the elliptic curve on the finite domain F.

In the applications of cryptography, there are two kinds of elliptic curves often used: the elliptic curves with prime values on the prime number domain F_p, where P is an odd prime number, and the elliptic curve on the finite field F_{2^m} with an eigenvalue of 2. The elliptic curve used in this paper is the eigenvalue with prime number domain F_p. In F_p, an elliptic curve E with a large prime number factor is randomly searched, and $G_0=(x'_0, y'_0)$ is the base point of the prime number p on E. a and b are the parameters of the elliptic curve E. The elliptic curve E defined on the prime number domain F_p is:

$$y^2 = x^3 + ax + b(mod\ p) \tag{8}$$

Where a and b satisfy $4a^2+27b^3 \neq 0$ (mod p), and p is the order of the elliptic curve. Then, the point that satisfies this equation and an infinity point O forms an elliptic curve [23-24].

Two randomly selected numbers from the M sequence are parameters a and b of the elliptic curve. If the selected a=180, b=226, p=251, then E: $y^2=x^3+180x+226$(mod 251), and $4\times(180)^2+27\times(226)^3=140\neq 0$ (mod 251). The base point G_0=(1, 77) of the elliptic curve is obtained. The system parameter is (F_{251}, (1, 77), 251, 180, 226).

Key generation: each user generates their own key, and the sender Alin randomly selects an integer d_a as the private key in the M sequence and $1 \leq d_a \leq p$-1. The receiver Bill randomly selects an integer d_b as the private key in the M sequence and $1 \leq d_b \leq p$-1.

The public key of both sides: if the sender Alin, $P_a=d_aG_0$, and the receiver Bill, $P_b=d_bG_0$, then $d_a \times P_b=d_b \times P_a=(x', y')$. It can be seen from the above algorithm that to obtain (x', y'), the d_a of Alin and the P_b of Bill must be obtained, or the private key d_b of Bill and the public key P_a of Alin must be obtained. According to the G_0, P_a, and P_b, the private key d_a of Alin or the private key d_b of user Bill is calculated. This is equivalent to solving the discrete logarithm problem of elliptic curves. As such, it is difficult to obtain (x', y').

3.4. The Construction of Hill Matrix

The Hill cipher is a replacement cipher. To avoid the complexity of the elliptic curve, symmetric cryptography cannot effectively carry out key management, and the correlation between the encryption matrix elements is strong, leading to the easy cracking of the encryption system. In this paper, the elliptic curve and M sequence are used to construct the encryption matrix.

By constructing an 8 by 8 reversible matrix K, the Hill cipher is conducted for each block of images. The specific equation is shown below:

$$E = (K \times I) mod 256 = \begin{bmatrix} k_{11} & \cdots & k_{18} \\ \vdots & \ddots & \vdots \\ k_{81} & \cdots & k_{88} \end{bmatrix} \times \begin{bmatrix} I_{11} \\ \vdots \\ I_{81} \end{bmatrix} mod 256 = \begin{bmatrix} E_{11} \\ \vdots \\ E_{81} \end{bmatrix} \tag{9}$$

Where E is the result of the Hill encryption, $I_{11\sim81}$ are a set of pixels to be encrypted, and $k_{11\sim88}$ are the Hill encryption matrix K; the ciphertext is decrypted by using the inverse matrix K^{-1} of K, $I=(K^{-1}\times E)$mod256=$(K\times E)$mod256.

To avoid the complexity of the algorithm, the G_0 point and the M sequence of the elliptic curve are combined to construct the self-inverse matrix K. The encryption matrix K is divided into four parts:

$$K = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}, K_{11} = \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{bmatrix} \tag{10}$$

(1) According to the parameters of elliptic curve system, calculate $(x', y') = d_a \times P_b = d_b \times P_a$, $(k_{11}, k_{12})=x'G_0$; $(k_{13}, k_{14})=m_1G_0$; $(k_{21}, k_{22})=m_2G_0$; $(k_{23}, k_{24})=m_3G_0$; $(k_{31}, k_{32})=m_4G_0$; $(k_{33}, k_{34})=m_5G_0$; $(k_{41}, k_{42})=m_6G_0$; $(k_{43}, k_{44})=y'G_0$, and the sub-matrix K_{11} is obtained. Among them, $m_1, m_2, \cdots, m_6$ are the first six elements in the M_1 sequence.

(2) The sub-matrix K_{11} is used as the following calculation to generate the sub-matrix K_{12}, $K_{12}=n\times(I-K_{11})$.

(3) $K_{22}=-K_{11}$.

(4) $K_{21}=1/n\times(I+K_{11})$. Then, the produced four sub-matrices K_{11}, K_{12}, K_{22}, and K_{21} are combined to acquire the cipher matrix K.

The elements in the M sequences are blocked every 16 times, and the 4×4 matrices are converted. The 4×4 matrices and K_{11} are multiplied to form the first part of the encryption matrices. Repeat steps (2)-(4) to obtain encryption matrices K_1, K_2, ⋯, K_L.

3.5. Encryption Algorithm

The Hill encryption matrix is constructed by combining an elliptic curve with a hyper-chaotic sequence; the image is ciphered, and the value of the plaintext is further diffused using dynamic DNA encoding technology. The specific flowchart is demonstrated in Figure 1 and the encryption processes are as shown below:

(1) Input the grayscale image matrix I_{mn}.

(2) Set each 8 pixels in a plaintext image is a block (if the last block is not enough 8 pixels, then fill 0). For each set of pixels, a matrix is selected from the Hill encryption matrix constructed in section 3.4, and the matrix is permuted and encrypted to obtain the image matrix I_1.

(3) According to the formula (2), the DNA encoding rule is dynamically selected to convert the image matrix I_1 into the DNA sequence matrix I_2. Take the first column of the encryption matrix K_1, K_2, ⋯, K_L, and synthesize a new matrix K_{L+1}. According to formula (3), the corresponding coding rule is selected, and the matrix K'_{L+1} is obtained by DNA encoding of the K_{L+1}. The matrix I_3 is acquired by performing the DNA sequence operation on the matrix I_2 and the matrix K'_{L+1}.

(4) According to formula (3), DNA decoding of DNA sequence matrix I_3 is carried out, and the image matrix I_4 is obtained.

(5) Each gray value of the image matrix I_4 is represented in binary, and each pixel value in I_4 is cyclically shifted by 2 bits to obtain an image matrix I_5.

(6) The hyper-chaotic sequence Q_4 is extracted, and a novel sequence is arranged on the basis of the order from small to large. The element in the original sequence is permuted by the position of the elements in the new sequence, and the index sequence is obtained. The image matrix I_5 is scrambled by the index sequence, and the final encrypted image matrix I_6 is acquired.

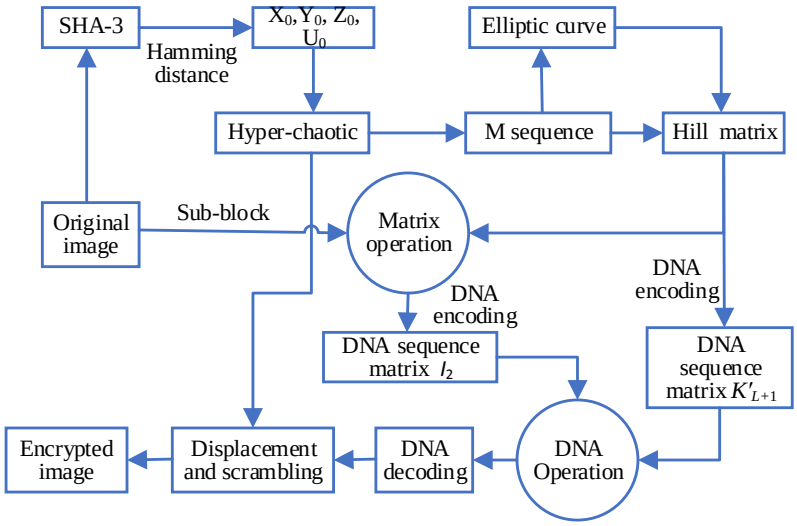


Figure 1. Encryption flowchart

Decryption is the inverse procedure of encryption because the invertible matrix K is a self-inverse matrix; therefore, the decryption algorithm does not need to calculate the inverse matrix K, which greatly saves computational time and computational complexity.

4. Experimental Results and Security Analysis

The experiments are conducted using the MATLAB 7.1(R2014a). The classical 256 by 256 Lena is utilized as the plaintext. By calculation, x_1=63, y_1=25, z_1=47 and u_1=20.75. The plaintext image and the ciphered image are demonstrated in Figure 2. As shown in Figure 2(b), the original image is completely unrecognizable after being encrypted, indicating the validity of the encryption. As seen from the decryption result, the image can be restored without distortion, indicating the feasibility of the algorithm.

(a) Lena image (b) Encrypted image

Figure 2. (a) Lena image; (b) Encrypted image

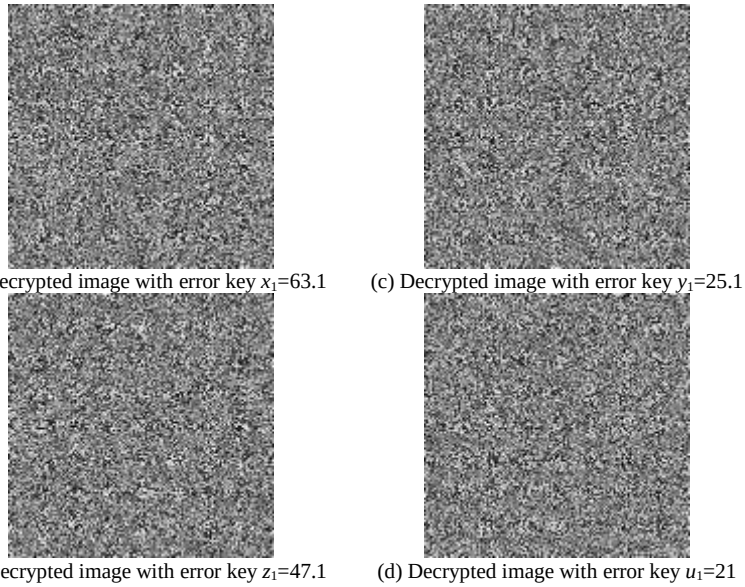
4.1. Exhaustive Attack Analysis

4.1.1. Key Space Analysis

In this encryption algorithm, the main keys include x_1, y_1, z_1, u_1, a, b, and the receiver key d_b. The key space is $10^{84}\times2^{128}\approx3.4\times10^{122}$, which indicates the method has a sufficient key space to defend exhaustive attack.

4.1.2. Key Sensitivity Analysis

The known key is modified slightly to verify the sensitivity of the image. Figure 3(a) represents the decryption diagram of x_1=63.1 with another key invariant. 3(b), 3(c), and 3(d) represent the decryption images of y_1=25.1, z_1=47.1, and u_1=21 with another key unchanged, respectively. Only if the decryption key is in line with the encryption key can the image be deciphered correctly. Otherwise, if there is a small change in the key, the plain image cannot be restored properly, and the error-deciphered image cannot mirror the plaintext image. As a result, the method has key sensitivity.



(a) Decrypted image with error key x_1=63.1 (c) Decrypted image with error key y_1=25.1

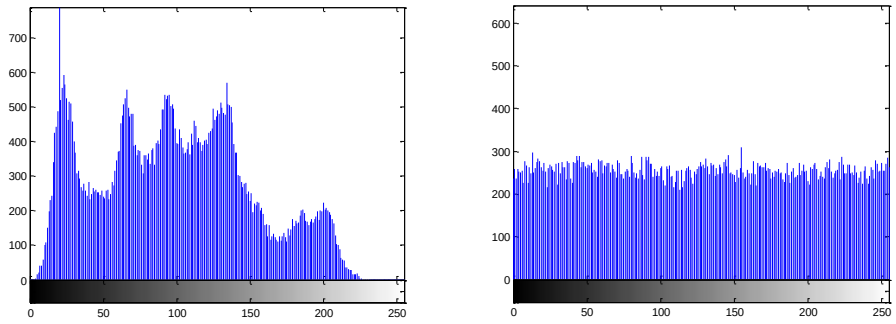
(b) Decrypted image with error key z_1=47.1 (d) Decrypted image with error key u_1=21

Figure 3. Decrypted image under the error key

4.2. Statistical Attack Analysis

4.2.1. Histogram Analysis

A histogram is adopted to represent the distribution of gray values in grayscale images. Figure 4(a) represents the plain image histogram, and Figure 4(b) represents the histogram of the encrypted image. The pixels are relatively scattered before encryption, but after encryption, the corresponding histogram is almost unified; this shows that the algorithm can effectively resist statistical attack.



(a) Histogram of the Lena (b) Histogram of the ciphered Lena

Figure 4. (a) Histogram of the Lena; (b) Histogram of the ciphered Lena

4.2.2. Correlation Analysis

To analyse the correlation coefficient between the pixels in the plain image and the ciphered image. 2500 pairs of adjacent pixels in three directions are randomly selected from the plain image and the ciphered image, and then formulas (11)-(14) are adopted to calculate the coefficient between pixels.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{11}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2 \tag{12}$$

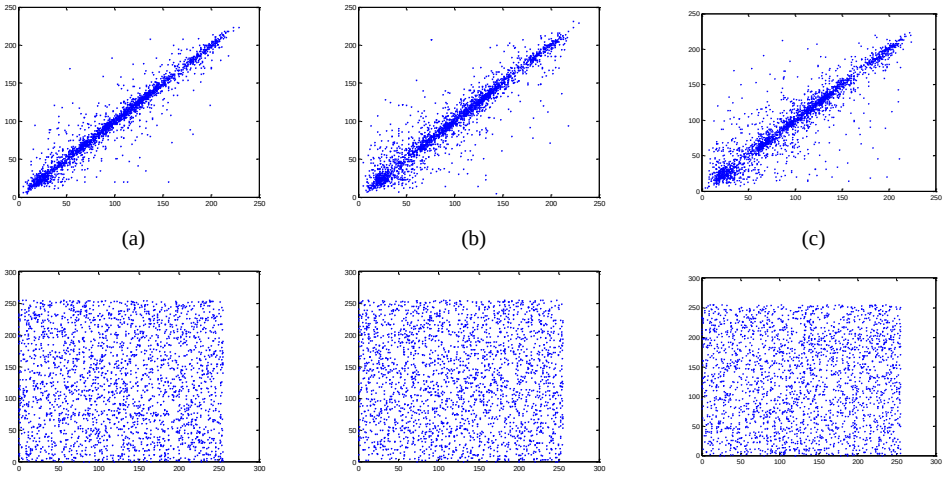
$$COV(x,y) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{13}$$

$$\rho_{xy} = \frac{COV(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{14}$$

Where x and y denote the values of the two adjacent pixels in the image, $E(x)$ is the average, $D(x)$ is the variance, and $COV(x, y)$ is the covariance. By calculation, the correlation coefficient of this method is -0.0002342. Table 3 shows the correlation coefficients in different directions. It can be seen from Figure 5 that the component of the original image has a great correlation in each direction, but after encrypting, the correlation of different components of the ciphertext image is very small. This can preserve the image information from being leaked; therefore, the image encryption algorithm can effectively defend against statistical attacks.

Table 3. Correlation coefficient of the plaintext image and the ciphered image

Correlation coefficient	Horizontal	Vertical	Diagonal
Plaintext	0.9689	0.9486	0.9228
Ciphertext	-0.0029	-0.0031	-0.0037
Ref.[6]	-0.0045	-1.62e-04	0.0053
Ref.[2]	0.0042	0.0034	0.0016
Ref.[7]	0.0041	0.0029	0.0019



(a) (b) (c)

(d) (e) (f)

Figure 5. Correlation analysis: (a)-(c) Correlations of the plaintext image in three directions; (d)-(f) Correlations of the ciphered image in three directions

4.2.3. Information Entropy Analysis

Information entropy is a criterion to judge the uncertainty of a grayscale image. The specific calculation formula is shown below:

$$H(m) = -\sum_{i=0}^{L} P(m_i)\, log_2 P(m_i), \sum_{i=0}^{L} P(m_i) = 1 \tag{15}$$

Here, $P(m_i)$ denotes the probability that the information m_i occurs. When the entropy approaches 8, the produced images are completely random. The information entropy of this method is 7.9895, as shown in Table 4, indicating that the leakage probability of the ciphertext is very small and further verifies the security of the method.

Table 4. Comparison of information entropy in this paper and other references

Information entropy	Lean	Ref.[28]	Ref.[15]
H	7.9895	7.9871	7.9874

4.3. Differential Attack Analysis

The two criterions of number of pixels change rate (NPCR) and unified average changing intensity (UACI) are applied to weight whether the encryption technology can resist the differential attack. If the algorithm has a strong sensitivity to the plaintext, the higher the NPCR value, the closer the NPCR is to 100%, showing that the method is more likely to defend against differential attacks. UACI represents the ratio of the average change of the pixel values of all the plain images and the corresponding positions of the ciphertext images. The closer the UACI value is to 33%, the stronger the ability to defend against differential attacks. The equations below are utilized to compute NPCR and UACI:

$$C(i,j) = \begin{cases} 0, & if\ \ P_1(i,j) = P_2(i,j) \\ 1, & if\ \ P_1(i,j) \neq P_2(i,j) \end{cases} \tag{16}$$

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C(i,j)}{M \times N} \times 100\% \tag{17}$$

$$UACI = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} |P_1(i,j) - P_2(i,j)|}{255 \times M \times N} \times 100\% \tag{18}$$

Where M and N denote the length and width of the image, respectively. $P_1(i, j)$ represents the pixel values of the plaintext image, and $P_2(i, j)$ signifies the pixel values of the ciphertext image. For the Lena images shown in Table 5, the NPCR and UACI of the algorithm are 99.6% and 33.38%, respectively, demonstrating that the encryption method has the capacity to defend against differential attacks.

Table 5. Comparison of NPCR and UACI in this paper and other references

	NPCR	UACI
Ours	99.6%	33.38%
Ref.[8]	99.0276%	32.8399%
Ref.[6]	99.59%	33.41%
Ref.[7]	99.1390%	32.2306%
Ref.[15]	99.60%	28.13%

5. Conclusions

The Hill encryption matrix is constructed by the combination of an elliptic curve and a hyper-chaotic system, thereby avoiding the complexity of elliptic curve encryption and the correlation between encryption matrix elements. This simplifies the encryption method and allows for randomness in the encryption matrix. Combined with dynamic DNA encoding rules, the security of the encryption method is increased and the correlation between pixels is reduced, making the ciphertext difficult to crack. The simulation and experimental results indicate that this algorithm has a better encryption result, larger key space, and higher sensitivity to the key. Furthermore, the algorithm can defend against exhaustive attacks, statistical attacks, and differential attacks.

Acknowledgements

The work for this paper was supported by the National Natural Science Foundation of China (Grant Nos. 61472371, 61572446, 61602424, and 61472372), the Program for Science and Technology Innovation Talents in Universities of Henan Province (Grant No. 15HASTIT019), the Key Scientific Research Projects of Henan High Educational Institution (Grant No. 18A510020), and the Plan for Scientific Innovation Talent of Henan Province (Grant No. 174100510009).

References

1. X. Chai, Y. Chen, and L. Broyde, "A Novel Chaos-based Image Encryption Algorithm using DNA Sequence Operations," *Optics & Lasers in Engineering*, Vol. 88, pp. 197-213, 2017
2. R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "A Novel Chaotic based Image Encryption using a Hybrid Model of Deoxyribonucleic Acid and Cellular Automata," *Optics & Lasers in Engineering*, Vol. 71, pp. 33-41, 2015
3. X. Wang, J. Zhao, and H. Liu, "A New Image Encryption Algorithm based on Chaos," *Optics Communications*, Vol. 285, No. 5, pp. 562-566, 2012
4. F. Özkaynak and S. Yavuz, "Analysis and Improvement of a Novel Image Fusion Encryption Algorithm based on DNA Sequence Operation and Hyper-chaotic System," *Nonlinear Dynamics*, Vol. 78, No. 2, pp. 1311-1320, 2014
5. L. Kong and L. Li, "A New Image Encryption Algorithm based on Chaos," in *Proceedings of 35th Chinese Control Conference* (CCC), pp. 4932-4937, 2016
6. F. Özkaynak, A. B. Özer, and S. Yavuz, "Security Analysis of an Image Encryption Algorithm based on Chaos and DNA Encoding," in *Proceedings of Signal Processing and Communications Applications Conference* (SIU), pp. 1-4, 2013
7. B. Santhosh and K. Viswanath, "A Novel Public Key Cryptosystem for Medical Images," in *Proceedings of International Conference on Inventive Systems and Control* (ICISC), pp. 1-4, 2017
8. K. Gupta, S. Silakari, R. Gupta, and S. A. Khan, "An Ethical Way of Image Encryption using ECC," in *Proceedings of First International Conference on Computational Intelligence*, *Communication Systems and Networks* (CICSYN), pp. 342-345, 2009
9. A. Soleymani, J. Nordin, A. N. Hoshyar, Z. M. Ali, and E. Sundararajan, "An Image Encryption Scheme based on Elliptic Curve and a Novel Mapping Method," *International Journal of Digital Content Technology & its Applications*, Vol. 7, No. 13, pp. 85, 2013
10. F. Wang, X. Q. Zhang, and G. L. Zhu, "A Block Image Element Encryption Algorithm based on ECC," *Communications Technology*, Vol. 41, No. 3, pp. 82-84, 2008
11. L. J. Chen and A. D. Shen, "A Novel Public Key Image Cryptosystem based on Elliptic Curve and Arnold Cat Map," *Advanced Materials Research,* Vol. 989-994, pp. 4183-4186, 2014
12. M. Kumar, A. Iqbal, and P. Kumar, "A New RGB Image Encryption Algorithm based on DNA Encoding and Elliptic Curve Diffie–hellman Cryptography," *Signal Processing*, Vol. 125, No. C, pp. 187-202, 2016
13. B. Acharya, S. K. Patra, and G. Panda, "Image Encryption by Novel Cryptosystem using Matrix Transformation," in *Proceedings of International Conference on Emerging Trends in Engineering and Technology*, pp. 77-81, 2008
14. R. Mahendran and K. Mani, "Generation of Key Matrix for Hill Cipher Encryption using Classical Cipher," in *Proceedings of World Congress on Computing and Communication Technologies* (WCCCT), pp. 51-54, 2017
15. K. D. Patel and S. Belani, "Image Encryption using Different Techniques," *International Journal of Emerging Technology and Advanced Engineering*, Vol. 1, No. 1, pp. 30-34, 2011
16. A. A. A. Gutub and F. A. A. Khan, "Hybrid Crypto Hardware Utilizing Symmetric-Key and Public-Key Cryptosystems," in *Proceedings of International Conference on Advanced Computer Science Applications and Technologies*, pp. 116-121, 2013
17. X. Wang and M. Wang, "A Hyperchaos Generated from Lorenz System," *Physica A Statistical Mechanics & its Applications*, Vol. 387, No. 14, pp. 3751-3758, 2008

18. R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based Image Encryption using a Hybrid Genetic Algorithm and a DNA Sequence," *Optics & Lasers in Engineering*, Vol. 56, No. 5, pp. 83-93, 2014
19. H. Liu, X. Wang, and A. Kadir, "Image Encryption using DNA Complementary Rule and Chaotic Maps," *Applied Soft Computing Journal*, Vol. 12, No. 5, pp. 1457-1466, 2012
20. I. I. Cisse, H. Kim, and T. Ha, "A Rule of Seven in Watson-Crick base Pairing of Mismatched Sequences," *Nature Structural & Molecular Biology*, Vol. 19, No. 6, pp. 623-627, 2012
21. R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A Novel Chaos-based Image Encryption using DNA Sequence Operation and Secure Hash Algorithm SHA-2," *Nonlinear Dynamics*, Vol. 83, No. 3, pp. 1-14, 2015
22. G. Cui, Y. Liu, X. Zhang, and Z. Zhou, "A New Image Encryption Algorithm based on DNA Dynamic Encoding and Hyper-Chaotic System," in *Proceedings of International Conference on Bio-Inspired Computing: Theories and Applications*, pp. 286-303, 2017
23. B. K. Alese, E. D. Philemon, and S. O. Falaki, "Comparative Analysis of Public-Key Encryption Schemes," *International Journal of Engineering & Technology*, Vol. 2, No. 9, pp. 1552-1568, 2012
24. J. Hoffstein, J. Pipher, and J. H. Silverman, "An Introduction to Mathematical Cryptography," 2nd Edition, Springer Publishing Company, 2014