Hindawi
Computational Intelligence and Neuroscience
Volume 2017, Article ID 4079793, 9 pages
http://dx.doi.org/10.1155/2017/4079793

Research Article

Image Encryption Algorithm Based on Hyperchaotic Maps and Nucleotide Sequences Database

Ying Niu, Xuncai Zhang, and Feng Han

College of Electric Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China

Correspondence should be addressed to Xuncai Zhang; zhangxuncai@163.com

Received 8 January 2017; Accepted 27 February 2017; Published 14 March 2017

Academic Editor: Reinoud Maex

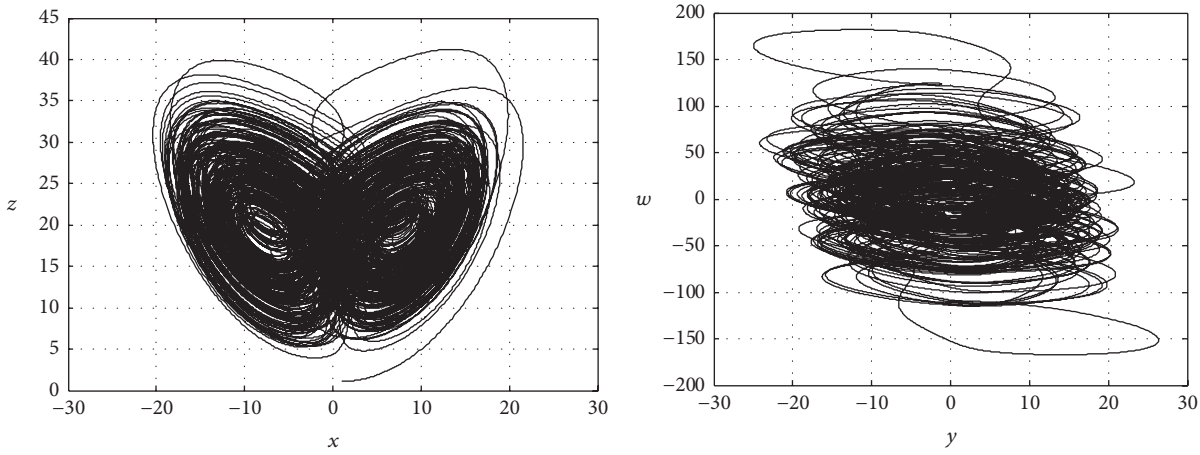
Image encryption technology is one of the main means to ensure the safety of image information. Using the characteristics of chaos, such as randomness, regularity, ergodicity, and initial value sensitiveness, combined with the unique space conformation of DNA molecules and their unique information storage and processing ability, an efficient method for image encryption based on the chaos theory and a DNA sequence database is proposed. In this paper, digital image encryption employs a process of transforming the image pixel gray value by using chaotic sequence scrambling image pixel location and establishing superchaotic mapping, which maps quaternary sequences and DNA sequences, and by combining with the logic of the transformation between DNA sequences. The bases are replaced under the displaced rules by using DNA coding in a certain number of iterations that are based on the enhanced quaternary hyperchaotic sequence; the sequence is generated by Chen chaos. The cipher feedback mode and chaos iteration are employed in the encryption process to enhance the confusion and diffusion properties of the algorithm. Theoretical analysis and experimental results show that the proposed scheme not only demonstrates excellent encryption but also effectively resists chosen-plaintext attack, statistical attack, and differential attack.

1. Introduction

Using digital images to express information is intuitive, vivid, and informative; as a result, they have become a mainstream way of expressing information. With the widespread use of image information, ensuring security has become a universally concerning problem. Currently, digital image encryption technology has become an important method to protect the security of image information [1]. Due to a digital image's large data volume and high redundancy characteristics, the existing classical encryption methods cannot meet the needs of image encryption because of low efficiency of encryption and low security.

In 1949, Shannon put forward the concept of perfect secrecy and proved that the one-time pad cryptosystem had perfect secrecy, as discussed in his paper "Communication Theory of Secrecy Systems" [2]. However, the secret key of a one-time pad encountered a major difficulty in its transfer and distribution. According to pseudorandomness, sensitivity to an initial value, the predictive difficulty of a chaotic system, and the chaotic sequence can achieve the same encryption effect with a one-time pad as a random key, and in theory it is not broken. Chaotic encryption technology has been widely used in the field of information security, especially in the field of image encryption [3, 4]. Chen et al. offered a confusion and diffusion structure of an image encryption algorithm based on the chaotic system [4]. However, due to the limits of computer word lengths, the use of chaotic sequences can lead to chaotic dynamics degradation, especially for low-dimensional chaotic systems [5]. This can seriously impact the security of chaotic encryption. Therefore, to improve the security of the algorithm, many scholars have used a hyperchaos system to ensure the complexity of chaotic sequence. However, there is no denying that a single-encryption algorithm of chaotic mapping cannot guarantee the security of an encrypted image.

DNA is an important genetic information carrier in biology and plays an important role in the genetic organism metabolism. Its advantages include very large-scale parallelism, ultrahigh storage density, and low energy consumption; the unique molecular structure and molecular recognition mechanism of DNA determines its outstanding



(a) x-z plane (b) y-w plane

Figure 1: The attractor of the Chen chaotic system.

information storage and information processing ability. DNA molecules have great development potential in terms of information encryption, hidden certification, and other areas of information security technology [6–8], which provides a new way for developing modern cryptography [9]. In 1995, Dan et al. [9] cracked a 56-key code within 4 months, which demonstrated for the first time the understanding of traditional encryption standard (DES) with DNA computing. Afterwards, the development of DNA cryptography research became a hot topic of research. In 1999, Gehani et al. [10] used DNA as an information carrier and realized a one-time traditional encryption algorithm using biochemical technology in a DNA molecule. In the same year, Celland et al. [11] realized information hiding using DNA as an information carrier and hid the famous information "June 6 invasion: Normandy" in a DNA micropoint in World War II, thus realizing steganography based on the natural storage capacity of DNA. In 2013, Le Goff et al. implemented a three-dimensional (array particle) encryption model and successfully formed three-dimensional DNA hydrogel particle arrays within 100 microns in size by combining DNA particle technology with thermal shrinkage film to fix DNA polymers on a polyethylene heat-shrink chip [12]. The DNA encryption algorithm has been used to encrypt text messages, but it is very difficult to encrypt directly for image information. In 2015, Wu et al. found a new color image encryption scheme based on DNA sequences, and chaotic maps were proposed [13]. These algorithms only realized the location replacement of image pixels, which changed the gray value but failed to achieve the goal of true diffusion.

Therefore, this paper proposes a new image encryption algorithm by combining the chaotic system with the DNA code database. It replaces the bases under the displaced rules by using DNA coding in a certain number of iterations that are based on the enhanced quaternary hyperchaotic sequence, which is generated by Chen chaos; then, the algorithm conducts database operation with the DNA code base, thus further enhancing the confusion and diffusion properties of the algorithm through the cipher-text feedback and iterative chaotic systems.

2. Library Hyperchaos Sequence and DNA Sequence

2.1. Hyperchaos System and Hyperchaos Sequence Generation. As a kind of special nonlinear phenomenon, chaos has a series of excellent features, such as good pseudo randomness, an unpredictable orbit, an extreme sensitivity to initial conditions, structural parameters, and nonrepetitive iterations; it has been widely used in secrecy communications. Compared with low-dimensional chaotic systems, high-dimensional chaotic systems have more positive Lyapunov exponents and are more complex, thus making it difficult to predict the dynamic characteristics that can effectively solve the degradation problem of low-dimensional chaotic system dynamics characteristics. High-dimensional chaos also provides strong confidentiality, a simple algorithm, and substantial key space. In 2005, Li et al. constructed a hyperchaos Chen system through the state feedback control:

$$\begin{aligned} \dot{x} &= a(y - x) + \omega \\ \dot{y} &= dx - xz + cy \\ \dot{z} &= xy - bz \\ \dot{\omega} &= yz + r\omega, \end{aligned} \tag{1}$$

where x, y, z, and w are system state variables and a, b, c, d, and r are system control parameters. The system performs hyperchaos movement when $a = 35$, $b = 3$, $c = 12$, $d = 7$, and $0.085 \le r \le 0.798$. The attractor diagram of the system is shown in Figure 1 when $a = 35$, $b = 3$, $c = 12$, $d = 7$, $r = 0.6$, $x = 1$, $y = 1.1$, $z = 1.2$, and $w = 1.3$.

Four discrete real value hyperchaos sequences can be obtained through system iteration, wherein A_1: $\{a_{11}, a_{12}, \ldots, a_{1n}\}$; A_2: $\{a_{21}, a_{22}, \ldots, a_{2n}\}$; A_3: $\{a_{31}, a_{32}, \ldots, a_{3n}\}$; and

A_4: $\{a_{41}, a_{42}, \ldots, a_{4n}\}$. For a uniform value range of the real number sequence, a new sequence can be obtained by taking a fractional part of the four sequences only, wherein B_1: $\{b_{11}, b_{12}, \ldots, b_{1n}\}$; B_2: $\{b_{21}, b_{22}, \ldots, b_{2n}\}$; B_3: $\{b_{31}, b_{32}, \ldots, b_{3n}\}$; and B_4: $\{b_{41}, b_{42}, \ldots, b_{4n}\}$.

$$\begin{aligned} B1 &= (A1 - [A1]) \\ B2 &= (A2 - [A2]) \\ B3 &= (A3 - [A3]) \\ B4 &= (A4 - [A4]), \end{aligned} \tag{2}$$

where $[x]$ represents the integer part of x. One can calculate or replace the DNA sequence for convenience and define the quaternary hyperchaos sequence P as $\{p_1, p_2, \ldots, p_n\}$.

$$p_i = \begin{cases} 0, & b_{1j} \le b_{2j},\ b_{3j} \le b_{4j}; \\ 1, & b_{1j} \le b_{2j},\ b_{3j} > b_{4j}; \\ 2, & b_{1j} > b_{2j},\ b_{3j} \le b_{4j}; \\ 3, & b_{1j} > b_{2j},\ b_{3j} > b_{4j}. \end{cases} \tag{3}$$

The quaternary hyperchaos sequence generated by this method can eliminate the correlation between adjacent elements in the chaotic sequence and demonstrate good random distribution.

2.2. Nucleotide Sequences. A DNA molecule is composed of four DNA nucleotides, which are adenine (A), cytosine (C), guanine (G), and thymine (T). Two single DNA molecules can form a stable DNA molecule through hydrogen bonds between the nucleotides. The chemical base structure determines the principle of complementary base pairing, which is known as the Watson-Crick base pairing principle, namely, A bonds with T using two hydrogen atoms and G bonds with C using three hydrogen atoms [14, 15]. The natural combination of a quaternary is similar to binary semiconductor switching. Therefore, information storage and computing can be completed using base permutation and combination [16].

The nucleic acid database is an information collection database that contains the nucleotide sequence of nucleic acids and their polymorphisms, structures, properties, and other related descriptions about a single nucleotide. The database file can be accessed from the biological information resource center through any computer network. A sequence ID in the database is called a sequence code; it is unique and permanent.

With the rapid development of sequencing technology, the scale of the nucleic acid database is growing; the index doubled in size in less than nine months. In January 1998, there were 15500 sequence species included in EMBL, and the sequence number is currently more than one million, more than 50% of which are biological sequences. The number of open DNA sequences is more than 163 million to date [17].

Table 1: The XOR operation for DNA sequences.

XOR	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

Table 2: The addition operation for DNA sequences.

ADD	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

Table 3: The subtraction operation for DNA sequences.

Sub	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

Such a large-scale database is equivalent to a natural password, which provides a new train of thought and possible solutions for image encryption technology.

In the image encryption algorithm, three base algorithms are defined to achieve the purpose of pixel confusion and diffusion.

(1) Encoding Rule. If the corresponding code is carried on as A → 00, C → 01, G → 10, and T → 11, the complementary digital match 00 ↔ 11 and 01 ↔ 10 fits the complementary base pairs matching A ↔ T and C ↔ G. A total of 8 encoding combinations meet the complementary pairing rule [18, 19].

For a gray image, each pixel gray value can be expressed with an 8-bit binary number. If DNA code is used, only 4 base sequences are needed. The DNA sequence transformation rules can be used in image processing when they are converted into DNA sequences. To reach the goal of pixel value disturbance, the following base operation and transformation rules are defined at the same time in the encrypted image.

(2) Base Algorithm. According to the complementary pairing rules, there is an algorithm between bases (see Tables 1–3) for A → 00, C → 01, G → 10, and T → 11. Similar algorithms can also be built for other coding.

(3) Base Substitution Rule. For base transformation, we introduce a mapping function $L(x)$ and make the agreement as follows:

$$\begin{aligned} & x \ne L(x) \ne L(L(x)) \ne L(L(L(x))) \\ & x = L(L(L(L(x)))), \end{aligned} \tag{4}$$

Mus musculus genomic fragment, 281000 bp, chromosome 7

GenBank: AJ276505.2

GenBank *Graphics*

>gi|12583595|emb|AJ276505.2| Mus musculus genomic fragment, 281000 bp, chromosome 7

TACATAGACACTAATGAAGGGAGAAATGATGCCTGGATATGTAGGTGGGTGATGGATGAATAGGGGGAGA
GAGGAGTGGACAAACAGATGGGCAAGTGAACGATTTAGTGGAGGGAAGGAGGAAGACAGAATAGTGTGTA
TGCTAGTGAATGATGGGGTGCACTTTCTGAAGAATCCTTCTAGATACTTACACACACCCTCCCCTGACCA
CACTTACTGCACGTGGGCAGATGCCTGATGGGACGGCTGACAGGAAGCTGTGAACTCTTCCCCAAGCCTG
TGTCACTCAATCCCTAAAGAAAGTGAAGCTTCCAGTAGGAGAGACCAATTATGTCAACACCCTTTGTCAC
ACTGCATGACGCCCTTTCCCTATGCAGGTCCCTAAGGGCCCAGCTTGCCTTAGTTGCCCTGGGCCTGGAA
CTACCCAGTTATCTGGAAATCTTAACTAAGTAATGAAATGTGCATGGGACAAAGATGGGCTTTGGGCTGT
GAACAGAAACCTCTGGAACCATTGACATTCCAGGTACCTGCCCATTCCCGAATCTCACCTGGTCCCCAAG
TTCAGCAGGAAATGCTATGCGTATTTGGGATCAGGCCATTGGAAAAAGAGAAGCCATTGGCCAACTACGG
AGGCTCAGGCTATGTCCCTAGAAAGCTGGGCAAGAGGGGAAGCTGGTCAGTGGACTATTGAAAAACCTGT
CCTTGAAAGCAGATAGATGAAGCAGGACAAAAAGTCTCTGCTTGCCAGCACCTGCCAGGAGACTCCAGAG
CAGAGCATTTGTGATTCTCTTATTTATAAAAATAGCTGAGATTGGATGGCTTCTGTCCGGTGGACAGGGA
AAGGCTTGGGAGGTGGCTGACCAAGCTGTTCTCAGCTGGCAGGCTGTGTTTAGGGTGAGACTGTGAGGAC
CTGTCACCTGCTGAAGACATTGCCAGTGGTCAAGAGTGTGGTGAGGCTGCCTATAGTTCCTCCTCTGTAA
CCTCCCCTGGTCCCAGAACTGCTTCCAGCAGGTAGGTGATATCATGGGCTAGTATGACCTGTGAGAGCAC
TCCTGTACCTTCTCACTGTTCAGGACTTTGAGTCTTGGGACCACAGACACTCAGGCAGGGCCAGAAACCT
CATATGTCCTAAAAATAGAACAAGCAGACCCCAGGGACACCCAGCCTCCTGTTATCTTGCCTCCTCACTC
TTCGGGGCCACCTGGTCTGCCCTCCCTTGACCTCTCTGTGGACATACCAGAACACTCCCCCTAGCCTTAG
ATGAGGTCTGACCATATGTCCCTGCTTCTTCCTTTCAGAAGCCCCCCAGCACCCACACCATGAAGGAGGA
GGCCTTTCTCCGGCGCCGTTTCTCGCTGTGTCCACCAGCTTCTACTCCACAGAAGACTGACCCCCGGAAA
GTCCCACGGAACCTGCTTCTGGGCTGCGAAAATGAGCTTGGTCCCATCACCCCAGGTTGGTACAAGCCAT
GGGGATCTGGGGTCCTCCTGGCTCTGCAGTTTGAGAGTTTAGCTAGTGTTCCACCCCATCTAGTACCTTC
ATGGCCAGTGAGAGAGTCACACAAATGGGACTATGATTGTTGTGGGCAAAGGGTTCACAGCACACTGAAG
GACCATGTCTGCTGGTGAGGTTCTAACTTAGAGATGATAAAGATCAGTTATCCCAAACACTGGCTGTGGG
GACAGGCACCTGACCCTAGCCCTGCTGTCATGGCTAAGTACCTGCAGACCACTTACTGGGGCTCAGTTTA

Figure 2: DNA sequence ID in GenBank for AJ276502.

where $x\{A, C, G, T\}$. According to this agreement, there are 6 kinds of reasonable base substitution combinations (see Table 4).

In the pixel value replacement, we can select a replacement combination randomly and perform base displacement to achieve the goal of pixel value disturbance.

Table 4: Base substitution rule.

1	$A \xrightarrow{L} T \xrightarrow{L} C \xrightarrow{L} G \xrightarrow{L} A$
2	$A \xrightarrow{L} T \xrightarrow{L} G \xrightarrow{L} C \xrightarrow{L} A$
3	$A \xrightarrow{L} C \xrightarrow{L} T \xrightarrow{L} G \xrightarrow{L} A$
4	$A \xrightarrow{L} C \xrightarrow{L} G \xrightarrow{L} T \xrightarrow{L} A$
5	$A \xrightarrow{L} G \xrightarrow{L} T \xrightarrow{L} C \xrightarrow{L} A$
6	$A \xrightarrow{L} G \xrightarrow{L} C \xrightarrow{L} T \xrightarrow{L} A$

3. Encryption Algorithms

In this paper, the digital image encryption is realized by using two kinds of chaotic sequences, the DNA sequence library, and its pixel gray value transformation and operation, to achieve the purpose of confusion and diffusion.

3.1. Lorenz Chaotic Mapping. Lorenz mapping is a typical chaotic mapping in chaotic systems, and the system dynamic equation is

$$\begin{aligned} \dot{x} &= \alpha(y - x) \\ \dot{y} &= -xz + \beta x - y \\ \dot{z} &= xy - \gamma z. \end{aligned} \tag{5}$$

Among them are system parameters, and their typical values are separately 10, 28, and 8/3. When they are invariable, the system goes into chaos under the condition of 24.74.

The chaotic sequence system structure generated by the Lorenz system is more complex than the low-dimensional one, which can produce a combination of univariate or multivariate chaotic sequences. The sequence design is very flexible. The system can generate three chaotic real value sequences x, y, and z when A, the initial value, is given. Arranging them in ascending order obtains three new sequences x', y', and z'. Determining the location of each element for the chaotic sequence x, y, and z in the new ordered arrangement x', y', and z' forms a replacement address collection index sequence X, Y, and Z. The index sequences are mainly used for scrambling the image pixel position matrix. Three indexes can realize three-pixel matrix scrambling.

3.2. DNA Sequences. Gray value diffusion is an essential step in the process of image encryption. In this paper, the pixel gray values are changed through the database operation between the image pixel gray value and the nucleic acid bases of the DNA sequences. As an example, this paper adopts the DNA sequence ID in GenBank for AJ276502, which contains 281000 bp bases, as shown in Figure 2. The base sequence information downloaded from the website is shown in the

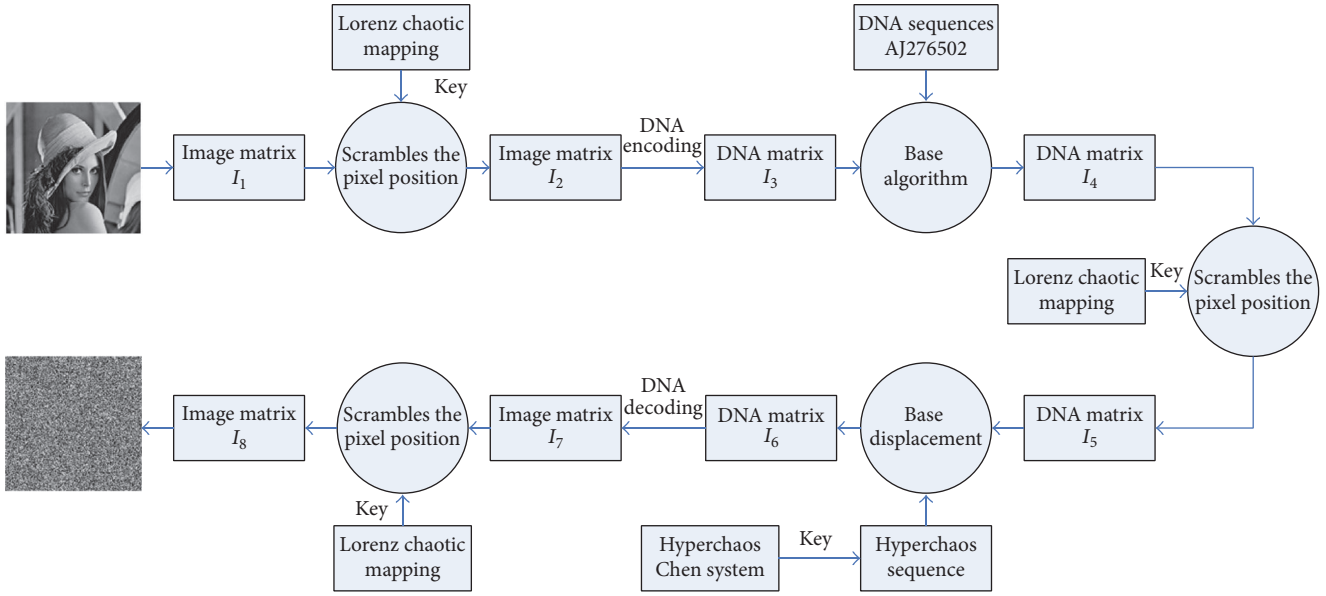


Figure 3: Description of the encryption process.

figure. In the image pixel gray value computation, the starting base location R can be determined randomly, such as $R = 101$.

3.3. Encryption Algorithm Design. In this paper, the digital image encryption algorithm is divided into two parts. The first part is the pixel position scrambling transformation. The image pixel location will be changed through the displacement index created by the Lorenz chaotic sequence. The second part is the pixel gray value transform and spread. We transform the value of each original image pixel into DNA sequences, operate with the sequence in the DNA coding sequence database, and then perform iteration replacement through the cipher-text feedback. The encryption process flow diagram is shown in Figure 3. Specific steps are as follows:

Input: gray image I, parameters of the initial value.

Output: encrypted image.

(1) Convert the gray-scale image I to two-dimensional $M \times N$ matrix I_1.

(2) Scramble the image pixel position matrix I_1 according to the index sequence X produced by Lorenz map and obtain the image pixel location matrix I_2.

(3) Encode each pixel to DNA four-base sequence under a random DNA encoding rule to obtain a new DNA encoding matrix I_3.

(4) Download the DNA sequence whose ID number is AJ276502 from GenBank database. Intercept $M \times N \times 4$ base sequences from R and translate them into matrix I'.

(5) Perform exclusive operation between I_3 and its corresponding base sequence in I', and then conduct addition operation with the previous pixel cryptograph to obtain new matrix I_4. To obtain the coding matrix I_5, scramble the code matrix I_4 using the index sequence Y produced by three-dimensional Lorenz chaos system.

(6) Produce the $M \times N \times 4$ base DNA sequence P using hyperchaos Chen system, and choose the number of the corresponding base displacement in I_5 according to the value of p_i and formula (6). Select a random rule from Table 4 to conduct base displacement and obtain the coding matrix I_6.

(7) After replacement, choose a DNA encoding rule to convert bases to binary code, and further convert them into a decimal gray value to be $M \times N$ matrix and obtain the matrix I_7. The displacement method is as follows:

$$\begin{aligned} x_i &= x_i; \quad p_i = 0 \\ x_i &= L(x_i); \quad p_i = 1 \\ x_i &= L(L(x_i)); \quad p_i = 2 \\ x_i &= L(L(L(x_i))); \quad p_i = 3. \end{aligned} \tag{6}$$

(8) Scramble the image pixel location matrix I_7 according to the index sequence Z produced by Lorenz map and obtain the encryption image matrix to export.

The decryption process is an inverse algorithm. Therefore, we will not illustrate it in this paper.

This algorithm can also be applied to color image encryption; merely conducting RGB decomposition on the values of pixels is sufficient.

(a) Plain Lena image

(b) Image after first-time scrambling

(c) Ciphered Lena image

(d) Recovery Lena image

Figure 4: Lena image and ciphered Lena.

4. Experimental Result

In view of the algorithm proposed in this paper, the feasibility of the algorithm is verified in MATLAB software. This paper adopts the $256 * 256$ Lena gray images.

The original image and encryption image are shown in Figure 4. Figure 4(b) is the image after first-time scrambling, and we cannot identify any of the original image information from it.

5. Security Analyses

5.1. Key Space and the Sensitivity Analyses. The keys in this paper are mainly used for pixel scrambling and the diffusion process: the preliminary Chen system is $x_0 = y_0 = z_0 = w_0 = 1e - 6$ and $r = 0.6$; the preliminary Lorenz chaotic mapping is $x_0' = 0.0006$, $y_0' = -0.0006$, and $z_0' = -0.0006$; rule 2 is selected as DNA encoding rule; rule 1 is selected as substitution rule; and the DNA sequence ID number is AJ276502 and the starting position is $R = 1$.

If the calculation accuracy is 10^{-14}, the key space will reach 10^{100}, which shows that this algorithm has sufficient space to resist a brute force attack.

To test the key sensitivity, we increase the initial value of x_0' for the Lorenz map to 0.0000000001 and keep the other keys invariant. Figure 5 shows the corresponding decryption figure. It shows that the key cannot decrypt the original image correctly when the key changes slightly, which indicates the algorithm has stronger key sensitivity.

5.2. Gray Histogram Analysis. The original image gray value distribution can be exposed to a certain extent from image statistics; therefore, it is vitally important to change the statistical distribution of the original image. The image pixel gray value arithmetic operation is used for the purpose of a gray statistical attack defense. As shown in Figure 6, experiment results show that exclusive processing and replacement operation make the encrypted image gray-scale distribution uniform, which demonstrates that the algorithm has a very

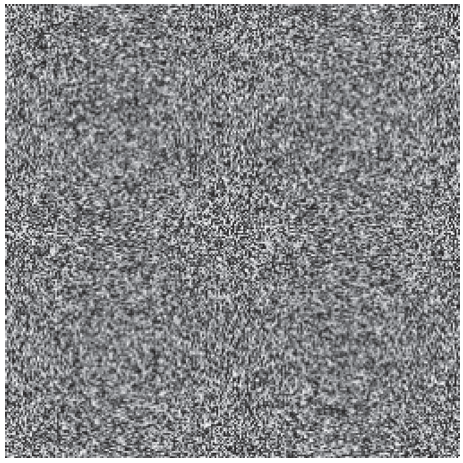
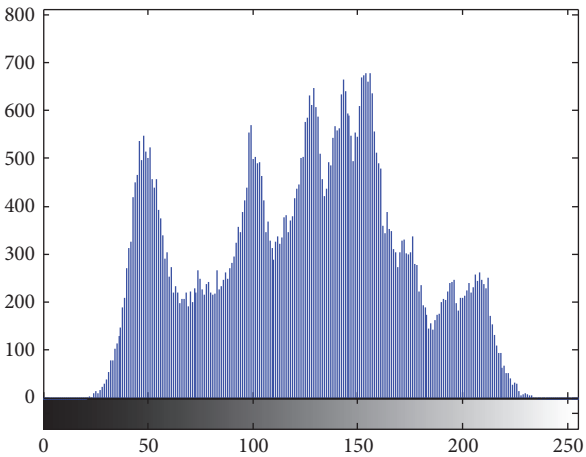
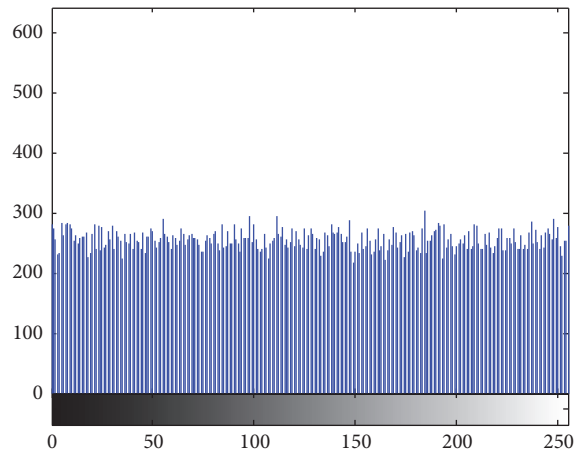


Figure 5: Failure of decryption of Lena.



(a) Histogram of the plain Lena image



(b) Histograms of the ciphered Lena image

Figure 6: Histogram of the plain Lena image and ciphered Lena image.

good ability to resist statistical analysis; attackers will not be able to analyze the original gray value distribution.

Table 5: Adjacent pixels correlation comparison.

	Original image	Encryption image
Horizontal direction	0.9700	−0.0207
Vertical direction	0.9384	−0.0176
Diagonal direction	0.9176	0.0168

5.3. Correlation Analysis. The original image pixel correlation is usually large, so we must prevent the reduction of the correlation of adjacent pixels to prevent statistical analysis. An encrypted image and its original image are selected randomly for 2500 pixels, and the horizontal, vertical, and diagonal pixel correlation results are shown in Table 5. Table 5 shows that former image pixels have great correlation, which greatly reduces after encryption compared with before. This suggests that the adjacent pixels have been largely irrelevant, and the statistical characteristics of the original image have been spread randomly to cipher-text images. Table 5 and Figure 7 present correlation comparisons of adjacent pixels between the original and encrypted images.

5.4. Information Entropy Analysis. The information entropy is a type of index for an uncertainty test. Its computation formula is as follows:

$$H(m) = -\sum_{k=0}^{2^N-1} p(m_i) \log_2 p(m_i), \tag{7}$$

where $p(m_i)$ is the appearance probability of information. For gray images, there are 256 information states for information m. The minimum value of m is 0, and the maximum is 255. According to the former formula, the information is completely random when the information entropy is 8. That is, the bigger the cipher-text information entropy is, the more security the information has. In this paper, the information entropy for the Lena image is 7.9888, which indicates that the cipher-text information leakage is minimal. This further proves the security of this algorithm.

6. Conclusions

This paper presents a type of digital image encryption technology based on hyperchaos mapping and DNA sequence library arithmetic to realize a scrambling position transformation of image pixels and the spread of the pixel values. A safety analysis shows that the algorithm can effectively resist plaintext attack, differential attack, and statistical attack. Additionally, it provides a large key space and high security.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

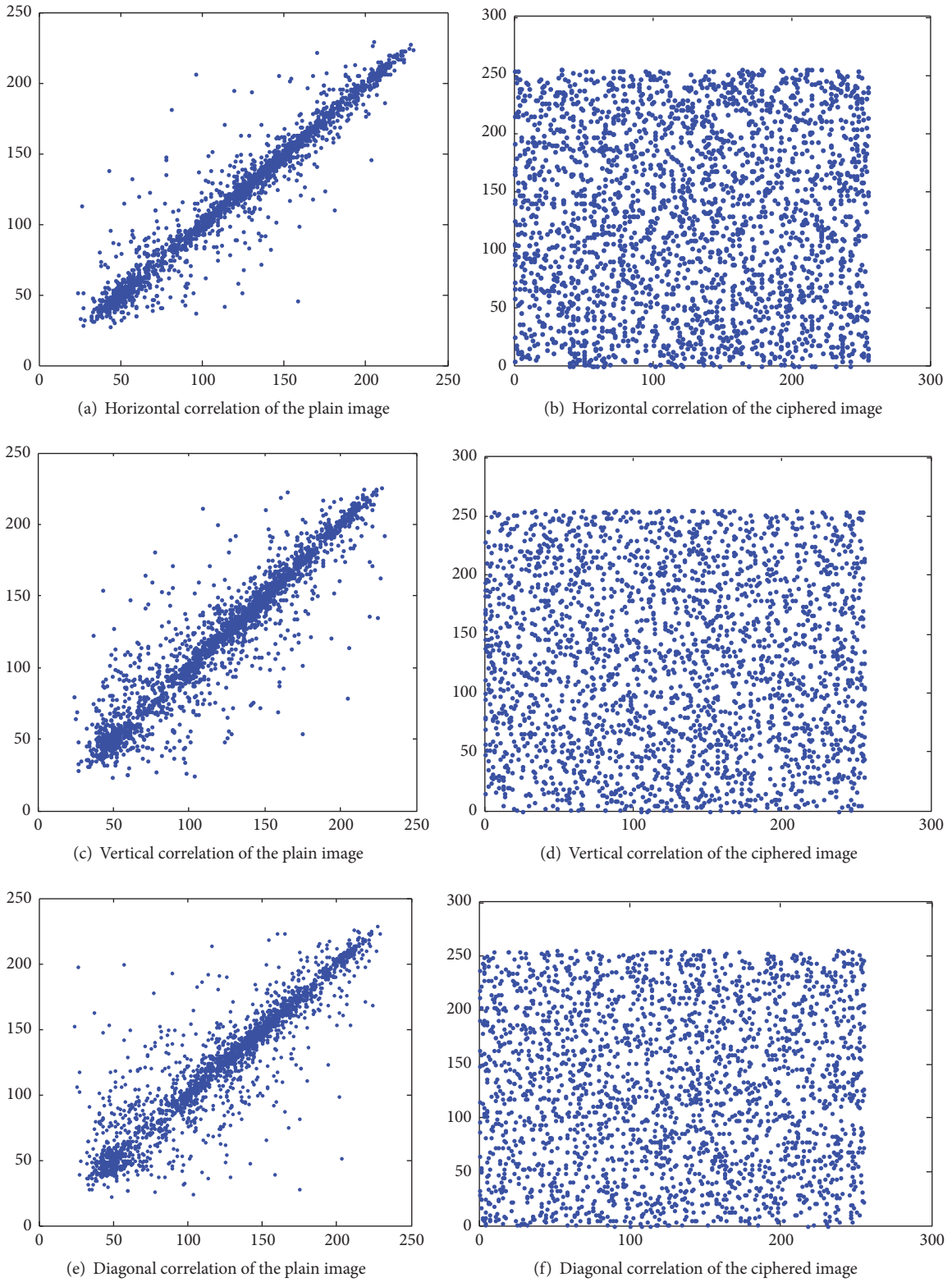


Figure 7: Correlation analysis of Lena as a ciphered image in three directions.

Acknowledgments

The work for this paper was supported by the National Natural Science Foundation of China (Grant nos. 61602424, 61472371, and 61572446), Plan for Scientific Innovation Talent of Henan Province (Grant no. 174100510009), and Program for Science and Technology Innovation Talents in Universities of Henan Province (Grant no. 15HASTIT019).

References

[1] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons and Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[3] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.

[4] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[5] X. Wang, X. Wang, J. Zhao, and Z. Zhang, "Chaotic encryption algorithm based on alternant of stream cipher and block cipher," *Nonlinear Dynamics. An International Journal of Nonlinear Dynamics and Chaos in Engineering Systems*, vol. 63, no. 4, pp. 587–597, 2011.

[6] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with DNA binary strands," *BioSystems*, vol. 57, no. 1, pp. 13–22, 2000.

[7] B. Shimanovsky, J. Feng, and M. Potkonjak, "Hiding data in DNA," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2578, pp. 373–386, 2003.

[8] W.-L. Chang, M. Guo, and M. S.-H. Ho, "Fast parallel molecular algorithms for DNA-based computation: factoring integers," *IEEE Transactions on NanoBioscience*, vol. 4, no. 2, pp. 149–163, 2005.

[9] B. Dan, C. Dunworth, and R. J. Lipton, "Breaking DES using a molecular computer," in *Proceedings of the DIMACS Workshop*, vol. 27 of *Series in Discrite Mathematics and Theoretical Computer Science*, Princeton University, Princeton, NJ, USA, April 1995.

[10] A. Gehani, T. Labean, and J. Reif, "DNA-based cryptography," in *Proceedings of the DIMACS Workshop*, vol. 54 of *Series in Discrite Mathematics and Theoretical Computer Science*, Massachusetts Institute of Technology, Cambridge, Mass, USA, June 1999.

[11] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots," *Nature*, vol. 399, no. 6736, pp. 533–534, 1999.

[12] G. C. Le Goff, L. J. Blum, and C. A. Marquette, "Shrinking hydrogel-DNA spots generates 3D microdots arrays," *Macromolecular Bioscience*, vol. 13, no. 2, pp. 227–233, 2013.

[13] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing Journal*, vol. 37, pp. 24–39, 2015.

[14] Z. Ignatova, I. Martinez-Perez, and K. Zimmermann, *DNA Computing Models*, Springer, New York, NY, USA, 2008.

[15] X. Zhang, Y. Niu, C. Shen et al., "Fluorescence resonance energy transfer-based photonic circuits using single-stranded tile self-assembly and DNA strand displacement," *Journal of Nanoscience and Nanotechnology*, vol. 17, pp. 1053–1060, 2017.

[16] J. P. L. Cox, "Long-term data storage in DNA," *Trends in Biotechnology*, vol. 19, no. 7, pp. 247–250, 2001.

[17] H. J. Shiu, K. L. Ng, J. F. Fang, R. C. Lee, and C. H. Huang, "Data hiding methods based upon DNA sequences," *Information Sciences. An International Journal*, vol. 180, no. 11, pp. 2196–2208, 2010.

[18] X. Zhang, Y. Wang, G. Cui, Y. Niu, and J. Xu, "Application of a novel IWO to the design of encoding sequences for DNA computing," *Computers & Mathematics with Applications*, vol. 57, no. 11-12, pp. 2001–2008, 2009.

[19] 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.