Hindawi
Journal of Electrical and Computer Engineering
Volume 2019, Article ID 8146093, 16 pages
https://doi.org/10.1155/2019/8146093

Research Article

A Novel Memcapacitor Model and Its Application for Image Encryption Algorithm

Nan Li,[1,2] **Junwei Sun**,[1,2] **and Yanfeng Wang**[1,2]

[1]*School of Electrics and Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China*
[2]*Henan Key Lab of Information-Based Electrical Appliances, Zhengzhou University of Light Industry, Zhengzhou 450002, China*

Correspondence should be addressed to Junwei Sun; junweisun@yeah.net

Received 23 August 2018; Revised 23 January 2019; Accepted 26 February 2019; Published 1 April 2019

Academic Editor: Ephraim Suhir

In this paper, a novel chaotic circuit with one memcapacitor is designed, which has abundant dynamic behaviors. As a potential application, combining the DNA binding mode and the characteristics of the chaotic system, a new image encryption scheme is proposed. Firstly, the original image is processed and generates a set of hash values by the SHA-3 algorithm. The generated hash value and original image are performed XOR operation. The hash values are processed to generate the initial value of the chaotic system by the Hamming distance. Furthermore, the elliptic curve with the hyperchaotic sequence is used to construct the Hill encryption matrix, and the plaintext image is permuted and encrypted. At last, the proposed chaotic system is used to scramble the image. The simulation results and theoretical analysis show that the chaotic system has abundant dynamic behaviors, and the proposed algorithm has a better anti-interference ability for image and information encryption.

1. Introduction

With the rapid development of multimedia technology and Internet technology, digital images have become one of the most important information carriers for people to communicate. It is so easy to obtain digital images through network and further use, process, reproduce, and distribute them. However, the digital images are vulnerable to attacks in unauthorized network transmission, so people have to take more attention on security and confidentiality of multimedia information, and encryption technology must be used to ensure the security of image transmission. Some traditional encryption algorithms such as Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA) do not take into account the strong correlation between the pixels in the digital image itself. Therefore, finding a new encryption method applied to image encryption will be a hot research topic at present.

Generally, there are two major approaches which are used to protect digital images. One is information hiding [1] which includes watermarking, anonymity, and cover channel. The other is encryption which includes conventional encryption and others such as chaotic encryption. There have been a large number of image-encrypted documents [2–5], based on chaotic systems and DNA algorithms. The low-dimensional system has the advantages of simple form and short time of generating chaotic sequence. But the disadvantage is that the key space is too small to be easily attacked. Therefore, the chaotic image encryption algorithm develops along the direction of complex chaotic systems, such as low-dimensional to high-dimensional chaos and hyperchaos. However, most of the processing technology is based on the computer software platform, which is difficult to meet the growing processing quantity and fast and timely processing requirements. So, it is necessary to explore the hardware implementation of digital image processing, that is, the design and implementation of high speed and accurate image encryption circuit. In order to solve these problems, with the research of DNA computing, DNA cryptography is born as a new cryptographic field emerged, in which DNA is used as information carrier and the modern biological technology is used as implementation tool [6, 7]. Some researchers

suggest that DNA computing [8, 9] is an effective way to improve the security of chaotic image encryption technology.

As we all know, DNA has the feature with large-scale parallelism, ultra-low energy consumption, and high storage density inherent in molecules. DNA computation was first introduced by Adleman in the literature [10]. More specifically, DNA encryption computation is based on DNA as the information carrier, with modern biotechnology as the realization tool, to excavate the inherent high storage density and high parallelism of DNA and realize cryptographic work such as encryption and decryption. An image encryption algorithm based on chaos and DNA dynamic encoding is proposed in the literature [11], which contains dynamic DNA encoding rules. Hanis et al. [12] designed an image encryption scheme using an improved chaotic map and a butterfly-like structure. Xue et al. proposed a digital image encryption technique based on DNA sequence and multichaotic mapping, which uses DNA sequences, cubic radiation, and logistic maps to fuse the encrypted images in the literature [13]. The method makes the pixel correlation of the encrypted image become higher, but the implementation process is complex. Wong et al. [14] proposed an image encryption with the chaotic standard map. The algorithm has large key space and high sensitive, but their security is not high enough. A novel encryption scheme based on the DNA sequence is proposed by Guesmi et al. [15]. They used the natural DNA sequences to encoding the information and encrypted an image by using the hash algorithm SHA-2. Such experiments can only be done in a well-equipped lab using current technology, and it needs high cost. For these reasons, the researches of DNA cryptography are still much more theory than practicality. As a result of ongoing studies, some promising image encryption schemes and improvements to the previous algorithms have been proposed recently [16–18].

On the other hand, more than 40 years ago, according to the principle of symmetry, Chua proposed the fourth fundamental circuit element memristor [19, 20]. But it was not confirmed until found that TiO_2 has the characteristics of the memristor in the nanoscale in Hewlett Packard Labs [21]. Since then, memristors have attracted widespread attention and become a hot research area. Compared with the conventional memories technology, memristors bring new technological innovation by virtue of its characteristics, such as instance, high density, low power, and good memory characteristics, which are utilized to design memory device, construct chaotic circuits [22, 23], improve neural networks [24], and so on. Some examples are circuits with two HP memristors in antiparallel [25] and a practical implementation of memristor-based chaotic circuits in a programmable gate array [26]. Also, the memristor-based chaotic circuit for pseudorandom number generation has been analyzed in a cryptography application study [27].

Compared with the development of memristor, memcapacitor and meminductor have received relatively little attention. Although actual solid-state memcapacitor has not been yet realized so far, it is important to design effective memcapacitor models and make prospective studies for its applications [28]. In 2009, Ventra and Chua [29] extended the concept of memristors to memcapacitors and meminductors. Memcapacitor has the characteristic of variable capacitance according to its accumulated state, e.g., charge and voltage [30]. It would be worthwhile to prospectively study effective memcapacitor models and its applications. Several memcapacitor models, such as piecewise linear, quadric, and cubic function models, memristor-based memcapacitor models, and memcapacitor emulators, were proposed in [31], and a mathematical memcapacitor model and a corresponding circuit model are established in [32].

In this work, a new image encryption scheme is proposed by analyzing the characteristics of the memcapacitor system and DNA encoding. Referring to the previous researches [2, 14] on chaotic encryption, there are some advantages which make our research more attractive and meaningful. At first, the original image is processed and generates a set of hash values by the SHA-3 algorithm. The generated hash value and original image are performed XOR operation. The hash values are processed to generate the initial value of the memcapacitor chaotic system by the Hamming distance. Then, the combination of the memcapacitor system and elliptic curve is used to construct the Hill encryption matrix to permute and encrypt the image. Finally, the hyperchaotic sequence is used to scramble the image.

The outline of this paper is organized as follows. In Section 2, a new chaotic system base on memcapacitor is proposed and analyzed. In Section 3, the related preparatory work is introduced. Section 4 presents the chaotic encryption scheme, and Section 5 gives some simulation results and security analysis. Finally, some conclusions and suggestions for future work are given in Section 6.

2. A Novel Base on Memcapacitor Chaotic System

2.1. Memcapacitor Chaotic System. Memcapacitor has the characteristic of variable capacitance according to its accumulated state, e.g., charge and voltage. In this section, the schematic of proposed four-order passive circuit base on the voltage-controlled memcapacitor is proposed. The chaotic circuit is shown in Figure 1, which contains two linear inductors, L_1 and L_2, a linear resistor, R, a linear capacitor, C, and a voltage-controlled memcapacitor, C_{M}. Its charge-voltage relation is

$$q = C_{\mathrm{M}}(q, v, t). \tag{1}$$

Considering a voltage-controlled memcapacitor whose capacitance is dependent on the applied voltage, the device's capacitance changes linearly or nonlinearly from the minimum value to maximum value according to the voltage add-on. The nonlinear capacitance-voltage relationship can be designed as follows:

$$\begin{aligned} C_M(v) &= C_{M\max}\left(1 - e^{-\beta v}\right) + C_{M\min}e^{-\beta v} \\ &= C_{M\max} - \left(C_{M\max} - C_{M\min}\right)e^{-\beta v}, \end{aligned} \tag{2}$$

where $C_{M\max}$ is the maximum capacitance of the memcapacitor while the applied voltage approaches to infinite

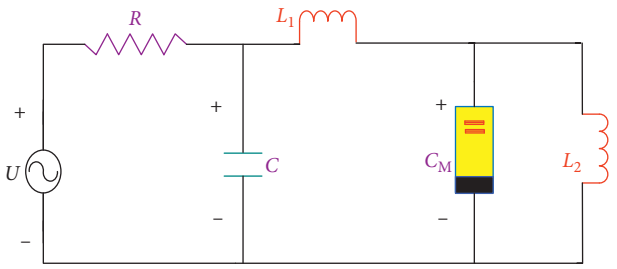


Figure 1: Four-order passive circuit based on voltage-controlled memcapacitor.

and $C_{M\min}$ is the minimum capacitance when applied voltage comes to zero.

The current flowing across a voltage-controlled capacitor is the derivation of charge to time, as

$$i = \frac{dq}{dt} = C_v\frac{dv}{dt} + v\frac{dC_v}{dt},$$
$$\frac{dC_v}{dt} = \operatorname{sign}(v)\beta\left(C_{M\max} - C_{M\min}\right)e^{-\beta v}\frac{dv}{dt}. \tag{3}$$

According to Kirchho's law, the KCL and KVL equations of this circuit are given in equation (4), where A and w are the amplitude and angular speed of this voltage source, respectively:

$$\begin{cases} \dfrac{dV_C}{dt} = \dfrac{(A\sin(wt) - V_C/R) - i_{L_1}}{C} = \dfrac{A\sin(wt) - V_C}{RC} - \dfrac{i_{L_1}}{C}, \\ \dfrac{di_{L_1}}{dt} = \dfrac{V_C - V_{C_M}}{L_1}, \\ \dfrac{dV_{CM}}{dt} = \dfrac{i_{L_1} - i_{L_2}}{C_M}, \\ \dfrac{di_{L_2}}{dt} = \dfrac{V_{C_M}}{L_2}. \end{cases} \tag{4}$$

Let $x = V_c$, $y = i_{L_1}$, $z = V_{C_M}$, and $u = i_{L_2}$, finally, we get the state equation as

$$\begin{cases} \dot{x} = \dfrac{(A\sin(wt) - V_C/R) - i_{L_1}}{C}, \\ \dot{y} = \dfrac{V_C - V_{C_M}}{L_1}, \\ \dot{z} = \dfrac{i_{L_1} - i_{L_2}}{C_M}, \\ \dot{u} = \dfrac{V_{C_M}}{L_2}. \end{cases} \tag{5}$$

Numerical simulation using MATLAB ode45 integration was adopted to research the dynamic behaviors of this proposed voltage-controlled memcapacitor circuit. The circuit's parameter conditions are set as follows: $A = 20$, $w = 30$ rad/s, $R = 100$ Ohm, $C = 0.2$ F, $L_1 = 0.1$H, $L_2 = 0.1$H, $C_{M\max} = 0.1$ F, $C_{M\min} = 0.01$ F, and $\beta = 10$. If the initial conditions are $x = 0$, $y = 0$, $z = 0$, and $u = 0$, then equation (5) can be written as

$$\begin{cases} \dot{x} = \sin(30t) - \dfrac{x}{20} - 5y, \\ \dot{y} = 10x - 10y, \\ \dot{z} = \dfrac{y - u}{0.1 + 0.09e^{-10|z|}}, \\ \dot{u} = 10z. \end{cases} \tag{6}$$

The Lyapunov exponents of the spectrum are $\mathrm{LE}_1 > 0$, $\mathrm{LE}_2 > 0$, $\mathrm{LE}_3 < 0$, and $\mathrm{LE}_4 < 0$ in Figure 2, which imply that system (6) is a hyperchaotic system. The attractor of the chaotic system (6) with initial conditions $x(0) = 0$, $y(0) = 0$, $z(0) = 0$, and $u(0) = 0$ is shown in Figures 3(a)–3(d).

2.2. Waveform Drawing. The time domain waveform of state variables Vc, i_{L_1}, Vc_M, and i_{L_2} is shown in Figures 4(a)–4(d).

2.3. Dissipativity and Equilibrium Point Set. It is well known that being dissipative is a necessary condition for nonlinear circuit to generate chaotic attractors. In order to evaluate the dissipativity of the circuit in Figure 1, mathematical expression of the exponential constrain rate is deduced from (6) as

$$\nabla V = \frac{\partial\dot{x}}{\partial x} + \frac{\partial\dot{y}}{\partial y} + \frac{\partial\dot{z}}{\partial z} + \frac{\partial\dot{u}}{\partial u} = -\frac{1}{20} - 10 - \frac{0.9(y-u)e^{-10|z|}}{\left(0.1 + 0.09e^{-10|z|}\right)^2}. \tag{7}$$

Considering that the exponential function is greater than or equal to zero, equation (7) can be simplified as

$$\nabla V = \frac{\partial\dot{x}}{\partial x} + \frac{\partial\dot{y}}{\partial y} + \frac{\partial\dot{z}}{\partial z} + \frac{\partial\dot{u}}{\partial u} \le -\frac{201}{20} < 0. \tag{8}$$

Obviously, the dissipativity of the circuit in Figure 1 is negative, implying that all orbits are ultimately confined to a specific subset of zero volume, and the asymptotic motion settles onto an attractor in the neighborhood of the unstable equilibrium points. Its dynamical behaviors can be qualitatively determined by evaluating the eigenvalues of the corresponding Jacobian matrix at each of the equilibrium points. The equilibrium points of system (6) are obtained by solving the following equations:

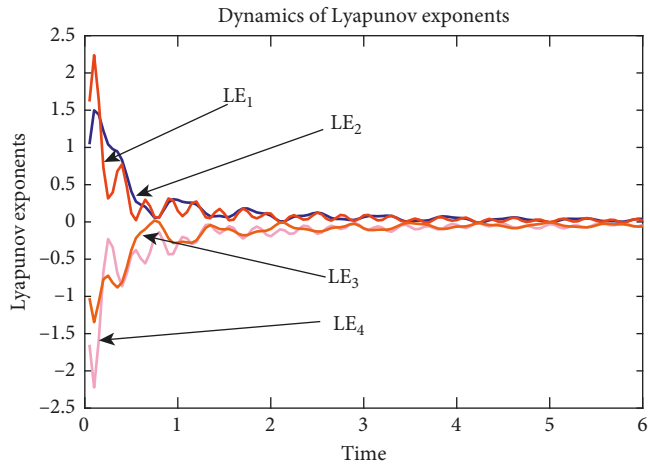


Figure 2: Lyapunov exponents of chaotic system (6) vs. t.

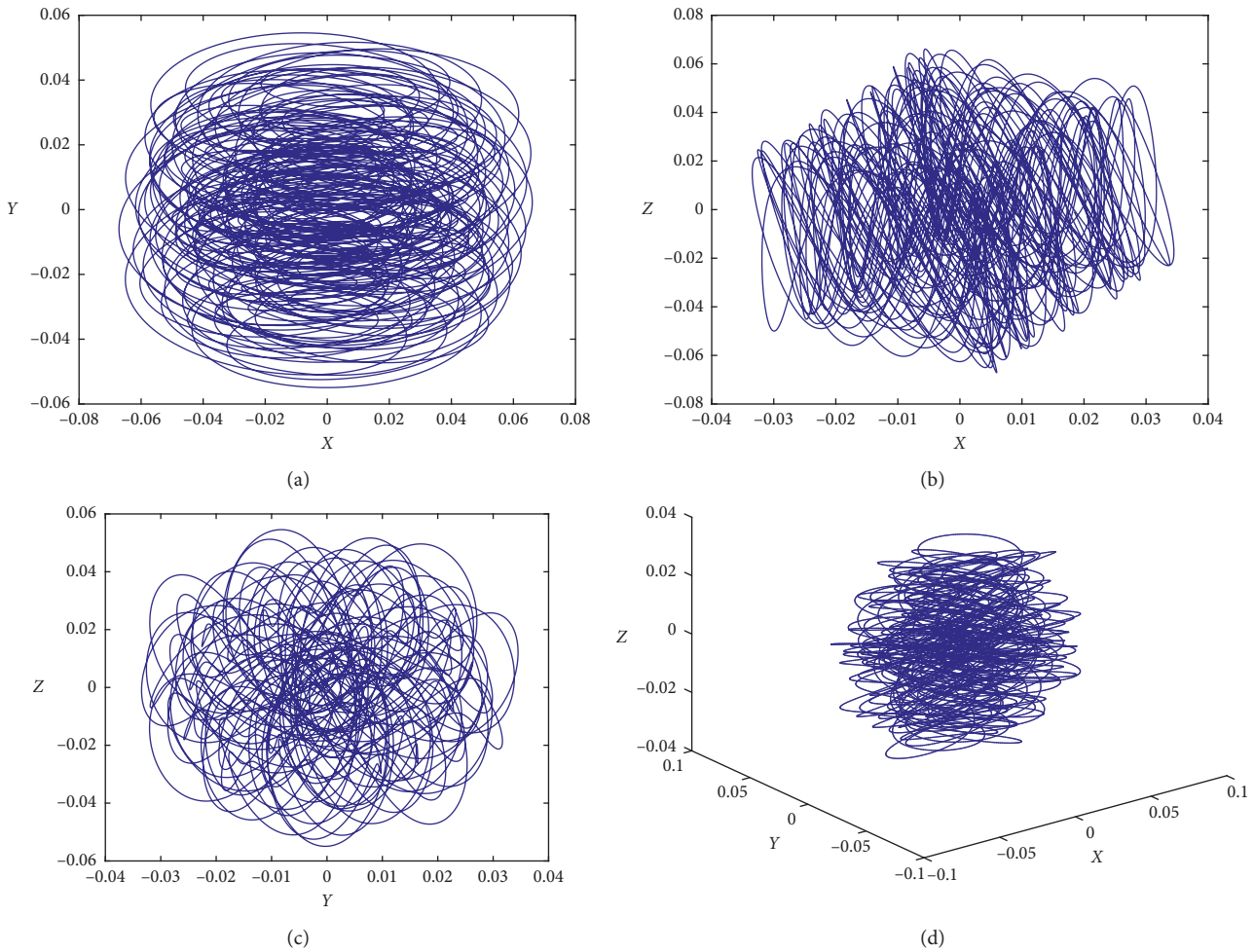


Figure 3: Phase portraits of system (6). Phase portraits of (a) system (6) x vs. y, (b) system (6) x vs. z, (c) system (6) y vs. z, and (d) system (6) x vs. z vs. z.

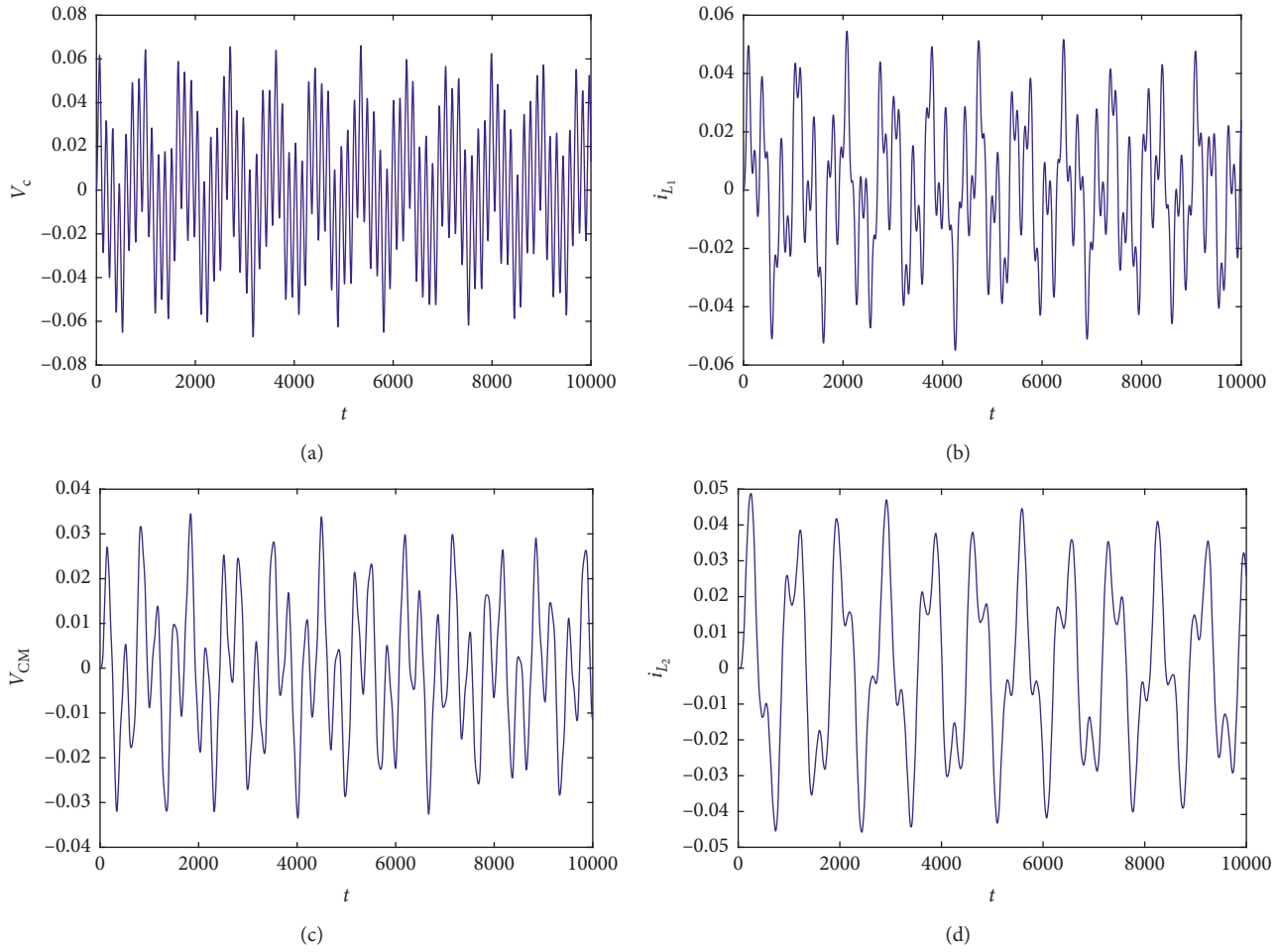


FIGURE 4: Waveform drawing of state variable: (a) Voltage of C; (b) current flow of inductor L_1; (c) voltage of C_M; (d) current flow of inductor L_2.

$$\begin{cases} \dot{x} = \sin(30t) - \dfrac{x}{20} - 5y = 0, \\ \dot{y} = 10x - 10y = 0, \\ \dot{z} = \dfrac{y - u}{0.1 + 0.09e^{-10|z|}} = 0, \\ \dot{u} = 10z = 0. \end{cases} \tag{9}$$

Clearly, the equilibrium point set is

$$E = \left\{ (x, y, z, u) \,\middle|\, x = y = u = \frac{20}{101}\sin(30t), z = 0 \right\}. \tag{10}$$

Their values are determined by the specified circuit parameters of A, R, C, L_1, and L_2. This property is different from the conventional memristor-based chaotic circuits.

2.4. Dynamics Dependent on System Parameters. Similar to dynamical analysis of the general chaotic circuit, by utilizing the conventional dynamical analysis tools such as bifurcation diagram, Lyapunov exponent spectra, and so on, the dynamical behaviors of the chaotic system (6) shown in Figure 1 are studied under the variation of system parameters. According to formula (5), we have the following assumptions: $1/RC = a$, $1/C = b$, $1/L_1 = c$, and $1/L_2 = d$.

2.4.1. Fix $b = 5$, $c = 10$, and $d = 10$ and Vary a. For the above circuit parameters, the initial conditions of system (6) are $x_0 = y_0 = z_0 = u_0 = 0$. Figures 5 and 6 show the spectrum of Lyapunov exponents and bifurcation diagrams of system (6) with respect to parameter a (to clearly see positive Lyapunov exponents, the horizontal axis is limited in [17, 24]). Obviously, when $a \in [17, 24]$, it can be observed from Figure 5 that the memcapacitor-based chaotic circuit has two positive Lyapunov exponents ($LE_1 > 0$ and $LE_2 > 0$), which implies that this system should be in hyperchaotic state.

Observed from Figures 5 and 6, when the parameter $a \in [17, 24]$, the Lyapunov exponents LE_1 and LE_2 are greater than 0 but they are closer to zero in Figure 5. System (6) can produce complex chaotic behaviors, which are transient hyperchaos phenomena in Figure 6. Also, some further examples of typical points are described in Figure 7. For example, when a equals to 18 and 23, the transient hyperchaos behaviors are observed in Figures 7(a) and 7(b),

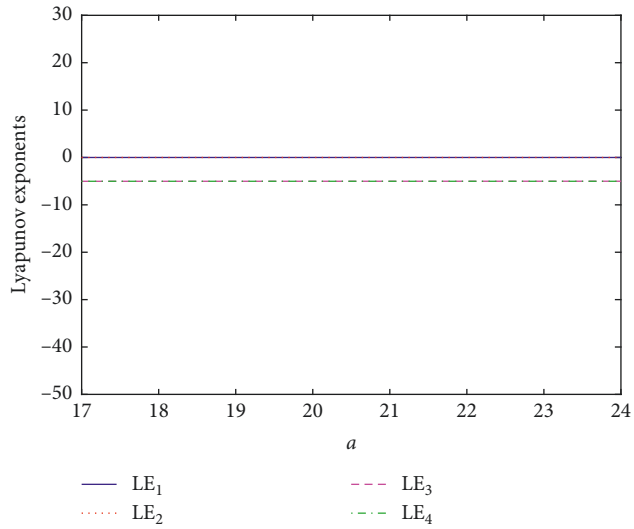


Figure 5: Lyapunov exponents of chaotic system (6) versus parameter a.

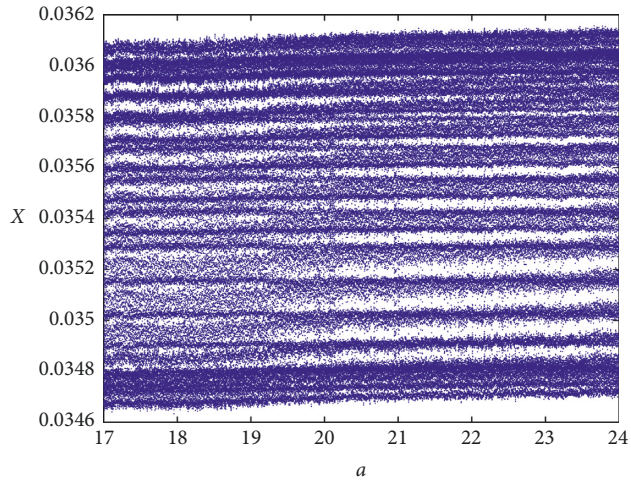


Figure 6: Bifurcation diagrams of chaotic system (6) versus parameter a.

respectively. The orbits of the system start from different initial states and have different dynamics. In the numerical simulation analysis, the initial states (0.1, 1, 0, 0) and (0.2, 0, 0.1, 1) are implemented, and the trajectories are shown in Figure 7 by the blue curve and the red curve, respectively [19, 21].

2.4.2. Fix $a = 20$, $b = 5$, and $d = 10$ and Vary c. When the system parameters and initial conditions of system (6) are $x_0 = y_0 = z_0 = u_0 = 0$, the system parameter c is a varying parameter. When parameter c belongs to [0, 15] and increases gradually, the Lyapunov exponent spectra and the corresponding bifurcation diagram of the state are shown in Figures 8 and 9, respectively. It can be observed from Figure 8 that the memcapacitor-based chaotic circuit has a positive Lyapunov exponent ($LE_1 > 0$), which implies that this system should be in a chaotic state, and the bifurcation behavior is produced in Figure 9. In addition, several periodic windows have been generated within the chaotic region of $c \in [0, 15]$. It is obvious that Figure 10(a) ($c = 8$) and Figure 10(b) ($c = 12$) are observed complicated state phenomena in the memcapacitor-based chaotic circuit, respectively. In the numerical simulation analysis, the initial states (1, 0, 1, −1) and (2, 1, 0.1, 1) are implemented, and the trajectories are shown in Figure 10 by the blue curve and the red curve, respectively [28, 32].

2.5. Realization of the Circuit. In this section, the basic complex dynamic characteristics of chaotic system (6) are realized by experimental circuit by Spice in Figure 11. The circuit in Figure 11 can be used as a schematic diagram to study system (6)'s parameters and characteristics and has certain theoretical significance. The schematic diagram consists of resistors, capacitors, operational amplifiers, analog multipliers, and peripheral circuits. The resistors and capacitance values are chosen as $R_1 = R_2 = R_3 = R_6 = R_7 = R_8 = R_9 = R_{10} = R_{11} = R_{12} = R_{13} = R_{14} = R_{15} = R_{16} = R_{17} = R_{18} = R_{19} = R_{20} = R_{21} = R_{22} = R_{23} = 1\ \text{K}\Omega$, $R_4 = 20\ \text{K}\Omega$, $R_5 = 0.5\ \text{K}\Omega$, $C_1 = 1\ \text{mF}$, $C_2 = C_3 = C_4 = 0.1\ \text{mF}$, $V_1 = 1\ \text{V}$, $V_2 = 0.1\ \text{V}$, $V_3 = 10\ \text{V}$, and $V_4 = 0.09\ \text{V}$.

Furthermore, the motion trajectories of the physical circuit are observed by oscilloscope in Figure 12. The images of the oscilloscope are consistent with the simulation images of MATLAB, which proves the correctness of system (6).

3. Preparatory Theory

3.1. DNA Sequence. A DNA sequence has four nucleic acids, which are adenine (A), cytosine (C), guanine (G), and thymine (T). A is complement to T, and C is complement to G. As we all know, 0 and 1 complement each other in binary numbers, so that 00 and 11, 01 and l0 are complementary, respectively. Therefore, one way to encode 00, 11, 01, and 10 using DNA bases is A, T, C, and G, respectively. Using this way, due to each pixel of an image can be represented by 8-bit binary digits, each pixel value can be expressed as a DNA sequence with a length of 4. For example, if the gray scale value of an image pixel is 210, its binary value 11010010 can be DNA encoded as TCAG, from which pixel value can be obtained back through DNA decoding by replacing DNA bases with their binary sequences. Obviously, there are 24 kinds of coding schemes. But there are only 8 kinds of coding schemes that satisfy the Watson–Crick complementary base pairing rule shown in Table 1. Because the color image could be divided into three channels, which are red channel, green channel, and blue channel, the three channels can be represented by using the DNA codes. The following base operations and transformation rules are defined at the same time.

3.2. Value Generation. In communication theory, the Hamming distance, named after Richard Hamming, is the number of positions in two strings of equal length for which the corresponding elements are different. Put another way, it measures the minimum number of substitutions required to change one into the other. The Hamming distance is used in

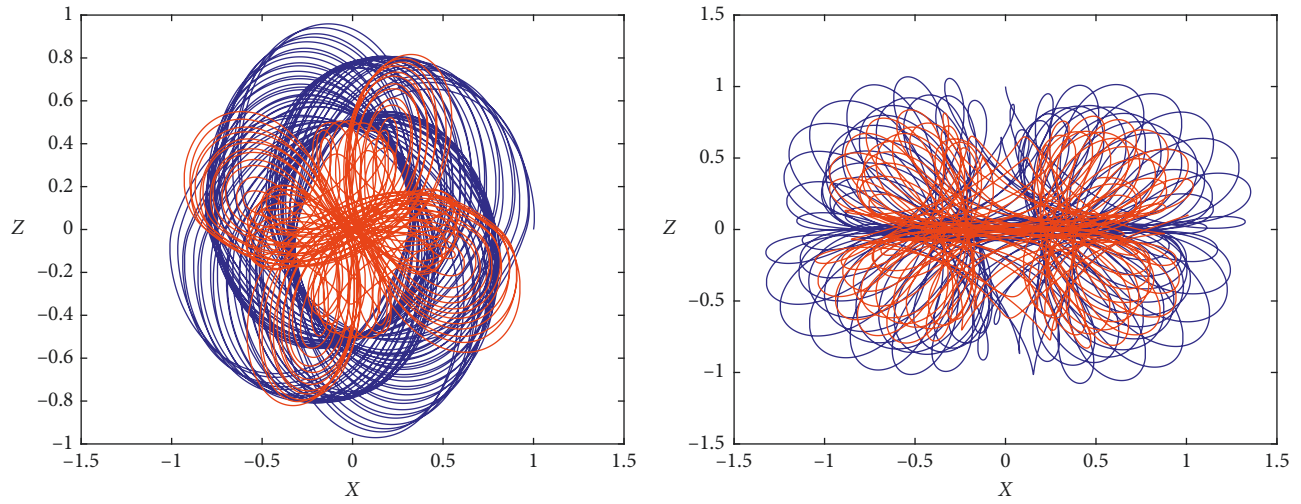


Figure 7: Phase portrait of system (6) with different circuit parameters (a) $a = 18$ and (b) $a = 23$.

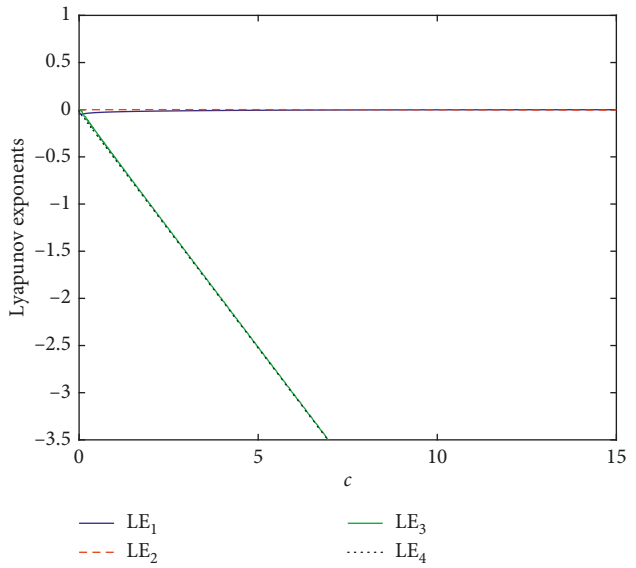


Figure 8: Lyapunov exponents of chaotic system (6) versus parameter c.

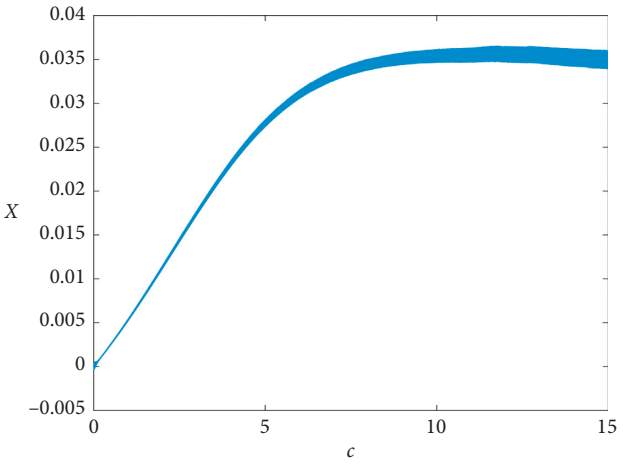


Figure 9: Bifurcation diagrams of chaotic system (6) versus parameter c.

telecommunication to count the number of flipped bits in a fixed-length binary word, an estimate of error, and so is sometimes called the signal distance. Hamming weight analysis of bits is used in several disciplines including information theory, coding theory, and cryptography. The Hamming distance $H(x, y)$ of sequence $x = \{x_1, x_2, \ldots, x_n\}$ and $y = \{y_1, y_2, \ldots, y_n\}$ can be defined as

$$\begin{cases} h(x_i, y_i) = \begin{cases} 0, & x_i = y_i, \\ 1, & x_i \neq y_i, \end{cases} \\ H(x, y) = \sum_{i=1}^{n} h(x_i, y_i). \end{cases} \tag{11}$$

The first set of hash values produced by SHA-3 was used as key K, which was used to generate the initial value of the memcapacitor system. The hash values produced by SHA-3, even if the original image has one bit difference, the hash values and the key will be completely different. The antiattack is 2^{256}, and the generated key has the advantage of randomness, periodicity, and long key space in the way. Combining the original image information with the key, the algorithm will effectively resist the known plaintext attacks. Divide K by byte, which can be expressed as $b_1, b_2, b_3, \ldots, b_{32}$. The initial value of the memcapacitor chaotic system is computed by

$$\begin{cases} x_0 = \alpha + 2 * H(C_1, C_2) - \dfrac{C_2}{4}, \\ y_0 = \beta + 2 * H(C_1, C_2) - \dfrac{C_3}{4}, \\ z_0 = \gamma + 2 * H(C_1, C_2) - \dfrac{C_4}{4}, \\ u_0 = \delta + 2 * H(C_1, C_2) - \dfrac{C_1}{4}, \end{cases} \tag{12}$$

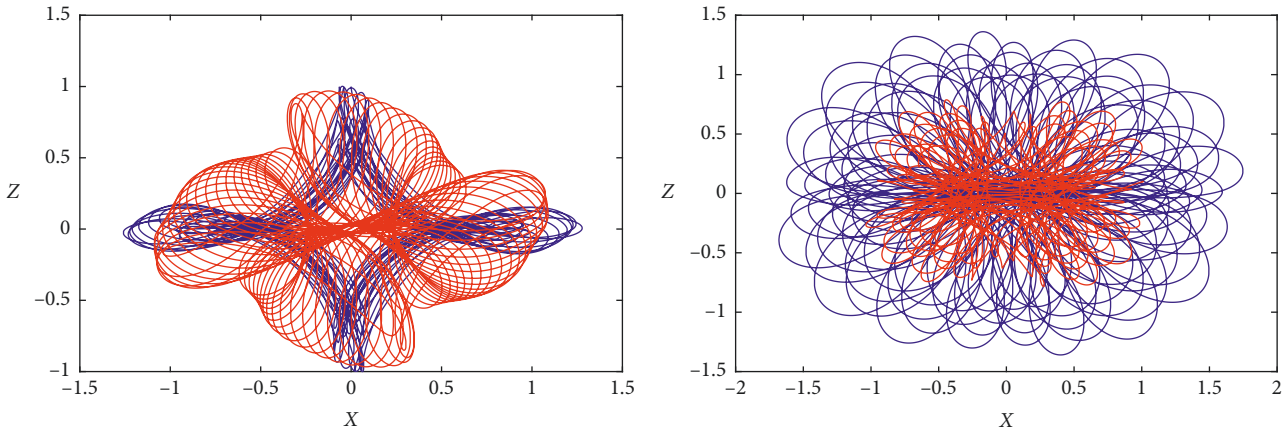


Figure 10: Phase portrait of system (6) with different circuit parameters (a) $c = 8$ and (b) $c = 12$.

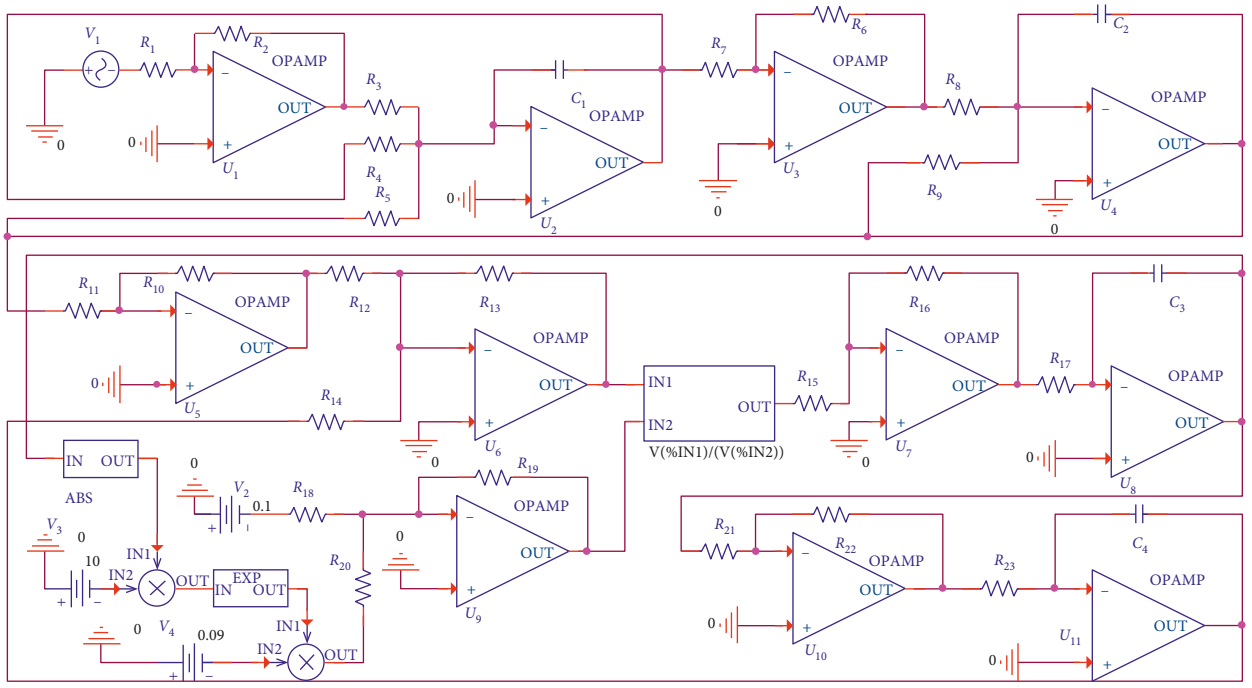


Figure 11: Realization of the circuit by Spice.

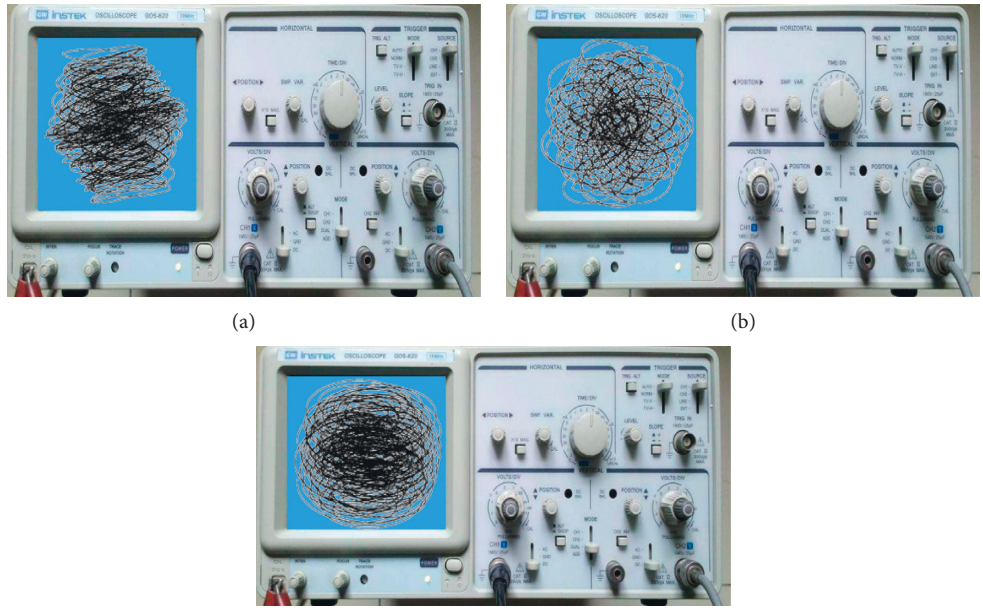
where $C_1 = b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_5 \oplus b_6 \oplus b_7 \oplus b_8$, $C_2 = b_9 \oplus b_{10} \oplus b_{11} \oplus b_{12} \oplus b_{13} \oplus b_{14} \oplus b_{15} \oplus b_{16}$, $C_3 = b_{17} \oplus b_{18} \oplus b_{19} \oplus b_{20} \oplus b_{21} \oplus b_{22} \oplus b_{23} \oplus b_{24}$, and $C_4 = b_{25} \oplus b_{26} \oplus b_{27} \oplus b_{28} \oplus b_{29} \oplus b_{30} \oplus b_{31} \oplus b_{32}$ and α, β, γ, and δ are given values.

3.3. Dynamic DNA Encoding. On the basis of the above theories, the DNA encoding is given. Reference to Table 1, we know that there are eight different encoding rules in the DNA computation. Dynamic DNA coding technology is based on the position of the matrix to be encoded in the image matrix I. The plain image is $m * n$ grayscale image, where each pixel is represented using a byte. The pixel values in the plain image according to formula (13) are encoded:

$$r_{i,j} = (\text{round}(\text{mod}((i-1)) * n + j, 8)) + 1, \quad (13)$$

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

3.4. Elliptic Curve. The application of elliptic curves to the field of cryptography has been relatively recent. Elliptic curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC needs smaller keys compared to non-ECC to provide equivalent security. Nowadays, elliptic curves are



(a) (b)

(c)

Figure 12: Debugging diagram of oscilloscope.

Table 1: 8 kinds of schemes encoding rule of DNA sequence.

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

used in key agreement, digital signatures, pseudorandom generators, and other tasks.

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

$$y_2 + a_1xy + a_3y = x_3 + a_2x_2 + a_4x + a_6. \quad (14)$$

F is a domain, where $a_i \in F$ ($i = 1, 2, 3, 4$, and 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 can be 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.

There are two kinds of elliptic curves that are often used: the elliptic curves with prime values on the prime number domain F_p, where P is the odd prime number, and the elliptic curve on the finite field ${F_2}^m$ with the eigenvalue 2. The elliptic curve used in this paper is the eigenvalue with prime number domain F_p. In F_p, an elliptic curve L with a large prime number factor is randomly searched, and the base point $G_0 = (x'_0, y'_0)$ of the prime number p on E. a and b are the parameters of the elliptic curve L. The elliptic curve L defined on the prime number domain F_p is

$$y^2 = x^3 + ax + b \,(\mathrm{mod}\ p), \quad (15)$$

where $a, b \in F_p$ and satisfy $4a^2 + 27b^3 \neq 0 \,(\mathrm{mod}\ p)$ and p is the order of the elliptic curve.

Key generation: each user generates its own key; the sender Alin randomly selects an integer d_a as the private key in the M sequence and $1 \leq d_a \leq p - 1$ and the receiver Bill randomly selects an integer d_b as the private key in the M sequence and $1 \leq d_b \leq p - 1$. If the public key of the sender Alin is $P_a = d_aG_0$ and the public key of the receiver Bill is $P_b = d_bG_0$, then $d_a * P_b = d_b * P_a = (x', y')$. d_a and d_b are the private keys of the users Alin and Bill, respectively. P_a and P_b are the public keys of Alin and Bill, respectively.

3.5. Hill Encryption Matrix. In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical to operate on more than three symbols at once. The Hill code is a replacement code. The key to the Hill code is the encryption matrix. If the encryption matrix is irreversible, the ciphertext will not be restored to the plaintext. In this paper, the elliptic curve and M sequence are used to construct the encryption matrix.

The image to be encrypted is grouped by 8 pixels, and each group of pixels is converted into an 8×1 matrix I_{8*1}. By constructing an 8×8 reversible matrix K, Hill encryption is performed for each group of images. The encryption formula is as follows:

$$E = (K * I)\text{mod}256 = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{17} & k_{18} \\ k_{21} & k_{22} & \cdots & k_{27} & k_{28} \\ \vdots & \vdots & & \vdots & \vdots \\ k_{71} & k_{72} & \cdots & k_{77} & k_{78} \\ k_{81} & k_{82} & \cdots & k_{87} & k_{88} \end{bmatrix} * \begin{bmatrix} I_{11} \\ I_{21} \\ I_{31} \\ I_{41} \\ I_{51} \\ I_{61} \\ I_{71} \\ I_{81} \end{bmatrix} \text{mod}256 \begin{bmatrix} E_{11} \\ E_{21} \\ E_{31} \\ E_{41} \\ E_{51} \\ E_{61} \\ E_{71} \\ E_{81} \end{bmatrix}, \tag{16}$$

where E is the result of Hill encryption, $I_{11\sim81}$ is a set of pixels to be encrypted, and $k_{11\sim88}$ is the Hill encryption matrix K. The ciphertext is decrypted by using the inverse matrix K^{-1} of K, $I = (K^{-1} * E)$ mod256$= (K * E)$ mod256. The encryption matrix K is divided into four parts:

$$K = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}, \quad K_{11} = \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{bmatrix}. \tag{17}$$

(1) $(x', \ y') = d_a * P_b = d_b * P_a$, $(k_{11}, \ k_{12}) = x'G_0$, $(k_{13}, k_{14}) = m_1G_0$, $(k_{21}, k_{22}) = m_2G_0$, $(k_{23}, k_{24}) = m_3G_0$, $(k_{31}, k_{32}) = m_4G_0$, $(k_{33}, k_{34}) = m_5G_0$, $(k_{41}, k_{42}) = m_6G_0$, $(k_{43}, k_{44}) = y'G_0$, and the submatrix K_{11} is obtained. m_1, $m_2, \ldots, m_6$ are the first six elements in the M_1 sequence.

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

(3) Submatrix $K_{22} = I - K_{12}$.

(4) Submatrix $K_{21} = (I + K_{12})$.

(5) The generated four submatrixes K_{11}, K_{12}, K_{21}, and K_{22} are merged to obtain the reversible cipher matrix K.

4. Encryption Algorithm

The image encryption algorithm is based on the proposed memcapacitor chaotic system and DNA encoding. The encryption algorithm is given as follows. At first, the original image is processed and generates a set of hash values by the SHA-3 algorithm. The generated hash value and original image are performed XOR operation. The hash values are processed to generate the initial value of the chaotic system by the Hamming distance. Then, the image pixels are dynamically encoded and converted to DNA sequences. Furthermore, the elliptic curve with the hyperchaotic sequence is used to construct the Hill encryption matrix, and the plaintext image is permuted and encrypted. At last, the proposed chaotic system is used to scramble the image again. The cryptographic flowchart is shown in Figure 13. The specific encryption steps are as follows:

(1) Input the grayscale image matrix $V(m * n)$

(2) The original image is splitted into unit pixels and encrypted according to the DNA encoding rules

(3) Hash function is used to calculate the hash value of the image matrix V, and the hash values generated and original image are performed XOR operation in Table 2, and the XOR results are encrypted according to the left cyclic shift 3 bits

(4) The first set of hash values produced by SHA-3 was used as key K, and then divide K by byte, and the four sequences C_1–C_4 are obtained

(5) For the encrypted image V, divide every 8 pixels into a block, according to formulas (11) and (12), the initial values of the chaotic system are obtained

(6) The image pixels are dynamically encoded and converted to DNA sequences according to formula (13)

(7) The elliptic curve with the hyperchaotic sequence is used to construct the Hill encryption matrix by Sections 3.4. and 3.5, and the matrix value obtained is shifted

(8) The proposed chaotic system is used to scramble the image again, and the results are encoded by the DNA encoding rule

5. Experiments and Analysis

In this section, simulation results indicate the effectiveness and feasibility of the above algorithm. An indexed image Lena of size 256×256 is used as a original image in Figure 14(a), we use MATLAB 2017*a* to simulate the experiment, and in our experiment, we set $\alpha = 0$, $\beta = 0$, $\gamma = 0$, and $\delta = 0$. The encrypted image is shown in Figure 14(b).

5.1. Secret Key Space Analysis. In this section, the performance and security of the proposed encryption scheme will be discussed and analyzed through several aspects. A good encryption algorithm should have a large key space to make it resist exhaustively and attack effectively.

In this algorithm, it consists of four types of key parameters, which are α, β, γ, and δ and 256 bytes of the SHA-3 function. However, the calculation accuracy of α, β, γ, and δ is 10^{14}, respectively. The key space of the memcapacitor system is $10^{14} \times 10^{14} \times 10^{14} \times 10^{14}$, and the key space of SHA-3 (256 bytes) is 2^{128}. The total key space is $10^{56} \times 2^{128} \approx 3.4 \times 10^{94}$, which shows the algorithm has a sufficiently large key space to resist the brute force attack.

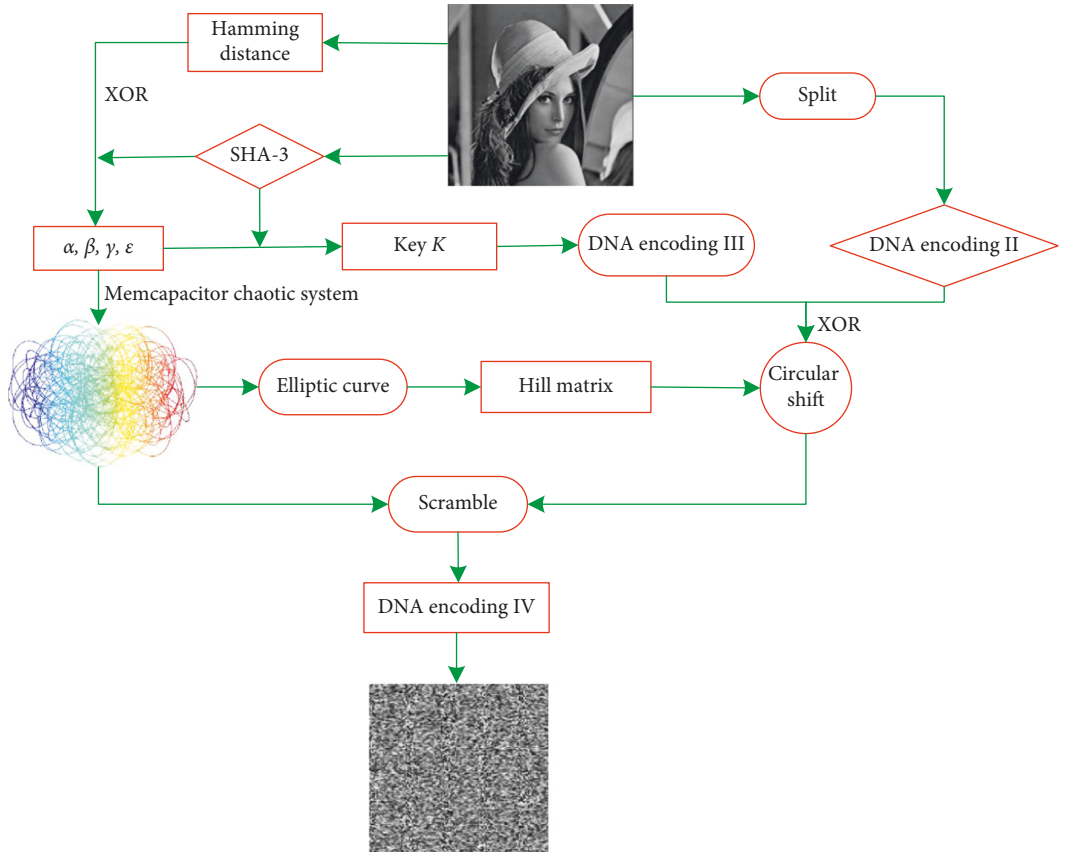
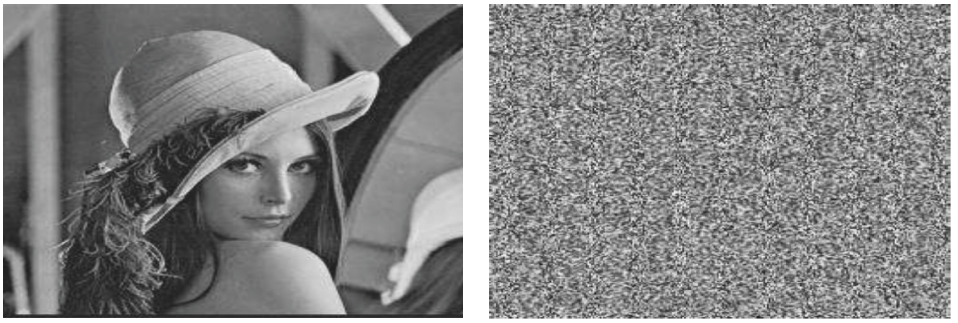


Figure 13: Encrypted flowchart.

Table 2: XOR operation for DNA sequences.

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



(a) (b)

Figure 14: Encrypted Lena image. (a) Original Lena image. (b) Encrypted Lena image.

5.2. Sensitivity Analysis. An ideal cryptosystem should be of high sensitivity, including key sensitivity and plaintext sensitivity. Key sensitivity means that a tiny change of the secret key should produce a completely different encrypted image or the decryption will fail even via using a slight change key. In order to evaluate the key sensitivity of the proposed algorithm, the following key sensitivity tests have been performed. Figures 15(a)–15(d) show the recovering

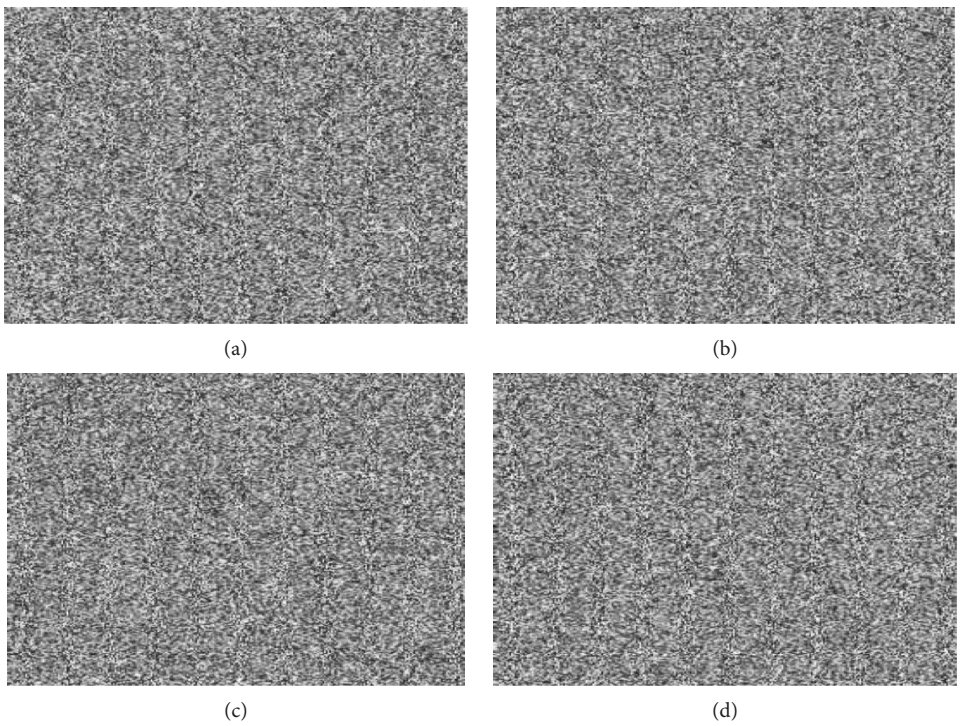


FIGURE 15: The recovering image under the worry secret key. (a) $\alpha = 0.00001$, other parameters are unchanged. (b) $\beta = 0.00001$, other parameters are unchanged. (c) $\gamma = 0.00001$, other parameters are unchanged. (d) $\delta = 0.00001$, other parameters are unchanged.

images when only one of the initial values from four chaotic systems add 0.00001, respectively. Figure 16 shows the decrypted image under the wrong DNA encoding rule. Only when the decryption key is consistent with the encryption key can the image be decrypted properly. The different results show that our algorithm has excellent sensitivity.

5.3. Differential Attack. Plaintext sensitive means that a tiny disturbance of the plain image will lead to dramatic changes in the cipher image. In order to measure the difference between the resulting cipher images, NPCR (number of pixel change rate) and UACI (unified average change intensity) are usually used to detect the ability of the image encryption scheme. NPCR and UACI are defined by

$$\begin{cases} \text{NPCR} = \dfrac{\sum_{i=1}^{m}\sum_{j=1}^{n} C(i,j)}{m \times n} \times 100\%, \\ \\ \text{UACI} = \dfrac{\sum_{i=1}^{m}\sum_{j=1}^{n} \left| P_1(i,j) - P_2(i,j) \right|}{255 \times m \times n} \times 100\%, \end{cases} \tag{18}$$

$$c(i,j) = \begin{cases} 0, & \text{if } P_1(i,j) = P_2(i,j), \\ 1, & \text{if } P_1(i,j) \neq P_2(i,j), \end{cases} \tag{19}$$

where m and n represent the length and width of the image, respectively. $P_1(i, j)$ and $P_2(i, j)$ represent the corresponding ciphertext pixel values before and after the change of plaintext. For Lena images as shown in Table 3, the NPCR and UACI values of the algorithm are 99.62% and 33.38%, respectively, which verifies that the image encryption scheme has the ability to resist differential attack.

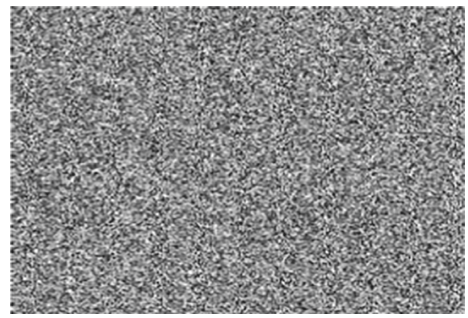


FIGURE 16: The recovering image under the worry DNA encoding rule.

5.4. Histogram Analysis. The image histogram is a method to evaluate the intensity distribution of pixels within one channel in color image, whose distribution shows a good permutation in an encryption algorithm and a high security against the potential statistical attack. The histograms of plain image and encrypted image are shown in Figure 17. Figure 17(a) with a disorder distribution represents the histogram of plain image. The rests with a distribution shows the result after encryption in Figure 17(b). Obviously, no useful information can be extracted from the encrypted image, and high security can be guaranteed to resist statistical attacks.

Table 3: Comparison of NPCR and UACI in this paper and other references.

	NPCR (%)	UACI (%)
Ours	99.62	33.38
Ref. [2]	99.02	32.83
Ref. [15]	99.59	33.12

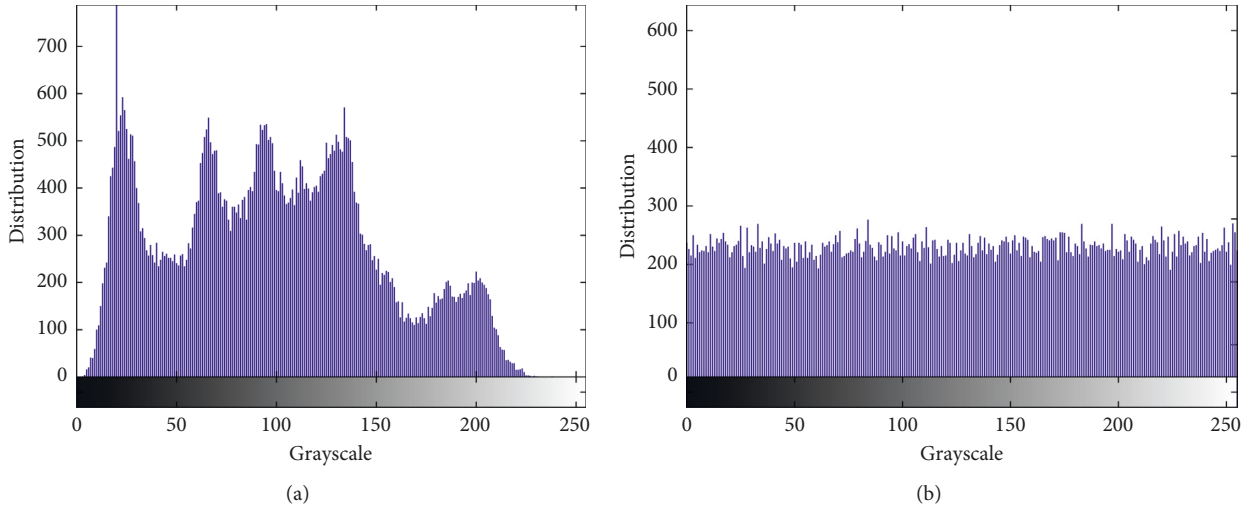


Figure 17: Histogram of (a) plain image and (b) encrypted image.

5.5. Correlation Coefficient Analysis. Correlation coefficient is an index to assess the image randomness. In this paper, it is employed to test the correlation between two adjacent pixels in plain image and ciphered image. In the original image, the correlation between two adjacent pixels is very high. In order to resist statistical attacks, the correlation of encrypted images must be reduced. 2500 pairs of two adjacent pixels are randomly selected from the plain and encryption image in horizontal, vertical, and diagonal directions to calculate the correlation between pixels. The function to calculate the correlation coefficient is shown as follows:

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

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

$$\mathrm{COV}(x, y) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)\left(y_i - E(x)\right), \tag{20}$$

$$r_{xy} = \frac{\mathrm{COV}(x, y)}{\sqrt{D(x)} \times \sqrt{D(y)}},$$

where x and y are values of two adjacent pixels selected in three directions randomly. N is the total number of duplets (x, y) obtained from the image. $E(x)$ and $D(x)$ are the expectation and the variance of x, respectively.

The calculated correlation coefficients of plaintext images of Lena and its corresponding ciphered images in the proposed algorithm are listed in Table 4. The correlation coefficient of adjacent pixels of the encrypted image is −0.000534. Therefore, the image encryption algorithm has a strong ability to resist statistical attacks. Table 4 and Figure 18 show the correlation comparison between the original image and the adjacent pixel of the encrypted image.

5.6. Information Entropy. The information entropy can test uncertainty. Entropy reflects whether grayscale values distribution is random or equality. The minimum and maximum values of entropy are zero and eight, respectively. The more uniform the distribution of the image gray value, the greater the entropy of the image. Therefore, the entropy value of the encrypted image should be as high as possible. Let m be the information source, and the equation for calculating information entropy is

$$H(m) = -\sum_{t=0}^{t} P(m_i)\log_2 P((m_i)), \tag{21}$$

where $P(m_i)$ represents the probability that the information m_i appears. Assume that there are 28 states of the information source and they appear with the same probability, according to formula (21), we can get the ideal $H(m) = 8$, which shows that the information is random. Hence, the information entropy of the encrypted image should be close to 8. The value of information entropy of the ciphered image in the proposed scheme is 7.98928, which indicate that the

Table 4: The correlation of the adjacent pixels for original and encrypted image.

Correlation coefficient	Horizontal	Vertical	Diagonal
Original image	0.9689	0.9486	0.9228
Encrypted image	−0.0029	−0.0031	−0.0037
Ref. [2]	0.0085	0.0021	0.0012
Ref. [15]	0.0265	0.0792	0.0625

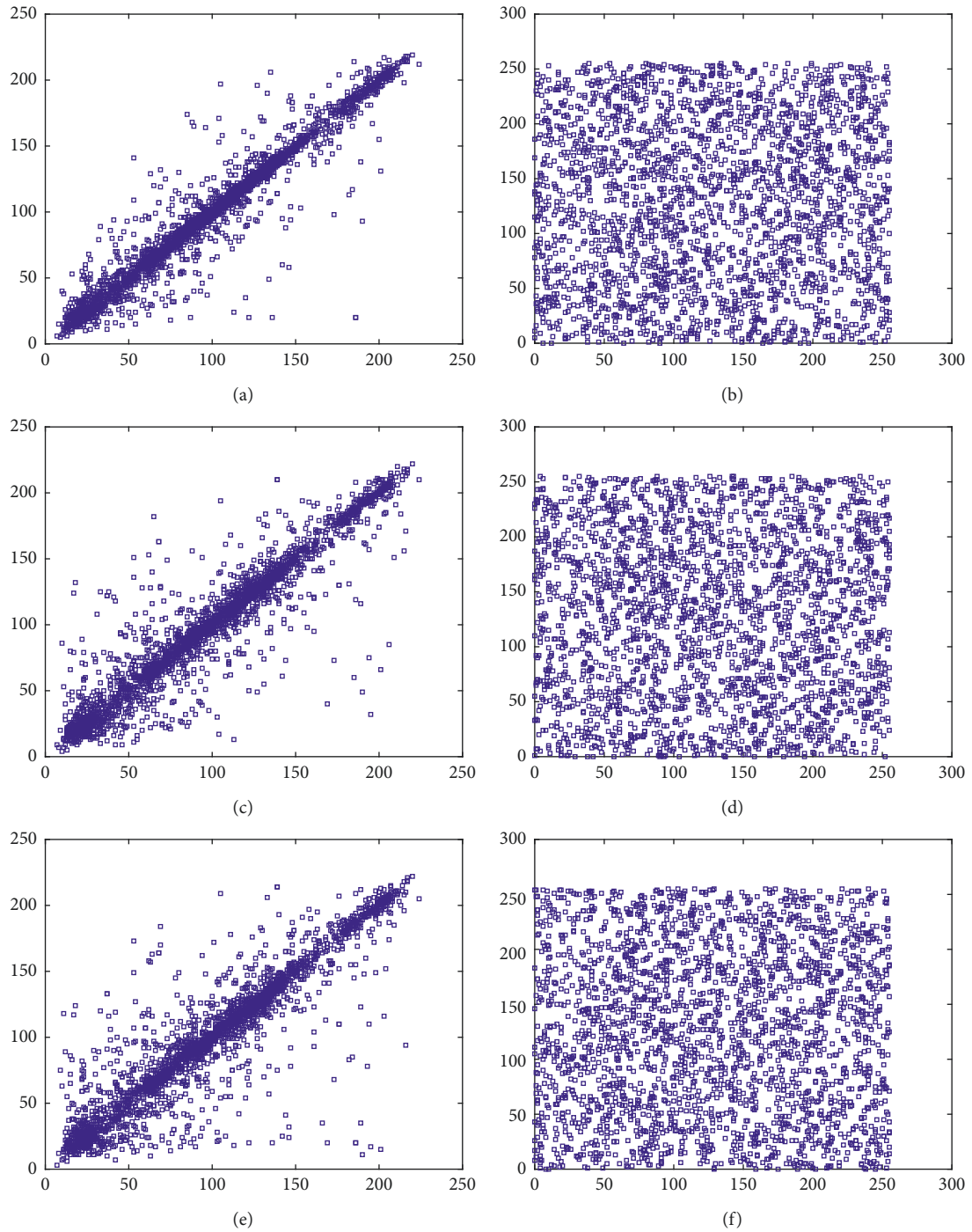


Figure 18: Correlation analysis of image: (a) plain image in horizontal; (b) cipher image in horizontal; (c) plain image in vertical; (d) cipher image in vertical; (e) plain image in diagonal; (f) cipher image in diagonal.

ciphered image obtained by the proposed algorithm could hardly divulge information.

6. Conclusion and Future Work

In this paper, a novel base on the memcapacitor chaotic system is proposed, and the waveform of the state variable is given. Moreover, the dynamic characteristics of the system are analyzed in detail, which indicate that the system has abundant dynamic behaviors. The corresponding implementation circuit is constructed by Spice. On this basis, a novel image encryption algorithm based on DNA sequence encoding operation and chaotic system is proposed. The Hill encryption matrix is constructed by the combination of the elliptic curve and hyperchaotic system, which avoids the complexity of elliptic curve encryption and reduces the correlation between encryption matrix elements. So, the encryption matrix has much more randomicity, and the encryption algorithm is more complex. Combined with the dynamic DNA encoding rules, the security of the encryption algorithm is increased, and the correlation between pixels is reduced, which makes the ciphertext difficult to crack. Experimental results show that this algorithm has better encryption effect, larger key space, and higher sensitivity to key.

Compared with the previous encryption algorithm [2, 15], the computational time is reduced by 30%, and it has better rapidity and convenience. In addition, the algorithm can resist exhaustive attack, statistical attack, and differential attack. All these features show that our algorithm is very suitable for digital image encryption. In the future, we intend to carry encryption computation for images if necessary. The specific application and algorithm exploration are our future work.

Data Availability

The contents of the article are examined and updated, and the data can be used by readers in this paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work was supported by the State Key Program of National Natural Science of China (Grant no. 61632002), the National Natural Science of China (Grant nos. 61572446, 61472372, 61603348, and 61602424), Science and Technology Innovation Talents Henan Province (Grant no. 174200510012), Research Program of Henan Province (Grant nos. 15IRTSTHN012, 162300410220, and 17A120005), and the Science Foundation for Doctorate Research of Zhengzhou University of Light Industry (Grant no. 2014BSJJ044).

References

[1] H. Al-Dmour and A. Al-Ani, "Quality optimized medical image information hiding algorithm that employs edge detection and data coding," *Computer Methods and Programs in Biomedicine*, vol. 127, pp. 24–43, 2016.

[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 and Lasers in Engineering*, vol. 71, pp. 33–41, 2015.

[3] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[4] W. L. Chang, Q. Yu, Z. K. Li et al., "Quantum speedup in solving the maximal-clique problem," *Physical Review A*, vol. 97, no. 3, 2018.

[5] W. L. Chang and A. V. Vasilakos, "DNA algorithms of implementing biomolecular databases on a biological computer," *IEEE Transactions on Nanobioscience*, vol. 14, no. 1, pp. 104–111, 2015.

[6] V. Siddaramappa and K. B. Ramesh, "DNA-Based XOR operation (DNAX) for data security using DNA as a storage medium," *Integrated Intelligent Computing, Communication and Security*, vol. 771, pp. 343–351, 2019.

[7] W. L. Chang, T. T. Ren, and M. Feng, "Quantum algorithms and mathematical formulations of Bio-molecular solutions of the vertex cover problem in the finite-dimensional Hilbert space," *IEEE Transactions on Nanobioscience*, vol. 14, no. 1, pp. 121–128, 2015.

[8] D. Carmean, L. Ceze, G. Seelig, K. Stewart, K. Strauss, and M. Willsey, "DNA data storage and hybrid molecular-electronic computing," *Proceedings of the IEEE*, vol. 107, no. 1, pp. 63–72, 2019.

[9] W. L. Chang, A. V. Vasilakos, M. Shan et al., "The DNA-based algorithms of implementing arithmetical operations of complex vectors on a biological computer," *IEEE Transactions on Nanobioscience*, vol. 14, no. 8, pp. 1–8, 2015.

[10] Q. Zhang, L. Liu, and X. Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps," *AEU-International Journal of Electronics and Communications*, vol. 68, no. 3, pp. 186–192, 2014.

[11] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, 2012.

[12] S. Hanis and R. Amutha, "A fast double-keyed authenticated image encryption scheme using an improved chaotic map and a butterfly-like structure," *Nonlinear Dynamics*, vol. 95, no. 1, pp. 421–432, 2019.

[13] X. Xue, Q. Zhang, X. Wei, L. Guo, and Q. Wang, "An image fusion encryption algorithm based on DNA sequence and multi-chaotic maps," *Journal of Computational and Theoretical Nanoscience*, vol. 7, no. 2, pp. 397–403, 2010.

[14] K. W. Wong, B. S. H. Kwok, and W. S. Law, "A fast image encryption scheme based on chaotic standard map," *Physics Letters A*, vol. 372, no. 15, pp. 2645–2652, 2008.

[15] 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. 1123–1136, 2016.

[16] Y. Samet, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, 2013.

[17] Y. Zhang and D. Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 74–82, 2014.

[18] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Processing*, vol. 148, pp. 272–287, 2018.

[19] B. Muthuswamy and L. O. Chua, "Simplest chaotic circuit," *International Journal of Bifurcation and Chaos*, vol. 20, no. 5, pp. 1567–1580, 2010.

[20] L. Wang, T. Dong, and M.-F. Ge, "Finite-time synchronization of memristor chaotic systems and its application in image encryption," *Applied Mathematics and Computation*, vol. 347, no. 15, pp. 293–305, 2019.

[21] A. Buscarino, L. Fortuna, M. Frasca et al., "A chaotic circuit based on Hewlett-Packard memristor," *Chaos*, vol. 22, no. 2, pp. 23–36, 2012.

[22] Z. Guo, G. Si, X. Xu et al., "Generalized modeling and character analyzing of composite fractional-order memristors in series connection," *Nonlinear Dynamics*, vol. 95, no. 1, pp. 101–115, 2019.

[23] H. Kizmaz, U. E. Kocamaz, and Y. Uyaroğlu, "Control of memristor-based simplest chaotic circuit with one-state controllers," *Journal of Circuits, Systems and Computers*, vol. 28, no. 1, article 1950007, 2019.

[24] I. E. Ebong and P. Mazumder, "CMOS and memristor-based neural network design for position detection," *Proceedings of the IEEE*, vol. 100, no. 6, pp. 2050–2060, 2012.

[25] F. Yuan, G. Wang, and X. Wang, "Extreme multistability in a memristor-based multi-scroll hyper-chaotic system," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 26, no. 7, article 073107, 2016.

[26] Y. M. Xu, L. D. Wang, and S. K. Duan, "A memristor-based chaotic system and its field programmable gate array implementation," *Acta Physica Sinica*, vol. 65, no. 12, article 120503, 2016.

[27] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 2014.

[28] K. Rajagopal, A. Akgul, S. Jafari, and B. Aricioglu, "A chaotic memcapacitor oscillator with two unstable equilibriums and its fractional form with engineering applications," *Nonlinear Dynamics*, vol. 91, no. 2, pp. 957–974, 2018.

[29] M. D. Ventra, Y. V. Pershin, and L. O. Chua, "Circuit elements with memory: memristors, memcapacitors, and meminductors," *Proceedings of the IEEE*, vol. 97, no. 10, pp. 1717–1724, 2009.

[30] F. Yuan, G. Wang, Y. Shen, and X. Wang, "Coexisting attractors in a memcapacitor-based chaotic oscillator," *Nonlinear Dynamics*, vol. 86, no. 1, pp. 37–50, 2016.

[31] M. S. Wang, A. Ahmadi, and M. Hayati, "Implementation of adaptive neuron based on memristor and memcapacitor emulators," *Neurocomputing*, vol. 309, pp. 157–167, 2018.

[32] G. Wang, C. Shi, X. Wang et al., "Coexisting oscillation and extreme multistability for a memcapacitor-based circuit," *Mathematical Problems in Engineering*, vol. 2017, Article ID 6504969, 13 pages, 2017.