A Unified Framework for Finite-/Fixed-Time Synchronization of Memristor Chaotic Systems and Its Application in Image Encryption

Leimin Wang (wangleimin@cug.edu.cn)
China University of Geosciences https://orcid.org/0000-0002-0663-3365
Shan Jiang
China University of Geosciences
Ming-Feng Ge
China University of Geosciences
Junhao Hu
China University of Geosciences

Research Article

Keywords: Memristor chaotic systems, finite-time synchronization, fixed-time synchronization, slidingmode control, image encryption

Posted Date: April 15th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-397817/v1

Noname manuscript No.
(will be inserted by the editor)

A unified framework for finite-/fixed-time synchronization of memristor chaotic systems and its application in image encryption

Leimin Wang* · **Shan Jiang** · **Ming-Feng Ge** · **Junhao Hu**

Received: date / Accepted: date

Abstract This paper proposes a sliding-mode-based unified control framework to solve the synchronization problem of memristor chaotic systems. Both finite- and fixed-time synchronization of the memristor chaotic systems can be obtained in the uniform framework. According to the Lyapunov stability and finite-time stability theories, we demonstrate that the trajectories of error system reach the presented sliding-mode surface and converge to the origin along the surface in a finite/fixed time. Moreover, an image encryption algorithm is developed based on the presented control framework. Finally, the numerical simulations and the statistical performance analyses are discussed to illustrate the correctness of synchronization results, the effectiveness of the proposed encryption algorithm, and its potential applications in the scope of secure communication.

Keywords Memristor chaotic systems · finite-time synchronization · fixed-time synchronization · sliding-mode control · image encryption

*Corresponding author
Leimin Wang

Leimin Wang · Shan Jiang
School of Automation, China University of Geosciences, Wuhan 430074, China
Hubei key Laboratory of Advanced Control and Intelligent Automation for Complex Systems
E-mail: wangleimin@cug.edu.cn, js0522@cug.edu.cn

Ming-Feng Ge
School of Mechanical Engineering and Electronic Information, China University of Geosciences, Wuhan 430074, China
E-mail: fmgabc@163.com

Junhao Hu
College of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430074, China
E-mail: junhaohu74@163.com

1 Introduction

For a chaotic system, small changes of the initial states cause large deviations of the system response. It thus generates a common belief that chaos is harmful among scientists until 1990 when Pecora and Carroll firstly put forward the theory of chaotic synchronization [1]. Since then, a large number of researchers have devoted great efforts to chaos control theory and chaotic synchronization problem [2–4]. A basic model of chaotic synchronization is the drive-response structure [5], in which the trajectories of the response system are supposed to be synchronized to that of the drive system. In the past decades, various effective synchronization control approaches have been proposed to achieve chaotic synchronization, including the fuzzy control [6–9], impulse control [10–12], adaptive control [13–15], etc.

It is worth pointing out that most of the existing results presented in the early research work can only be used to achieve asymptotic synchronization of chaotic systems [16–20], namely, the states of the chaotic systems reach agreement (i.e., synchronization) as time approaches infinity. This has already become the big obstacle greatly hindering the development and application of the above-mentioned asymptotic synchronization algorithms. To surmount the bottleneck, scholars have paid great efforts to solve the finite-time synchronization (FTS) problem, namely, to synchronize the states of all the chaotic systems to reach agreement in a finite time, which depends heavily on the initial value of the chaotic system [21, 22]. However, the initial value may not be known and used in advance, which prevents the applications of the FTS technology in the case that the upper bound of the convergence time is highly required.

To remove this constraint, significant research findings of fixed-time control theory were presented in [23] to achieve a fixed convergence time regardless of the initial value and only depending on the system parameters and related control parameters. Therefore, the fixed-time synchronization (FxTS) can be achieved in a specific time, which expands the application field when initial values are unknown. Recently, a series of control strategies and synchronization results based on fixed-time control have been reported [24–27]. In [26], a fixed-time control scheme with fast convergence speed which was employed to power systems was proposed. In [27], a unified framework for the finite-time stabilization and fixed-time stabilization of a chaotic system was discussed. The results of the above two papers are derived based on the sliding-mode control (SMC) method. The SMC is a popular control method due to its insensitivity to the changes of system parameters, strong anti-interference ability and fast dynamic response [28]. The time evolutions of the states of the dynamic system are propelled to slide along the desired sliding-mode surface and stay on it by designing an appropriate controller. Based on its high control efficiency, this technology has been widely applied in the field of the synchronization of chaotic systems [29, 30].

More recently, applying the chaotic synchronization theory to realize secure communication has become a hot research topic [31]. It requires the image information to be encrypted as binary data streams by employing some encoding methods. Especially, it is an effective way to use chaotic signals for scrambling the data streams and accomplishing image encryption. In [32], an encryption algorithm based on the synchronization scheme of chaotic systems was proposed, showing its stronger anti-deciphering ability compared to the non-chaotic synchronization ones. In 1971, Prof. Chua predicted the existence of memristor according to the completeness principle of circuit theory [33]. An experiment in HP laboratory successfully confirmed the existence of memristor [34] in 2008. Later, increasing research results prove that the chaotic system based on memristor behaves more complex dynamic behaviors and initial condition sensitivity [35, 36]. In the consequence, combining memristor chaotic system (MCS) with cryptography, high security image encryption algorithms are designed, showing its great application value in image encryption, secure communication and other fields [37, 38].

The special characteristics of memristor make the MCS an effective tool with higher initial value sensitivity, stronger pseudo-random and continuous broadband power spectrum characteristics in contrast to other traditional chaotic systems [39, 40]. Thus, applying the synchronization of MCSs to achieve color image encryption will generate the anti-decoding ability and the key space. In [41], the FTS of MCSs was achieved and used to design an image encryption algorithm. The simulation results indicated that the encryption effect based on MCS had better decryption effect and less data loss compared with the same encryption algorithm based on the generalized chaotic systems. In [42], a new chaotic circuit with multiple memristors was used to implement image encryption. In [43], the proposed MCSs show great security on color image encryption by analyzing the encryption performances.

Inspired by the above analysis, this paper aims to realize the FTS and FxTS of MCSs via a unified control framework. In addition, an effective image encryption algorithm based upon MCSs is devised to show the potential application value. The main contributions of this paper are threefold.

(1) A unified framework based on SMC is proposed to solve the synchronization problem of MCSs.

(2) Different from the separate discussion of FTS and FxTS of MCSs, a unified framework is designed in this paper. By selecting different control parameters in the presented controller, FTS and FxTS of MCSs can be achieved at the same time.

(3) An effective image encryption algorithm is put forward based on the synchronization of MCSs. We prove that the presented algorithm is a suitable choice for different size of general images and has great value for secure communication.

The rest of this paper is arranged as follows. In the second section, the preparation work is introduced. The main results are given in Section 3 and the numerical simulations are presented in Section 4. Section 5 introduces an image encryption algorithm, while its experiment performances are demonstrated in Section 6. Finally, the conclusion is given in Section 7.

2 Preliminaries

2.1 System Description

Based on Chua's circuit [44], a memristor chaotic circuit is constructed as shown in Fig. 1. The mathematical model of the current $I_M(t)$ and the voltage $V_M(t)$ is described as

$$\begin{cases} I_M(t) = \left(\eta z^2(t)\right) V_M(t) \\ \dot{z}(t) = V_M(t) - \xi z(t) \end{cases} \tag{1}$$

where η and ξ are constants, $z(t)$ is the internal state variable of the memristor. According to Kirchhoff's cur-

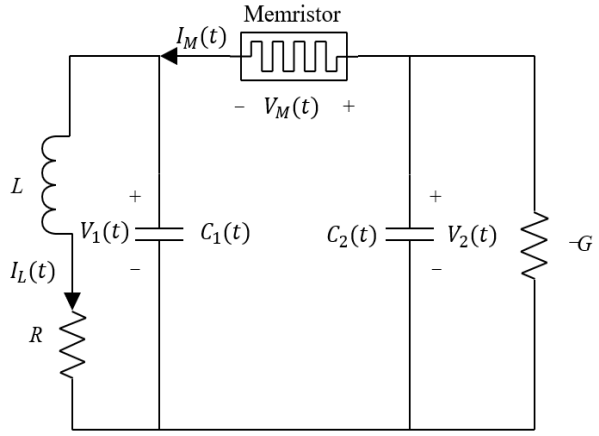


Fig. 1 The memristor chaotic circuit.

rent law, it implies that

$$\begin{cases} \dot{V}_1(t) = \frac{1}{C_1}\left[2z^2(t)\left(V_2(t) - V_1(t)\right) + GV_1(t)\right] \\ \dot{V}_2(t) = \frac{1}{C_2}\left[2z^2(t)\left(V_1(t) - V_2(t)\right) - I_L(t)\right] \\ \dot{I}_L(t) = \frac{1}{L}\left(V_2(t) - RI_L(t)\right) \\ \dot{z}(t) = \left(V_2(t) - V_1(t)\right) - 0.01z(t) \end{cases} \tag{2}$$

where $V_1(t)$ is the voltage across the capacitor C_1 and $V_2(t)$ is the voltage across the capacitor C_2, $-G$ is a negative conductance, L is an inductor, R is a common resistor, and $I_L(\mathrm{t})$ is the current flowing through R and L.

Set $x_1(t) = V_1(t), x_2(t) = V_2(t), x_3(t) = I_L(t), x_4(t) = z(t), a = 1/C_1, b = 1/C_2, c = 1/L, d = G, h = R$. Then

$$\begin{cases} \dot{x}_1(t) = a\left[2x_4^2(t)(x_2(t) - x_1(t)) + dx_1(t)\right] \\ \dot{x}_2(t) = b\left[2x_4^2(t)(x_1(t) - x_2(t)) - x_3(t)\right] \\ \dot{x}_3(t) = c(x_2(t) - hx_3(t)) \\ \dot{x}_4(t) = x_2(t) - x_1(t) - 0.01x_4(t). \end{cases} \tag{3}$$

Set system (3) as the drive system and the corresponding response system is described as

$$\begin{cases} \dot{y}_1(t) = a\left[2y_4^2(t)(y_2(t) - y_1(t)) + dy_1(t)\right] + u_1(t) \\ \dot{y}_2(t) = b\left[2y_4^2(t)(y_1(t) - y_2(t)) - y_3(t)\right] + u_2(t) \\ \dot{y}_3(t) = c(y_2(t) - hy_3(t)) + u_3(t) \\ \dot{y}_4(t) = y_2(t) - y_1(t) - 0.01y_4(t) + u_4(t) \end{cases} \tag{4}$$

where $u_i(t)$ $(i = 1, 2, 3, 4)$ are controllers designed later.

Define the errors as $e_i(t) = y_i(t) - x_i(t)$, $i = 1, 2, 3, 4$. Based on systems (3) and (4), the error dynamic system is expressed as

$$\begin{cases} \dot{e}_1(t) = a[2y_4^2(t)(y_2(t) - y_1(t)) - 2x_4^2(t)(x_2(t) - x_1(t)) \\ \qquad + de_1(t)] + u_1(t) \\ \dot{e}_2(t) = b[2y_4^2(t)(y_1(t) - y_2(t)) - 2x_4^2(t)(x_1(t) - x_2(t)) \\ \qquad - e_3(t)] + u_2(t) \\ \dot{e}_3(t) = c\left(e_2(t) - he_3(t)\right) + u_3(t) \\ \dot{e}_4(t) = e_2(t) - e_1(t) - 0.01e_4(t) + u_4(t). \end{cases} \tag{5}$$

2.2 Definitions and Lemma

Here are some of the important definitions and lemma involved in this paper.

Definition 1 Systems (3) and (4) are said to be synchronized in a finite time, if for any initial state $e(0)$, there exists a finite time $T(e(0)) \in [0, +\infty)$ such that

$$\lim_{t \to T(e(0))} |e_i(t)| = 0, \quad |e_i(t)| \equiv 0 \ (t \geq T(e(0))).$$

Definition 2 Systems (3) and (4) are said to be synchronized in a fixed time, if they are firstly finite-time synchronized, and the settling time $T(e(0))$ is bounded by a positive constant $t_{\max}$ which is independent of the initial state, i.e., $T(e(0)) \leq t_{\max}$.

Remark 1 From the definitions above, the settling time for FTS is related to the initial condition, while the settling time of FxTS is regardless of the initial condition and there is a specific upper limit of the time.

Lemma 1 [45] For any real numbers $\varrho_1, \varrho_2, \ldots, \varrho_n$ and $0 \leq \mu \leq 1, \vartheta > 1$, the following two inequalities hold

$$\sum_{i=1}^{n} |\varrho_i|^{\mu+1} \geq \left(\sum_{i=1}^{n} |\varrho_i|^2\right)^{\frac{\mu+1}{2}}, \tag{6}$$

$$\sum_{i=1}^{n} |\varrho_i|^{\vartheta+1} \geq n^{(1-\vartheta)/2} \left(\sum_{i=1}^{n} |\varrho_i|^2\right)^{(\vartheta+1)/2}. \tag{7}$$

3 Main Results

First of all, a sliding-mode surface (SMS) is devised. Then effective controller is designed to ensure that the system state variables reach the SMS in a finite/fixed time and remain on the surface afterward. The fourth-order SMS is designed as

$$\Gamma = \left\{e(t) | S(t) = (S_1(t), \ldots, S_4(t))^T = 0\right\}. \tag{8}$$

The state variables of the designed fourth-order SMS are given as

$$S_i(t) = \gamma_i e_i(t) + \int_0^t \left(|e_i(\tau)|^{v_1} + |e_i(\tau)|^{v_2}\right) \mathrm{sign}\left(e_i(\tau)\right) d\tau \tag{9}$$

where $\gamma_i > 0 (i = 1, 2, 3, 4), 0 \leq v_1 < 1, v_2 \geq 0$, $\mathrm{sign}(\cdot)$ is the signum function. And the derivation of (9) is

$$\dot{S}_i(t) = \gamma_i \dot{e}_i(t) + \left(|e_i(t)|^{v_1} + |e_i(t)|^{v_2}\right) \mathrm{sign}\left(e_i(t)\right). \tag{10}$$

It is assumed that the system state variables are able to arrive at the surface Γ within a finite/fixed time T_1. From the equivalent condition for existence of the sliding-mode, it implies that

$$S_i(t) = \dot{S}_i(t) = 0, \tag{11}$$

for all $t \geq T_1$. It implies that

$$\dot{e}_i(t) = -\frac{1}{\gamma_i} \left(|e_i(t)|^{v_1} + |e_i(t)|^{v_2}\right) \mathrm{sign}\left(e_i(t)\right). \tag{12}$$

The state variables of system (5) converge to the SMS within a finite/fixed time T_1 firstly. After reaching the surface, system (12) is activated and its state variables tend to zero within another finite/fixed time T_2. As a result, the settling time T satisfies $T = T_1 + T_2$.

3.1 Reachability of the SMS

In this part, a suitable controller is designed first. Then reachability of SMS Γ will be discussed next. The controller is described as

$$\begin{cases} u_1(t) = -\frac{1}{\gamma_1}(|e_1(t)|^{v_1} + |e_1(t)|^{v_2})\mathrm{sign}(e_1(t)) - a|(y_2(t) \\ \quad -y_1(t))2y_4^2(t) - 2x_4^2(t)(x_2(t) - x_1(t)) + de_1(t)| \\ \quad -(\alpha + |S_1(t)|^{v_2})\mathrm{sign}(S_1(t)) \\ u_2(t) = -\frac{1}{\gamma_2}(|e_2(t)|^{v_1} + |e_2(t)|^{v_2})\mathrm{sign}(e_2(t)) - b|(y_1(t) \\ \quad -y_2(t))2y_4^2(t) - 2x_4^2(t)(x_1(t) - x_2(t)) - e_3(t)| \\ \quad -(\alpha + |S_2(t)|^{v_2})\mathrm{sign}(S_2(t)) \\ u_3(t) = -\frac{1}{\gamma_3}(|e_3(t)|^{v_1} + |e_3(t)|^{v_2})\mathrm{sign}(e_3(t)) - c|e_2(t) \\ \quad - he_3(t)| - (\alpha + |S_3(t)|^{v_2})\mathrm{sign}(S_3(t)) \\ u_4(t) = -\frac{1}{\gamma_4}(|e_4(t)|^{v_1} + |e_4(t)|^{v_2})\mathrm{sign}(e_4(t)) - |e_2(t) \\ \quad - e_1(t) - 0.01e_4(t)| - (\alpha + |S_4(t)|^{v_2}\mathrm{sign}(S_4(t)) \end{cases} \tag{13}$$

where α is a positive constant.

Theorem 1 The state variables of system (5) by employing the designed control rules (13) move to the SMS Γ and reach on it within a finite/fixed time T_1 satisfying

$$T_1 \leq \begin{cases} \min\left\{\frac{\|S(0)\|}{\alpha\check{\gamma}}, \frac{\|S(0)\|^{1-v_2}}{\check{\gamma}(1-v_2)}\right\}, & 0 \leq v_2 < 1 \\ \frac{1}{\check{\gamma}} \ln\left(1 + \frac{1}{\alpha}\|S(0)\|\right), & v_2 = 1 \\ \frac{\sqrt{2}}{\alpha\check{\gamma}} + \frac{2^{\frac{v_2-1}{2}}}{\check{\gamma}(v_2-1)}, & v_2 > 1 \end{cases} \tag{14}$$

where $\check{\gamma} = \min\{\gamma_i\}$, $\|\cdot\|$ denotes the Euclidean norm.

Proof The proof process with detailed mathematical reasoning is shown in Appendix I.

Remark 2 In (14), the upper bound of T_1 depends on the initial condition $\|S(0)\|$ and T_1 is a finite time when $0 \leq v_2 \leq 1$. For $v_2 > 1$, the upper bound of T_1 depends on the values of parameters α, $\check{\gamma}$ and v_2 and is independent of the initial condition, namely T_1 is a fixed time.

3.2 Stability of System Dynamics

Theorem 2 The system (12) is stable within a finite/fixed time T_2 satisfying

$$T_2 \leq \begin{cases} \min\left\{\frac{\hat{\gamma}\|e(0)\|^{1-v_1}}{1-v_1}, \frac{\hat{\gamma}\|e(0)\|^{1-v_2}}{1-v_2}\right\}, & 0 \leq v_2 < 1 \\ \frac{\hat{\gamma}}{1-v_1} \ln\left(1 + \|e(0)\|^{1-v_1}\right), & v_2 = 1 \\ \frac{\hat{\gamma}\cdot 2^{\frac{1-v_1}{2}}}{1-v_1} + \frac{\hat{\gamma}\cdot 2^{\frac{v_2-1}{2}}}{v_2-1}, & v_2 > 1 \end{cases} \tag{15}$$

where $\hat{\gamma} = \max\{\gamma_i\}$.

Proof See Appendix II.

Remark 3 In (15), the upper bound of T_2 relies on the initial condition $\|e(0)\|$ and T_2 is a finite time when $0 \leq v_2 \leq 1$. For $v_2 > 1$, the upper bound of T_2 is only related to the values of parameters $\hat{\gamma}$, v_1 and v_2, namely T_2 is a fixed time independent of the initial condition.

On the SMS, the equivalent system (12) along the surface is able to realize finite-time stability or fixed-time stability as v_2 takes different values. According to the theoretical results in Theorems 1 and 2, the conclusion is obtained that systems (3) and (4) can realize FTS or FxTS within the settling time $T = T_1 + T_2$.

Remark 4 Different from the FTS and FxTS results of the chaotic system separately studied in [21, 26, 46], this paper puts forward a unified framework to realize the FTS and FxTS of the chaotic system simultaneously. In the meanwhile, the formulas for calculating the theoretical settling time range in different cases are also given.

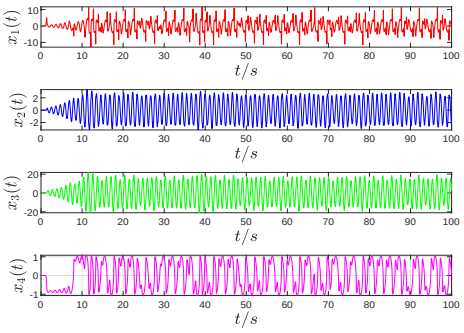


Fig. 2 The trajectories of the state variables in system (3).

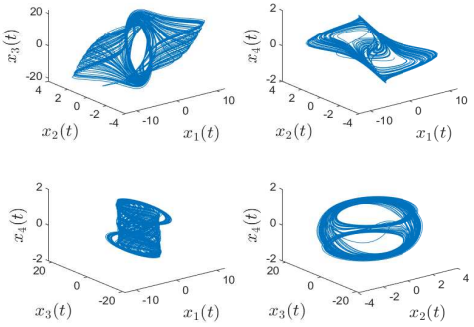


Fig. 3 The attractor phase diagrams of the memristor chaotic system (3).

Remark 5 In [47–49], theoretical synchronization results of ordinary chaotic systems were studied. By contrast, the chaotic system with memristor studied in this paper is more complex. Besides considering the unified framework of FTS and FxTS of chaotic systems, a secure image encryption algorithm based upon the FTS/FxTS of the MCSs is designed in this paper as well to realize image encryption and decryption.

4 Numerical Simulation

In this section, the numerical simulations are given to show the effectiveness of the FTS/FxTS results. Choose the parameters of the system (3) as $a = 30, b = 1, c = 36, d = 0.5, h = 0.003$ and the initial states as $x(0)$=(0, 0.01, 0. As shown in Fig. 2, the timing diagrams of the state variables of the drive system (3) indicate that the trajectories of state variables are irregular. The attractor phase diagrams of the system (3) are shown in Fig. 3. It is not difficult to see from Fig. 3 that the three-dimensional phase diagrams of system (3) have double scroll chaotic attractors, which is a typical feature shared by a kind of Chua's chaotic system.

In the simulation experiment, choose the controller parameters $\gamma_i = 1$ $(i = 1, 2, 3, 4), \alpha = 2$. The initial conditions of systems (3) and (4) are $x(0)$=$(0, 0.01, 0.01, 0)^T$ and $y(0)$=$(2, 3.01, 4.01, 1)^T$. v_1 is assigned a fixed value of 0.2, while v_2 is assigned two different values of 0.8 and 3 respectively to correspond to the situations of FTS and FxTS. Then the simulation curves are obtained as shown in Figs. 4 and 5. The state variables of drive system (3) and response system (4) can be synchronized and the system error curves in two cases can approach zero in a finite/fixed time under the action of the controller.

Next, the initial value $y(0)$ of system (4) is changed to $(40, 60.01, 80.01, 20)^T$ while keeping other conditions unchanged, then we get Figs. 6 and 7. As shown in Table I, the theoretical upper bound of settling time required for synchronization of MCSs under the initial condition of $e(0) = (2, 3, 4, 1)^T$ or $e(0) = (40, 60, 80, 20)^T$ is given when v_2 is taken as 0.8 and 3 respectively. By comparing Fig. 4 with Fig. 6, the upper limit for the settling time varies with the initial value obviously. By comparing Fig. 5 with Fig. 7, it is inescapably clear that the settling time keeps the same even if the initial value changes. That is to say, the FTS of chaotic system is related to the initial values of the systems, while the FxTS of chaotic system is independent of the initial values of the systems.

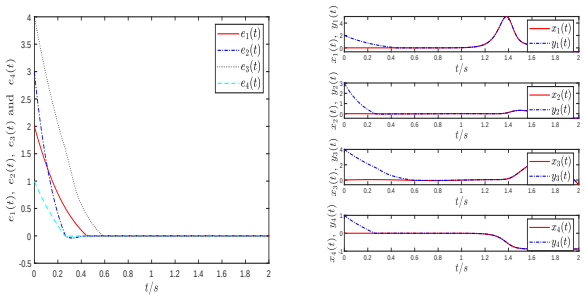


Fig. 4 The time evolutions of the state variables and errors when $v_2 = 0.8$ with $e(0)$=$(2, 3, 4, 1)^T$.

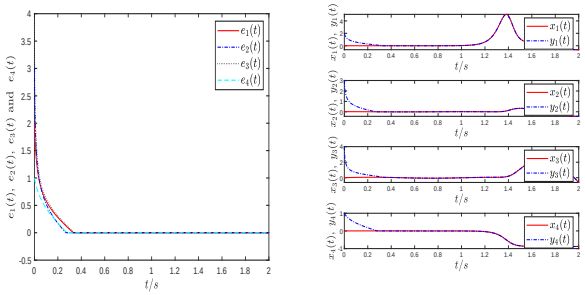


Fig. 5 The time evolutions of the state variables and errors when $v_2 = 3$ with $e(0)$=$(2, 3, 4, 1)^T$.

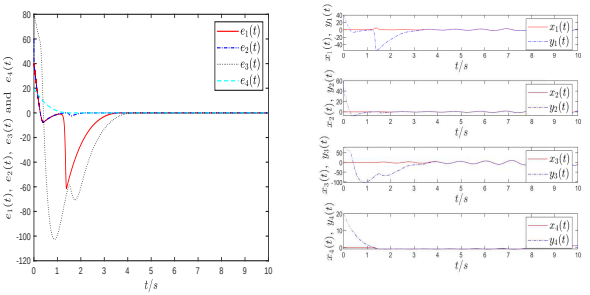


Fig. 6 The time evolutions of the state variables and errors when $v_2 = 0.8$ with $e(0)=(40, 60, 80, 20)^T$.

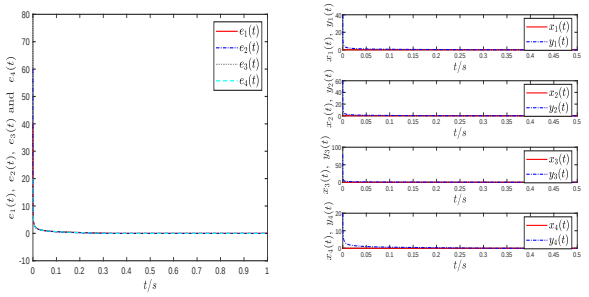


Fig. 7 The time evolutions of the state variables and errors when $v_2 = 3$ with $e(0)=(40, 60, 80, 20)^T$.

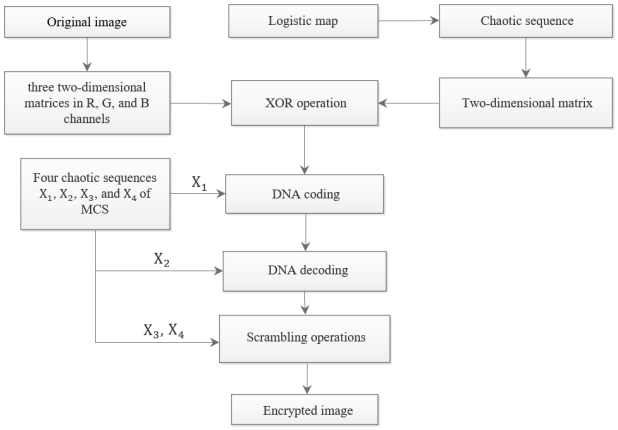


Fig. 8 The flow chart of encryption algorithm.

Table 1 The theoretical settling time of different v_2 under different initial values

Conditions	$e(0) = (2, 3, 4, 1)^T$	$e(0) = (40, 60, 80, 20)^T$
$v_1 = 0.2$, $v_2 = 0.8$	$T \leq 7.6112$	$T \leq 25.5810$
$v_1 = 0.2$, $v_2 = 3$	$T \leq 4.3565$	$T \leq 4.3565$

5 Design of Encryption Algorithm

With the development of chaos theory, the application of chaotic synchronization in communication security has become a hot topic for scholars. A large number of chaotic encryption algorithms have been proposed.

Table 2 DNA coding rules

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

From a genetic point of view, base pairs are chemical structures that form DNA encode genetic information. Base pairs consist of A-T and C-G. Strictly speaking, a base pair is a pair of matching bases connected. Similarly, when a decimal number is represented in binary, only two separate symbols 0 and 1 are required. Consequently, it is a nature idea that binary numbers converted from decimal numbers can be represented by bases in the DNA and there are eight coding methods shown in Table II that meet the requirements.

The following example illustrates the use of the above coding methods in the image encryption process. Suppose that for a color image, the gray value of a pixel point is decimal 100, and its binary form is 01100100, which is coded to be "GCGA" by DNA coding according to mode 1. However, "GCGA" is decoded to be 10011000 according to mode 2, which is converted to the decimal value 152. It can be seen that through the simple operation of DNA encoding and decoding in different modes, a value can be greatly changed, which is also the basic principle of the encryption algorithm based on DNA encoding. On this basis, the specific steps of the DNA encryption algorithm on the basis of the synchronization of MCSs are introduced. Fig. 8 shows the flow chart of the DNA encryption algorithm and the specific steps are as follows:

(1) The color digital image needing to be encrypted is divided into three image pixel value matrices with the size of $M \times N$ in R, G, and B components. The three matrices are described as I_1, I_2 and I_3, each element of which has a value range of 0-255.

(2) The size of each sub block is $p \times p$ which is much smaller than $M \times N$. Then, each image pixel value matrix is divided into $\frac{M \times N}{p^2}$ pieces.

(3) The Logistic map is expressed as

$$k_n = \theta k_{n-1} (1 - k_{n-1}) \tag{16}$$

where θ is the branch parameter. If θ keeps approaching to 4, an aperiodic and non convergent sequence can be obtained after iterating continuously with the mapping initial value $k_0 \in (0, 1)$. In this paper, θ is set to 3.9999 as one of the encryption keys. k_0, as one of the

encryption keys as well, satisfies

$$k_0 = \frac{\text{Sum}\,(I_1) + \text{Sum}\,(I_2)}{255 \times M \times N \times 2} \tag{17}$$

where $\text{Sum}\,(I_1)$, $\text{Sum}\,(I_2)$ are used to calculate the sum of all the elements of the matrices I_1, I_2 respectively.

(4) A chaotic sequence K_1 is decided by successive iteration of Logistic map according to (16) and its length is set as $M \times N$. The element values of the sequence K_1 are converted into the range of 0 to 255 by

$$\begin{cases} k_j{}' = \text{mod}\left(\text{round}\left(k_j \times 10^4\right), 256\right) \\ Q = \text{reshape}(K_1{}', M, N) \end{cases} \tag{18}$$

where k_j $(j = 0, \ldots, M \times N - 1)$ are elements of K_1, $k_j{}'$ are elements of $K_1{}'$ converted from K_1, Q is a two-dimensional matrix transformed from the sequence $K_1{}'$ with the size of $M \times N$.

(5) In consideration of the encryption efficiency, the XOR operation is applied in the corresponding blocks of I_1, I_2, I_3 with that of Q, which gets I_1', I_2', I_3'.

(6) The four-order Runge-Kurta method is adopted to calculate system (3), and four chaotic sequences with length of $\frac{M \times N}{p^2}$ are acquired and expressed as X_1, X_2, X_3, X_4 respectively. The initial values of these four sequences $X_1(0), X_2(0), X_3(0), X_4(0)$ are also part of the encryption algorithm keys.

(7) The same DNA coding method is chosen for the sub blocks at the same location of I_1', I_2' and I_3', which is determined by X_1. Because there are eight ways of DNA code, it needs to convert the element values of the sequence X_1 into an integer ranging from 1 to 8 determined by

$$\omega_m{}' = \text{mod}\left(\text{round}\left(\omega_m \times 10^4\right), 8\right) + 1 \tag{19}$$

where ω_m $(m = 0, \ldots, \frac{M \times N}{p^2} - 1)$ are elements of the chaotic sequence X_1.

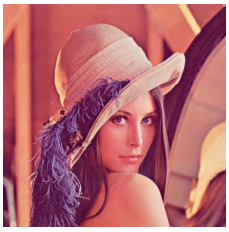
(8) Sequence X_2 determines the rules of DNA decoding after DNA coding and the element values are similarly converted into an integer ranging from 1 to 8 according to (19). DNA decoding is the reverse process of DNA coding.

(9) Scramble the positions of sub blocks twice. The element values of the sequences X_3 and X_4 are arranged in order from largest to smallest by

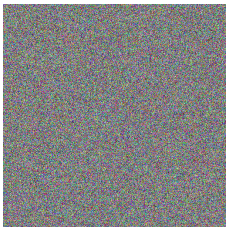
$$\begin{cases} [\sim, P_1] = \text{sort}(X_3,\ \text{descend's}) \\ [\sim, P_2] = \text{sort}(X_4,\ \text{descend's}) \end{cases} \tag{20}$$

where P_1 and P_2 are two position sequences gained before the ordering of each element in the sequences X_3 and X_4. The the element values of P_1 and P_2 are taken as the coordinates of sub blocks to exchange positions, so as to get better scrambling effects.

(10) By merging the two-dimensional matrices after two substitutions into a three-dimensional matrix, the encrypted image is obtained.

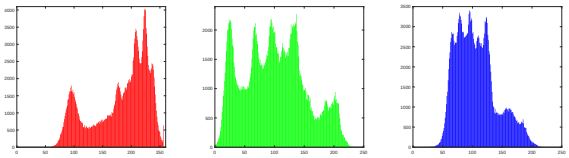


(a)



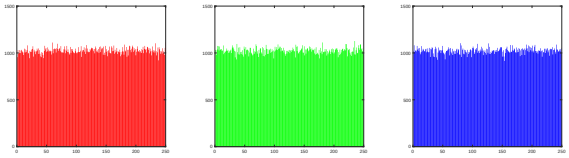
(b)

Fig. 9 Original image and encrypted image. (a) Original image. (b) Encrypted image.



(a) (b) (c)

Fig. 10 Histograms of original image. (a) Red channel. (b) Green channel. (c) Blue channel.



(a) (b) (c)

Fig. 11 Histograms of encrypted image. (a) Red channel. (b) Green channel. (c) Blue channel.

6 Experiment and Analysis of DNA Encryption Algorithm

Taking Lena's color image as an example, the encrypted image is obtained by using the designed encryption algorithm. By comparing the original image with the encrypted image shown in Fig. 9, the encrypted image dose not resemble the original image obviously. Next, the two images will be analyzed from statistical perspectives.

Table 3 Comparison of correlation coefficients of adjacent pixels in Lena's image.

Image	Horizontal	Vertical	Diagonal
Original Image	0.97688	0.98350	0.95348
Encrypted Image of this paper	-0.00887	0.00479	0.00532
Encrypted Image of Ref. [51]	-0.0445	-0.0168	0.0022
Encrypted Image of Ref. [52]	-0.02457	-0.02264	-0.01930

Table 4 Comparison of the information entropy of Lena's image.

Image	R	G	B
Original Image	7.2682	7.5901	6.9951
Encrypted Image of this paper	7.9993	7.9993	7.9993
Encrypted Image of Ref. [50]	7.9973	7.9975	7.9977
Encrypted Image of Ref. [51]	7.9278	7.9744	7.9705
Encrypted Image of Ref. [53]	7.9974	7.9971	7.9972

6.1 Histogram Analysis

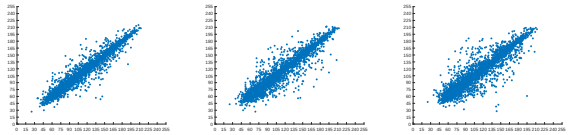
In this part, the histograms of the original image are compared with that of the encrypted image. Each image has specific histograms, which can reflect the scrambling of image encryption algorithm. Histogram can directly reflect the statistical changes of the image before and after the operation of encryption. In order to prevent attackers from cracking the image information by analyzing the gray value distribution, the encrypted image histogram is required to be smooth and uniform. Fig. 10 shows the histograms of the Fig. 9 (a) in R, G, and B channels. It can be seen that the histogram shapes are steep and fluctuating. Fig. 11 shows the histograms of the encrypted image in R, G, and B three channels. It can be seen that the histogram shapes are uniform distributions. This indicates that if an attacker makes a statistical attack, he will not be able to obtain accurate information about the Fig. 9 (a) from the Fig. 9 (b).

6.2 Correlation Analysis of Pixel Values in Adjacent Locations

In this part, it has tested the correlation of 5000 pairs of adjacent pixels of the Fig. 9 (a) and the Fig. 9 (b) in the horizontal direction, vertical direction and diagonal direction respectively to analyze the encryption effect. The calculating method of correlation coefficient is expressed as

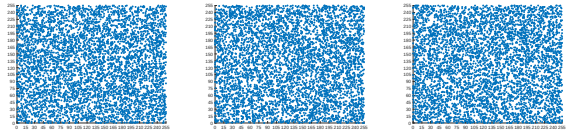
$$\varphi_{\delta\sigma} = \frac{E((\delta - E(\delta))(\sigma - E(\sigma)))}{\sqrt{D(\delta)D(\sigma)}} \tag{21}$$

where δ and σ are the values of two adjacent pixels in the image. The mean value $E(\delta)$ and variance $D(\delta)$ are



(a) (b) (c)

Fig. 12 Correlation distributions in B channel of original image. (a) Horizontal direction. (b) Vertical direction. (c) Diagonal direction.



(a) (b) (c)

Fig. 13 Correlation distributions in channel B of encrypted image. (a) Horizontal direction. (b) Vertical direction. (c) Diagonal direction.

defined as follows:

$$E(\delta) = \frac{1}{n}\sum_{i=1}^{n}\delta_i,$$
$$D(\delta) = \frac{1}{n}\sum_{i=1}^{n}(\delta_i - E(\delta))^2. \tag{22}$$

The smaller the correlation between the gray values of adjacent areas, the stronger the ability of the image to resist attacks is. Fig. 12 shows the value distribution of 5000 pairs of adjacent pixels in Fig. 9 (a) of channel B. It is apparent that the value distribution of these pixels is similar to a positive scale function curve, which shows direct correlation of adjacent pixels in Fig. 9 (a). Fig. 13 shows the value distribution of 5000 pairs of adjacent pixels of Fig. 9 (b) in the horizontal, vertical, and diagonal direction of channel B. It is inescapably clear that these pixels are completely randomly distributed, and the correlation coefficient between adjacent position data values is almost zero. The validity of the encryption algorithm is verified.

Table III shows the correlation coefficients between the adjacent positions of the original image and the encrypted image of Lena by different algorithms.

It is clear that the correlation coefficients of horizontal, vertical and diagonal directions of the three channels of Fig. 9 (a) are all close to 1, which shows that the gray values of adjacent positions are highly correlated. The correlation coefficients of the encrypted images are all almost 0, which indicates that the adjacent position gray values of R, G , and B channels of Fig. 9 (b) in horizontal, vertical and diagonal directions are basically

not connected. Moreover, compared with the encrypted images in Refs. [51, 52], the correlation of adjacent pixels of the encrypted image of this paper is lower, which reflects that the proposed encryption algorithm is relatively better.

6.3 Key Space Analysis

To prevent attacks, an effective encryption algorithm should have a large enough key space at least 2^{100} in general assumption. The key space of an algorithm can be calculated according to the sensitivity of each key. The keys of the encryption algorithm in this paper includes the initial values of the four chaotic sequences derived from the system (3) and the Logistic map's parameter θ and its initial value k_0 , and the key space they constitute is $10^{16}\times10^{16}\times10^{16}\times10^{16}\times10^{15}\times10^{16} = 10^{95} \approx 2^{315}$. There is no doubt that this has a very large key capacity that can easily resist the exhaustive key method to crack the image.

6.4 Information Entropy Analysis

In information theory, entropy is the average amount of information contained in each message received. The more random the information source is, the greater the entropy is. Information entropy represents the overall characteristics of information sources in an evaluative sense. In the meanwhile, it can reflect the degree of confusion of information of a picture and its specific mathematical definition is

$$H(w) = \sum_{i=0}^{W-1} p\left(w_i\right) \log \frac{1}{p\left(w_i\right)} \tag{23}$$

where $p\left(w_i\right)$ is the proportion of the image grey value and W represents the gray scale of the image, $H(w)$ is the maximum information entropy. For example, when $W = 256 = 2^8, H = \log_2 256 = 8$. In particular, the actual information entropy measured will be little smaller than the ideal value. Therefore, the information entropy of the encrypted image of an effective encryption algorithm should be very close to 8. Table IV is the numerical comparisons about information entropy of the encrypted image of Lena in different algorithms. Obviously, the experimental data obtained by the proposed encryption algorithm are closer to the ideal value 8.

Remark 6 In [50], an encryption algorithm based on DNA coding was adopted and showed good performance. Through the comparison of experimental data, the key space of the proposed encryption algorithm is much larger than 2^{256} of [50]. In addition, the information entropy of the proposed algorithm of the encrypted image is 7.9993 and is closer to 8 than that of [50, 51, 53], which indicates that the encryption effect is more marvelous.

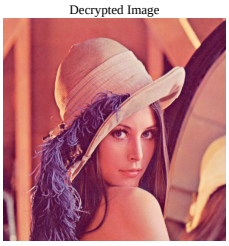


Fig. 14 Decrypted image.

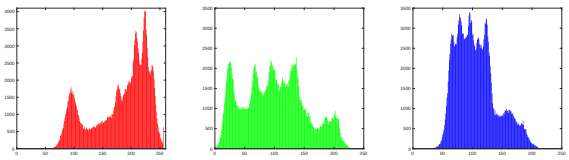


Fig. 15 Histograms of decrypted image. (a) Red channel. (b) Green channel. (c) Blue channel.

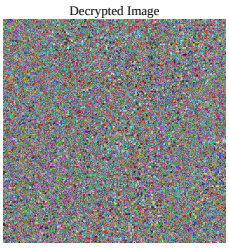


Fig. 16 Decrypted image with keys slightly changed.

6.5 Analysis of Decrypted Image

The decryption process is completely opposite to the encryption process on the encrypted image. This paper will not repeat it. In the process of decryption, only if all the keys are accurate can the decrypted image be correctly gained. At the same time, the decrypted image ought to be like a replica of the original image. As shown in Fig. 14, the decrypted image is identical to Fig. 9 (a) from the visual point of view. In addition, Fig. 15 shows the histograms of Fig. 14 in three channels, which is identical with Fig. 10. It reflects that the encryption and decryption results are excellent.

6.6 Key Sensitivity Analysis

A secure image encryption algorithm is supposed to be sensitive to the keys in the processes of encryption and decryption. It means that small changes in the keys can lead to severe distortions of the encrypted and decrypted images. Key sensitivity guarantees the uniqueness of the keys. The encryption algorithm contains multiple keys, each of which contributes different values during the encryption process. Only when all the keys are correct can the clear original image be decrypted accurately. No matter which key is changed slightly during decryption, the correct original image cannot be obtained.

The sensitivity of the algorithm to the keys by slightly changing the value of one of the keys during decryption is tested. For example, after changing the value 0.7803 of $X_4(0)$ into 0.7803000000000001 when used to the decryption, a new decrypted image not containing any relevant information on original image is shown in Fig. 16. The range of key changes only as small as 10^{-16}, but the original image is still not visible from the decrypted image. The experimental results show that only accurate keys can get the accurate decrypted image. It indicates that the key sensitivity of this algorithm is extremely strong.

7 Conclusion

This paper has presented a unified framework for using SMC to design FTS/FxTS of MCSs. Unlike separate discussions of FTS and FxTS of MCSs, a unified framework is designed in this paper to achieve FTS and FxTS of MCSs at the same time by selecting different control parameters in a simple controller. In addition, an efficient image encryption algorithm on the bases of the FTS/FxTS of MCSs has been designed. Simulation results and performance analyses have demonstrated that our proposed image encryption algorithm has good encryption and decryption effects with high security, large key space and superb key sensitivity. In practical applications, synchronization studies are generally not limited to the synchronization of one drive system and one response system. Consequently, studying the synchronization of multiple MCSs will be a part of our next research plan. Moreover, the ability of encryption algorithm to resist attack is also an important indicator to measure whether the algorithm is reliable enough, which is not taken into account in this paper. Therefore, we intend to design new encryption algorithms with faster encryption speed and stronger reliability and use more convincing indicators to judge the encryption algorithms.

Acknowledgements This work was supported by the National Natural Science Foundation of China under Grants 62076229, 62073301 and 61876192.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Appendix I

Proof of Theorem 1

Choose the quadratic function

$$V(t) = \frac{1}{2}\sum_{i=1}^{4} S_i(t)^2. \tag{24}$$

And the derivation of (24) is

$$\begin{aligned}\dot{V}(t) &= \sum_{i=1}^{4} S_i(t)\dot{S}_i(t) \\ &= \sum_{i=1}^{4} S_i(t)[\gamma_i \dot{e}_i(t) + (|e_i(t)|^{v_1} + |e_i(t)|^{v_2})\text{sign}(e_i(t))].\end{aligned} \tag{25}$$

By substituting (13) into (5) and then into (25), we can get

$$\begin{aligned}\dot{V}(t) &\le -\check{\gamma}\sum_{i=1}^{4}\left(\alpha\left|S_i(t)\right| + \left|S_i(t)\right|^{v_2+1}\right) \\ &\le 0\end{aligned} \tag{26}$$

where $\check{\gamma} = \min\{\gamma_i\}, i = 1, 2, 3, 4$.

The following part will discuss the different three cases of v_2.

(Case $1, 0 \le v_2 < 1$*):* According to lemma 1 and (26),

$$\dot{V}(t) \le -\alpha\check{\gamma}\left(2V(t)\right)^{\frac{1}{2}} - \check{\gamma}\left(2V(t)\right)^{\frac{v_2+1}{2}}. \tag{27}$$

Then integrate two sides of (27), we get

$$T_1 \le \min\left\{\frac{\|S(0)\|}{\alpha\check{\gamma}}, \frac{\|S(0)\|^{1-v_2}}{\check{\gamma}(1-v_2)}\right\}. \tag{28}$$

(Case $2, v_2 = 1$*)* : (27) can be written as

$$\dot{V}(t) \le -\alpha\check{\gamma}\left(2V(t)\right)^{\frac{1}{2}} - \check{\gamma}\left(2V(t)\right). \tag{29}$$

By integrating the two sides of (29), we can get

$$T_1 \le \frac{1}{\check{\gamma}}\ln\left(1 + \frac{1}{\alpha}\|S(0)\|\right). \tag{30}$$

(Case $3, v_2 > 1$*):* According to (26), if $V(t) \le 1$, then

$$\dot{V}(t) \le -\alpha\check{\gamma}\left(2V(t)\right)^{\frac{1}{2}}. \tag{31}$$

If $V(t) > 1$, according to lemma 1,

$$\dot{V}(t) \leq -\check{\gamma}\left(2V(t)\right)^{\frac{v_2+1}{2}} \leq -\check{\gamma}2^{1-v_2}(2V(t))^{\frac{v_2+1}{2}}. \quad (32)$$

It implies that

$$T_1 \leq \frac{\sqrt{2}}{\alpha\check{\gamma}} + \frac{2^{\frac{v_2-1}{2}}}{\check{\gamma}\left(v_2-1\right)}. \quad (33)$$

The proof is completed. ■

Appendix II

Proof of Theorem 2

Choose the quadratic function

$$V(t) = \frac{1}{2}\sum_{i=1}^{4} e_i(t)^2. \quad (34)$$

And the derivation of (34) is

$$\begin{aligned}\dot{V}(t) &= \sum_{i=1}^{4} e_i(t)\dot{e}_i(t) \\ &\leq -\frac{1}{\hat{\gamma}}\sum_{i=1}^{4}\left(|e_i(t)|^{v_1+1} + |e_i(t)|^{v_2+1}\right) \end{aligned} \quad (35)$$

where $\hat{\gamma} = \max\left\{\gamma_i\right\}, i = 1,2,3,4$.

The following will also discuss the three different cases of v_2.

(*Case* $1, 0 \leq v_2 < 1$)*:* According to lemma 1,

$$\dot{V}(t) \leq -\frac{1}{\hat{\gamma}}\left[\left(2V(t)\right)^{\frac{v_1+1}{2}} + \left(2V(t)\right)^{\frac{v_2+1}{2}}\right]. \quad (36)$$

Integrate two sides of (36), we get

$$T_2 \leq \min\left\{\frac{\hat{\gamma}\|e(0)\|^{1-v_1}}{1-v_1}, \frac{\hat{\gamma}\left\|e(0)\right\|^{1-v_2}}{1-v_2}\right\}. \quad (37)$$

(*Case* $2, v_2 = 1$)*:* (36) can be written as

$$\dot{V}(t) \leq -\frac{1}{\hat{\gamma}}[\left(2V(t)\right)^{\frac{v_1+1}{2}} + \left(2V(t)\right)]. \quad (38)$$

By integrating the two sides of (38), we can get

$$T_2 \leq \frac{\hat{\gamma}}{1-v_1}\ln\left(1 + \|e(0)\|^{1-v_1}\right). \quad (39)$$

(*Case* $3, v_2 > 1$)*:* According to lemma 1 and (35), it is easy to get that

$$\left(\sum_{i=1}^{4}|e_i(t)|^2\right)^{\frac{v_1+1}{2}} \leq \sum_{i=1}^{4}|e_i(t)|^{v_1+1}. \quad (40)$$

$$2^{1-v_2}\left(\sum_{i=1}^{4}|e_i(t)|^2\right)^{\frac{v_2+1}{2}} \leq \sum_{i=1}^{4}|e_i(t)|^{v_2+1}. \quad (41)$$

As is putted above, we can obtain

$$\begin{aligned}\dot{V}(t) \leq -\frac{1}{\hat{\gamma}}\Bigg[&\left(\sum_{i=1}^{4}|e_i(t)|^2\right)^{\frac{v_1+1}{2}} \\ &+2^{1-v_2}\left(\sum_{i=1}^{4}|e_i(t)|^2\right)^{\frac{v_2+1}{2}}\Bigg] \\ = -\frac{1}{\hat{\gamma}}&\left[\left(2V(t)\right)^{\frac{v_1+1}{2}} + 2^{1-v_2}(2V(t))^{\frac{v_2+1}{2}}\right]. \end{aligned} \quad (42)$$

If $V(t) \leq 1$,

$$\dot{V}(t) \leq -\frac{1}{\hat{\gamma}}(2V(t))^{\frac{v_1+1}{2}}. \quad (43)$$

If $V(t) > 1$,

$$\dot{V}(t) \leq -\frac{1}{\hat{\gamma}}2^{1-v_2}(2V(t))^{\frac{v_2+1}{2}}, \quad (44)$$

Therefore

$$T_2 < \frac{\hat{\gamma}2^{\frac{1-v_1}{2}}}{1-v_1} + \frac{\hat{\gamma}2^{\frac{v_2-1}{2}}}{v_2-1}. \quad (45)$$

The proof is completed. ■

References

1. L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821-824, Jun. 1990.
2. Z. Zhang, K. T. Chau, and Z. Wang, "Chaotic speed synchronization control of multiple induction motors using stator flux regulation," *IEEE Trans. Magn.*, vol. 48, no. 11, pp. 4487-4490, Nov. 2012.
3. H. Zhang, Y. Xie, Z. Wang, and C. Zheng, "Adaptive synchronization between two different chaotic neural networks with time delay," *IEEE Trans. Neural Netw.*, vol. 18, no. 6, pp. 1841-1845, Dec. 2007.
4. G. Li and B. Zhang, "A novel weak signal detection method via chaotic synchronization using Chua's circuit," *IEEE Trans. Ind. Electron.*, vol. 64, no. 3, pp. 2255-2265, Mar. 2017.
5. T. L. Carroll and L. M. Pecora, "Synchronizing chaotic circuits," *IEEE Trans. Circuits Syst.*, vol. 38, no. 4, pp. 453-456, Apr. 1991.
6. K. Tanaka, T. Ikeda, and H. Wang, "A unified approach to controlling chaos via an LMI-based fuzzy control system design," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 45, no. 10, pp. 1021-1040, Oct. 1998.
7. Z. Wu, P. Shi, H. Su, and J. Chu, "Sampled-data fuzzy control of chaotic systems based on a T-S fuzzy model," *IEEE Trans. Cybern.*, vol. 45, no. 4, pp. 819-829, Apr. 2014.

8. Z. Wang and H. Wu, "On fuzzy sampled-data control of chaotic systems via a time-dependent Lyapunov functional approach," *IEEE Trans. Fuzzy Syst.*, vol. 22, no. 1, pp. 153-163, Feb. 2015.
9. S. Djennoune, M. Bettayeb, and U. M. Al-Saggaf, "Impulsive observer with predetermined finite convergence time for synchronization of fractional-order chaotic systems based on Takagi-Sugeno fuzzy model," *Nonlinear Dyn.*, vol. 98, pp. 1331-1354, Sep. 2019.
10. C. Hu, H. Jiang, and Z. Teng, "Impulsive control and synchronization for delayed neural networks with reaction-diffusion terms," *IEEE Trans. Neural Netw.*, vol. 21, no. 1, pp. 67-81, Jan. 2010.
11. X. Yang and J. Lu, "Finite-time synchronization of coupled networks with Markovian topology and impulsive effects," *IEEE Trans. Autom. Control*, vol. 61, no. 8, pp. 2256-2261, Aug. 2016.
12. A. Khadra, X. Liu, and X. Shen, "Analyzing the robustness of impulsive synchronization coupled by linear delayed impulses," *IEEE Trans. Autom. Control*, vol. 54, no. 4, pp. 923-928, Apr. 2009.
13. H. Zhang, Y. Xie, Z. Wang, and C. Zheng, "Adaptive synchronization between two different chaotic neural networks with time delay," *IEEE Trans. Neural Netw.*, vol. 18, no. 6, pp. 1841-1845, Nov. 2007.
14. X. Wang and Y. Wang, "Adaptive control for synchronization of a four-dimensional chaotic system via a single variable," *Nonlinear Dyn.*, vol. 65, no. 3, pp. 311-316, Aug. 2011.
15. L. Shanmugam, P. Mani, P. Rajan, and Y. H. Joo, "Adaptive synchronization of reaction-diffusion neural networks and its application to secure communication," *IEEE Trans. Cybern.*, vol. 50, no. 3, pp. 911-922, Mar. 2020.
16. H. Bai and J. T. Wen "Asymptotic synchronization of phase oscillators with a single input," *IEEE Trans. Autom. Control*, vol. 64, no. 4, pp. 1611-1618, Apr. 2019.
17. Z. Li and G. Chen, "Global synchronization and asymptotic stability of complex dynamical networks," *IEEE Trans. Circuits Syst. II Exp. Briefs*, vol. 53, no. 1, pp. 28-33, Jan. 2006.
18. C. Zhang, Y. He, and M. Wu, "Improved global asymptotical synchronization of chaotic Lur'e systems with sampled-data control," *IEEE Trans. Circuits Syst. II Exp. Briefs*, vol. 56, no. 4, pp. 320-324, Apr. 2009.
19. X. Wang, X. Zhang, and C. Ma, "Modified projective synchronization of fractional-order chaotic systems via active sliding mode control," *Nonlinear Dyn.*, vol. 69, no. 1-2, pp. 511-517, Jul. 2012.
20. Z. Wu, P. Shi, H. Su, and J. Chu, "Local synchronization of chaotic neural networks with sampled-data and saturating actuators," *IEEE Trans. Cybern.*, vol. 44, no. 12, pp. 2635-2645, Dec. 2014.
21. J. Sun, Y. Wu, G. Cui, and Y. Wang, "Finite-time real combination synchronization of three complex-variable chaotic systems with unknown parameters via sliding mode control," *Nonlinear Dyn.*, vol. 88, no. 3, pp. 1677-1690, Feb. 2017.
22. T. Lin and T. Lee, "Chaos synchronization of uncertain fractional-order chaotic systems with time delay based on adaptive fuzzy sliding mode control," *IEEE Trans. Fuzzy Syst.*, vol. 19, no. 4, pp. 623-635, Aug. 2011.
23. A. Polyakov, "Nonlinear feedback design for fixed-time stabilization of linear control systems," *IEEE Trans. Autom. Control*, vol. 57, no. 8, pp. 2106-2110, Aug. 2012.
24. J. Ni, L. Liu, C. Liu, X. Hu, and T. Shen, "Fixed-time dynamic surface high-order sliding mode control for chaotic oscillation in power system," *Nonlinear Dyn.*, vol. 86, pp. 401-420, Oct. 2016.
25. A. Khanzadeh and M. Pourgholi, "Fixed-time sliding mode controller design for synchronization of complex dynamical networks," *Nonlinear Dyn.*, vol. 88, pp. 2637-2649, Jun. 2017.
26. J. Ni, L. Liu, C. Liu, X. Hu, and S. Li, "Fast fixed-time nonsingular terminal sliding mode control and its application to chaos suppression in power system," *IEEE Trans. Circuits Syst. II, Express Briefs*, vol. 64, no. 2, pp. 151-155, Feb. 2017.
27. L. Wang, Z. Zeng, and M. Ge, "A disturbance rejection framework for finite-time and fixed-time stabilization of delayed memristive neural networks," *IEEE Trans. Syst., Man, Cybern.*, vol. 51, no. 2, pp. 905-915, Feb. 2021.
28. W. Perruquetti and J. P. Barbot, *Sliding Mode Control in Engineering*. New York: Marcel Dekker, 2002.
29. H. Wang, Z. Han, Q. Xie, and W. Zhang, "Finite-time chaos control of unified chaotic systems with uncertain parameters," *Nonlinear Dyn.*, vol. 55, no. 4, pp. 323-328, Mar. 2009.
30. L. Yin, Z. Deng, B. Huo, and Y. Xia, "Finite-time synchronization for chaotic gyros systems with terminal sliding mode control," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 49, no. 6, pp. 1131-1140, Jun. 2019.
31. W. He, T. Luo, Y. Tang, W. Du, Y. Tian, and F. Qian, "Secure communication based on quantized synchronization of chaotic neural networks under an event-triggered strategy," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 3, no. 4, pp. 425-436, Sep. 2015.
32. M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Process.*, vol. 171, p. 107484, Jun. 2020.
33. L. O. Chua, "Memristor-the missing circuit element," *IEEE Trans. Circuit Theory*, vol. 18, no. 5, pp. 507-519, Sep. 1971.
34. D. B. Strukov, G. S. Snider, G. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, no. 7191, pp. 80-83, May 2008.
35. L. V. Gambuzza, A. Buscarino, L. Fortuna, and M. Frasca, "Memristor-based adaptive coupling for consensus and synchronization," *IEEE Trans. Circuits Syst. I Reg. Papers*, vol. 62, no. 4, pp. 1175-1184, Apr. 2015.
36. M. Di Marco, M. Forti, and L. Pancioni, "New conditions for global asymptotic stability of memristor neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 5, pp. 1822-1834, May 2018.
37. J. Luo, S. Qu, Y. Chen, and Z. Xiong, "Synchronization of memristor-based chaotic systems by a simplified control and its application to image en-/decryption using DNA encoding," *Chin. J. Phys.*, vol. 62, pp. 374-387, Dec. 2019.
38. G. Peng and F. Min, "Multistability analysis, circuit implementations and application in image encryption of a novel memristive chaotic circuit," *Nonlinear Dyn.*, vol. 90, pp. 1607-1625, Aug. 2017.
39. S. Duan, X. Hu, Z. Dong, L. Wang, and P. Mazumder, "Memristor-based cellular nonlinear/neural network: design, analysis, and applications," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 6, pp. 1202-1213, Jun. 2015.
40. L. Wang, H. He, and Z. Zeng, "Global synchronization of fuzzy memristive neural networks with discrete and distributed delays," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 9, pp. 2022-2034, Sep. 2020.
41. L. Wang, T. Dong, and M. Ge, "Finite-time synchronization of memristor chaotic systems and its application in image encryption," *Appl. Math. Comput.*, vol. 347, pp. 293-305, Apr. 2019.
42. M. E. Sahin, Z. G. C. Taskiran, and H. Guler, "Application and modeling of a novel 4D memristive chaotic system for communication systems," *Circuits, Syst., Signal Process.*, vol. 39, pp. 3320-3349, Jan. 2020.
43. M. Yuan, W. Wang, Z. Wang, X. Luo, and J. Kurths, "Exponential synchronization of delayed memristor-based uncertain complex-valued neural networks for image protection," *IEEE*

Trans. Neural Netw. Learn. Syst., vol. 32, no. 1, pp. 151-165, Jan. 2021.
44. M. Itoh and L. O. Chua, "Memristor oscillators," *Int. J. Bifurcat. Chaos*, vol. 18, no. 11, pp. 3183-3206, Nov. 2008.
45. G. Hardy, J. Littlewood, and G. Polya, *Inequalities*. Cambridge, U.K: Cambridge Univ. Press, 1988.
46. X. Yang, J. Lam, W. C. Ho, and Z. Feng, "Fixed-time synchronization of complex networks with impulsive effects via nonchattering control," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 5511-5521, Nov. 2017.
47. J. Xiao, Z. Zeng, S. Wen, A. Wu, and L. Wang, "A unified framework design for finite-time and fixed-time synchronization of discontinuous neural networks," *IEEE Trans. Cybern.*, 2019, doi: 10.1109/TCYB.2019.2957398.
48. J. Xiao, Z. Zeng, S. Wen, A. Wu, and L. Wang, "Finite-/fixed-time synchronization of delayed coupled discontinuous neural networks with unified control schemes," *IEEE Trans. Neural Netw. Learn. Syst.*, 2020, doi: 10.1109/TNNLS.2020.3006516.
49. X. Liu, D. W. C. Ho, Q. Song, and J. Cao, "Finite-/fixed-time robust stabilization of switched discontinuous systems with disturbances," *Nonlinear Dyn.*, vol. 90, no. 3, pp. 2057-2068, Sep. 2017.
50. N. Benyamin and M. Sattar, "An image encryption algorithm based on DNA sequence operations and cellular neural network," *Multimed Tools Appl.*, vol. 76, pp. 13681-13701, Jun. 2017.
51. A. Kadir, A. Hamdulla, and W. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik*, vol. 125, no. 5, pp. 671-675, Mar. 2014.
52. Y. Zhang and Y. Tang, "A plaintext-related image encryption algorithm based on chaos," *Multimed Tools Appl.*, vol. 77, pp. 6647-6669, Mar. 2018.
53. G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, pp. 45-53, Aug. 2017.

Figures

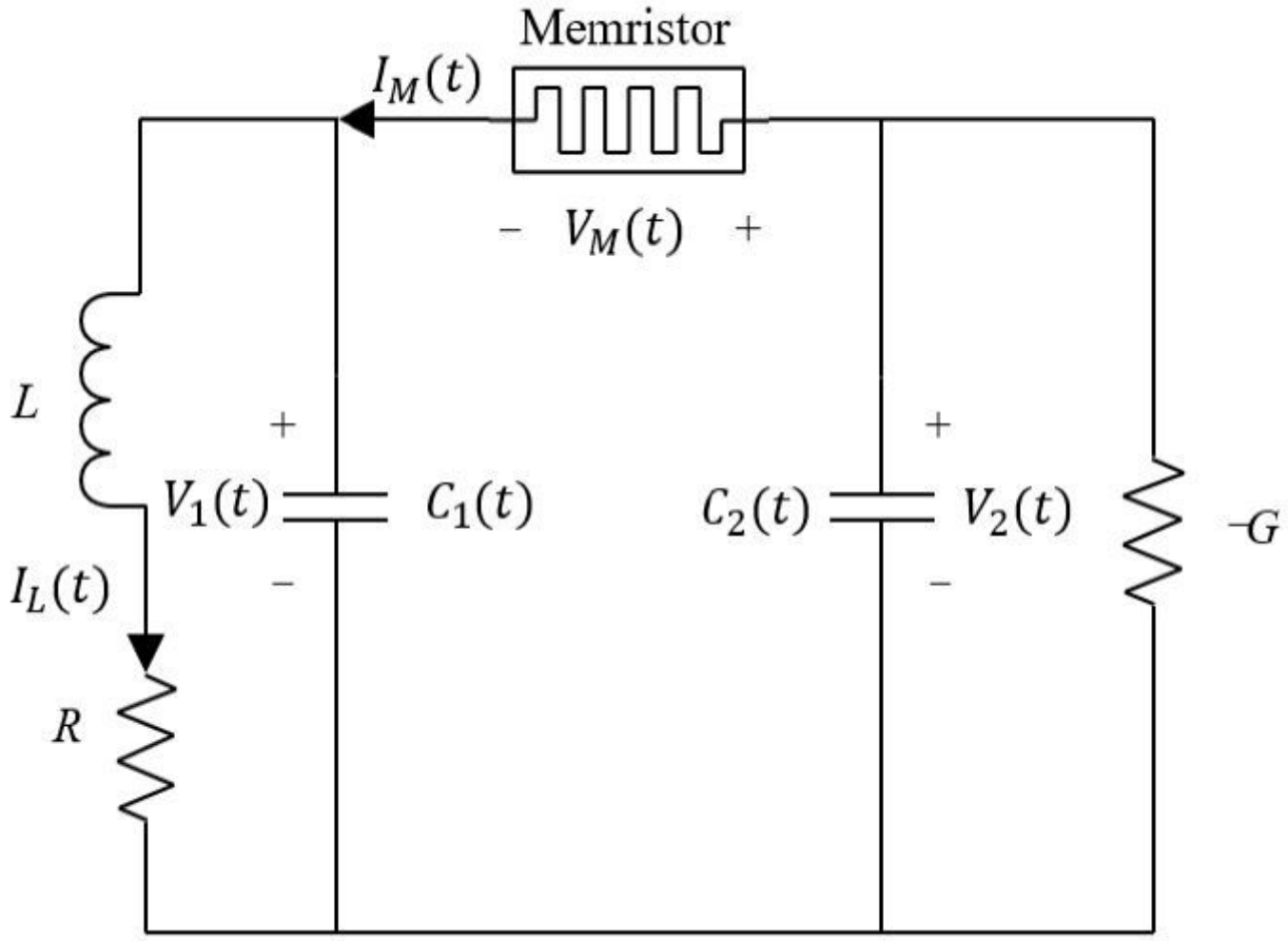


Figure 1

The memristor chaotic circuit.

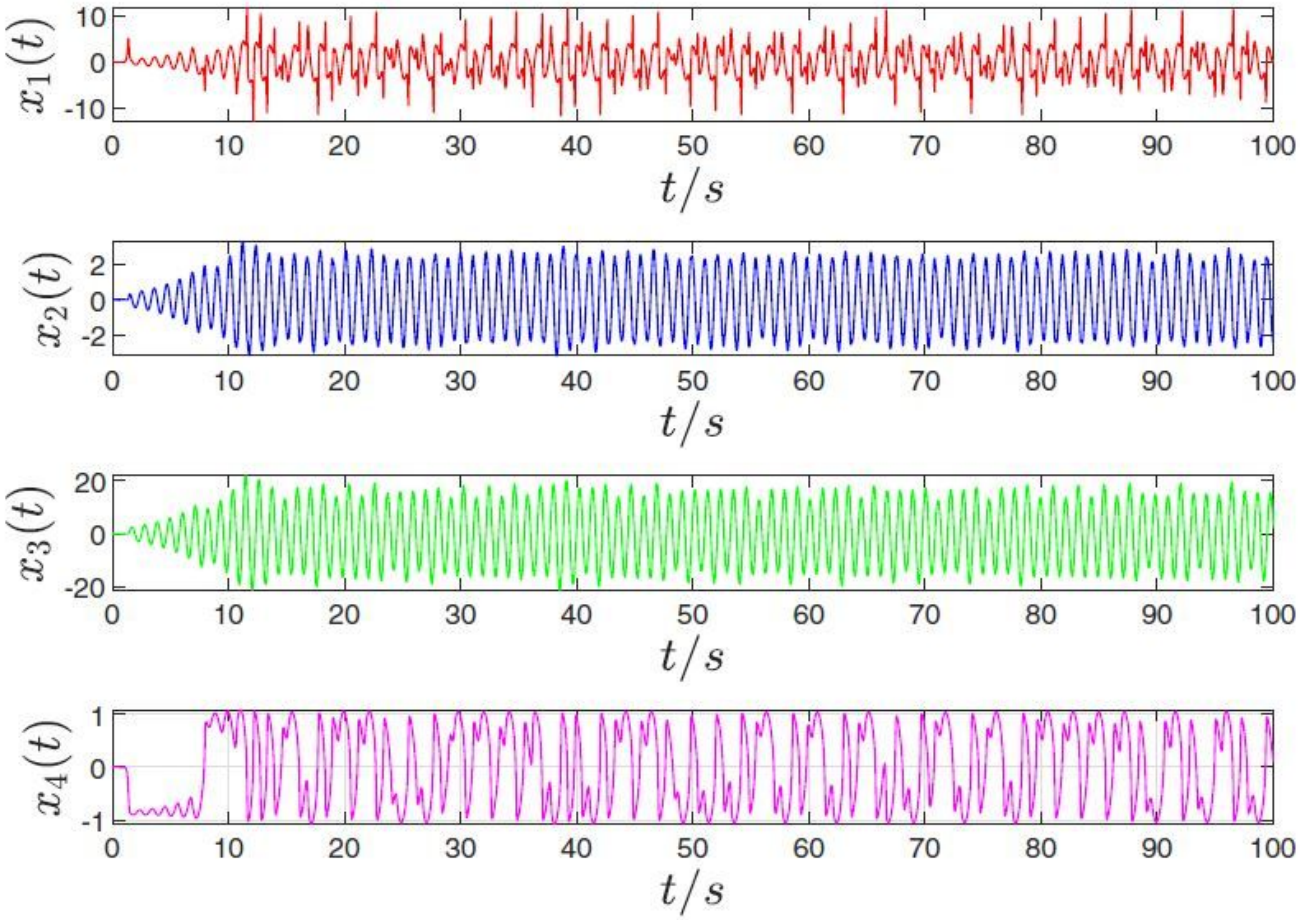


Figure 2

The trajectories of the state variables in system (3).

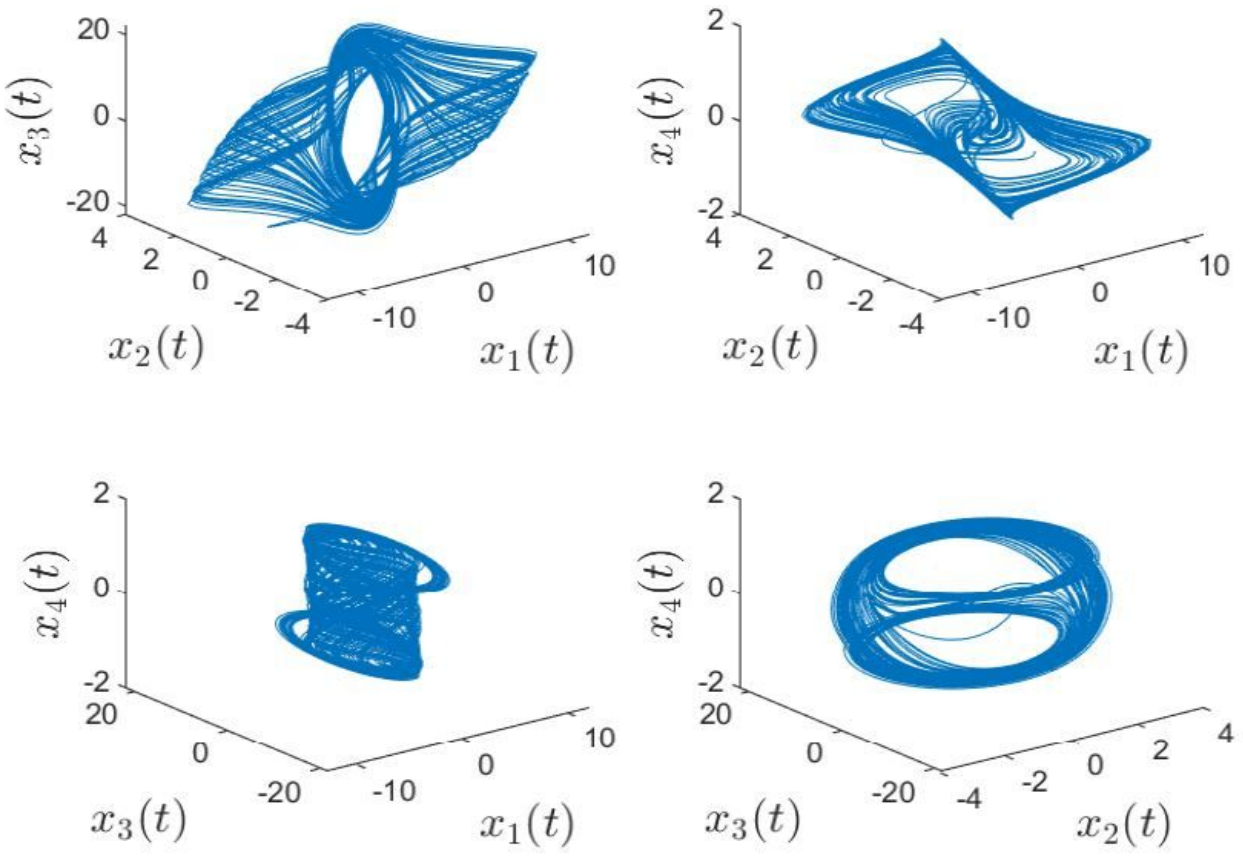


Figure 3

The attractor phase diagrams of the memristor chaotic system (3).

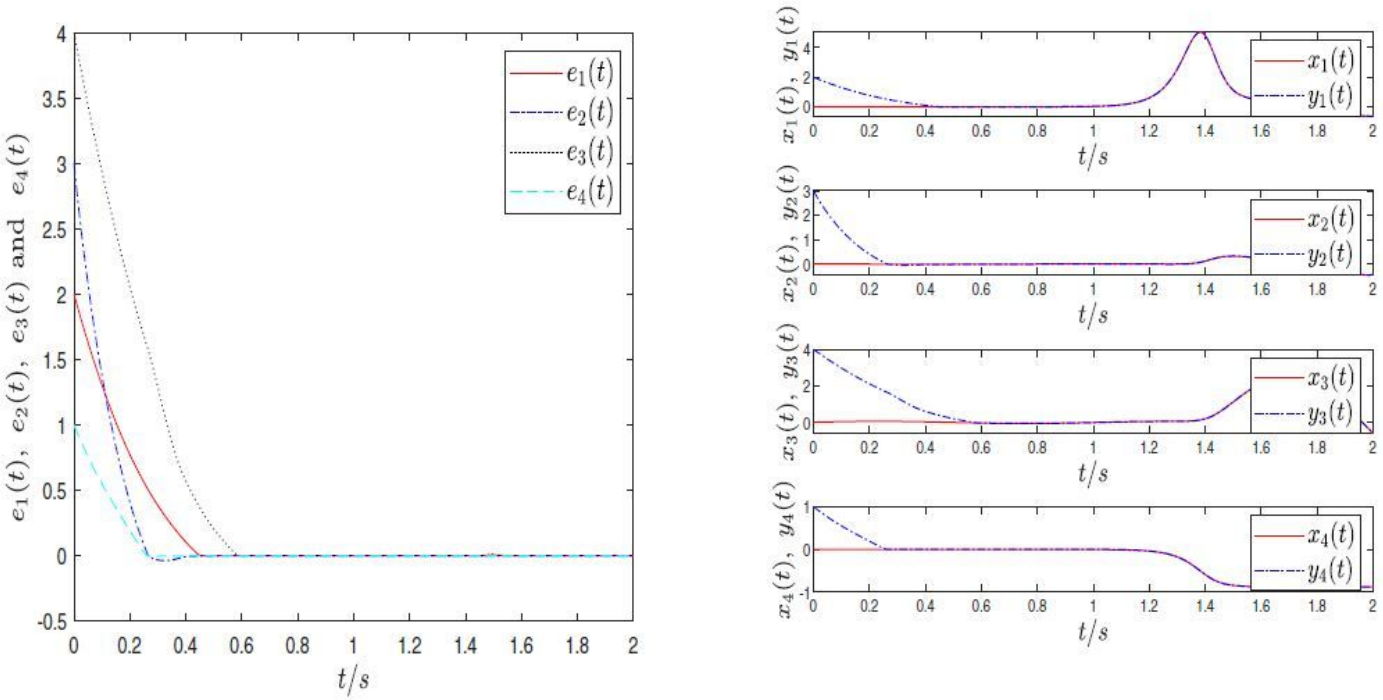


Figure 4

The time evolutions of the state variables and errors when v2 = 0:8 with e(0)=(2; 3; 4; 1)T .

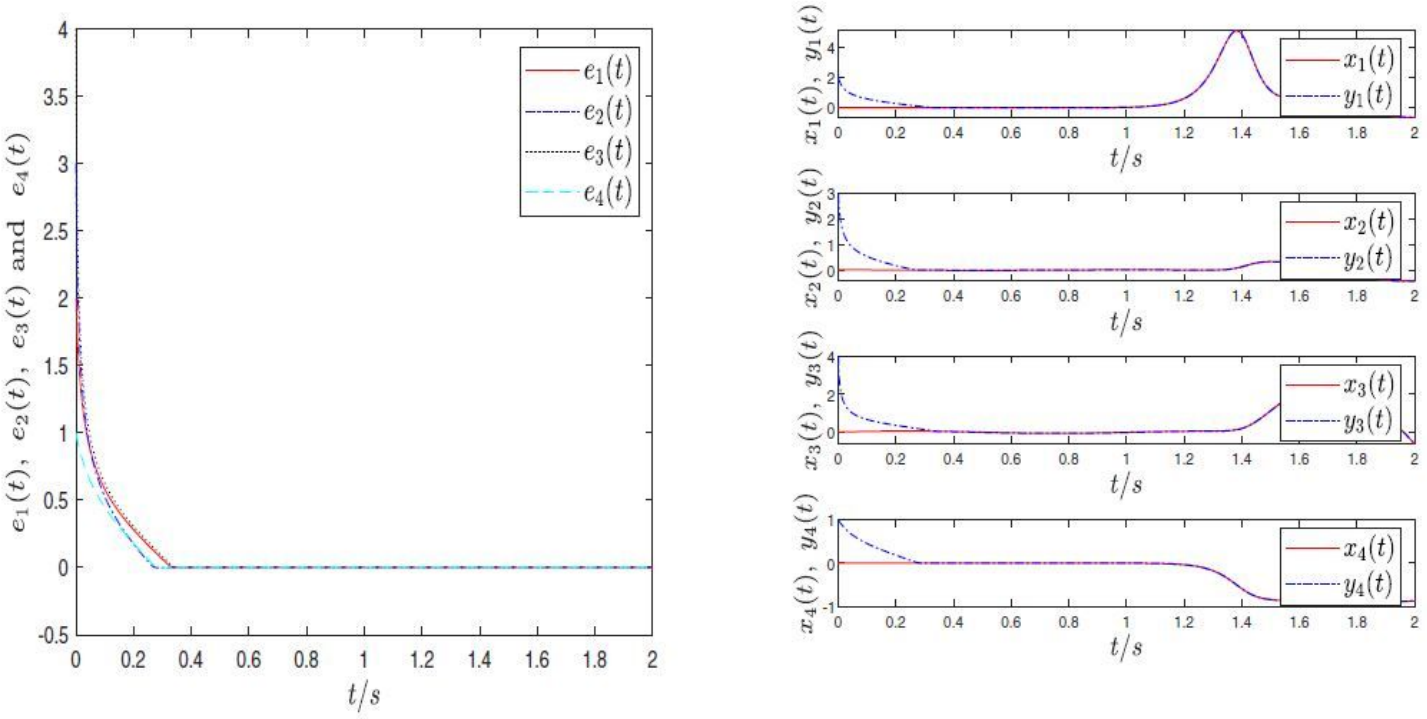


Figure 5

The time evolutions of the state variables and errors when v2 = 3 with e(0)=(2; 3; 4; 1)T .

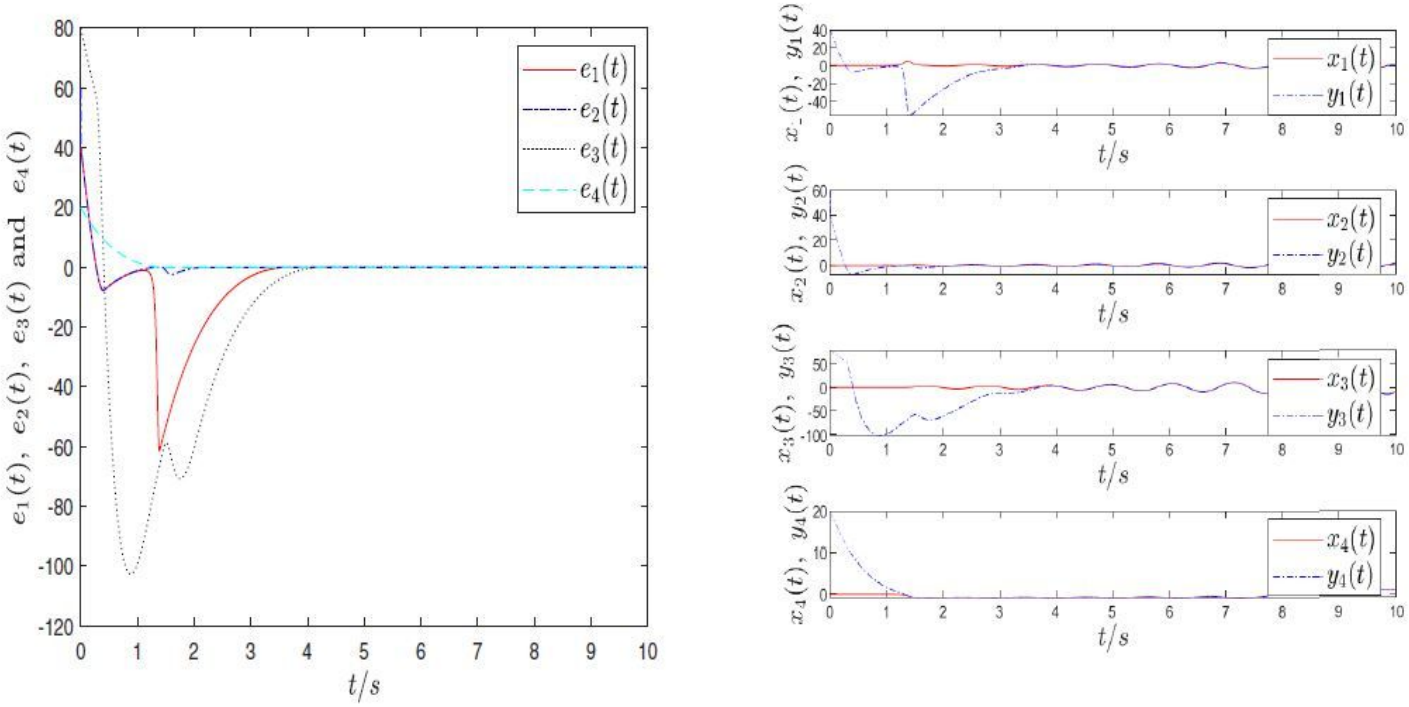


Figure 6

The time evolutions of the state variables and errors when v2 = 0:8 with e(0)=(40; 60; 80; 20)T .

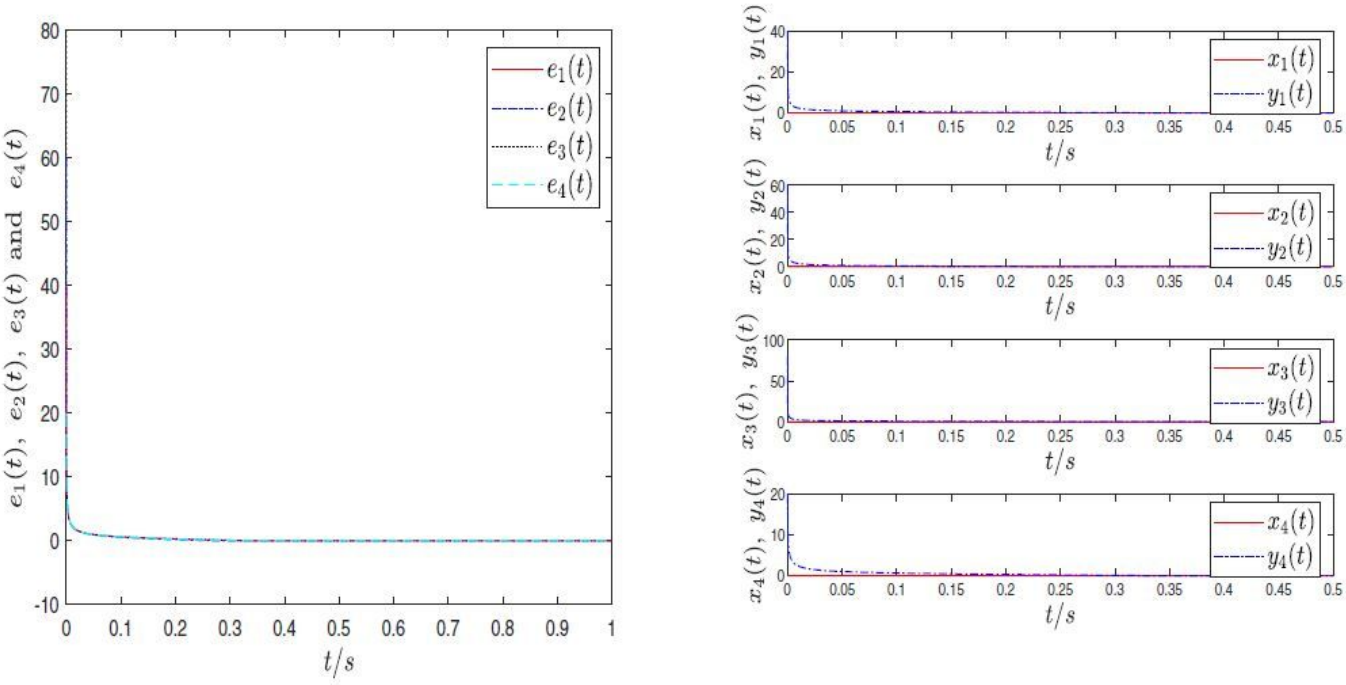


Figure 7

The time evolutions of the state variables and errors when v2 = 3 with e(0)=(40; 60; 80; 20)T .

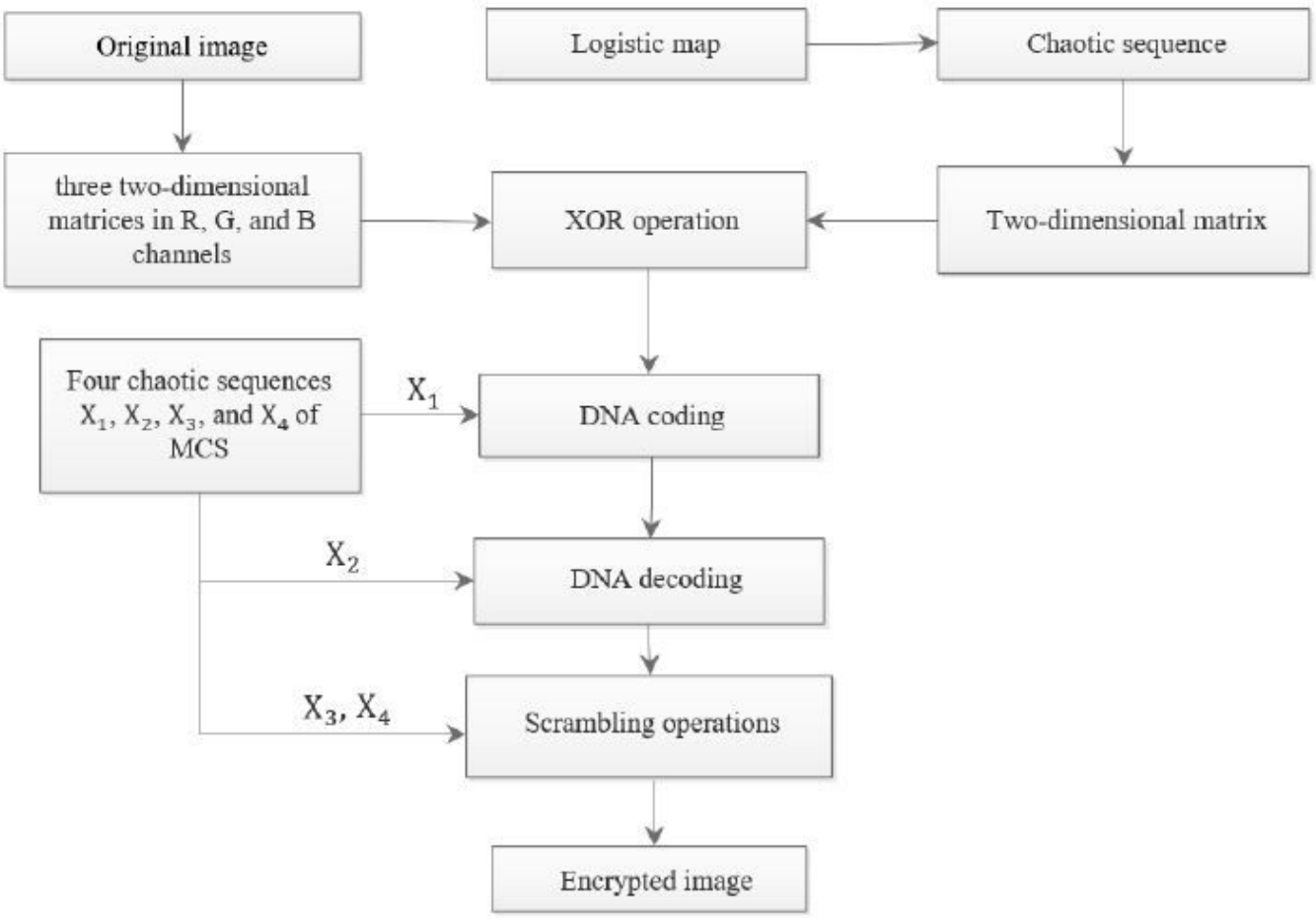
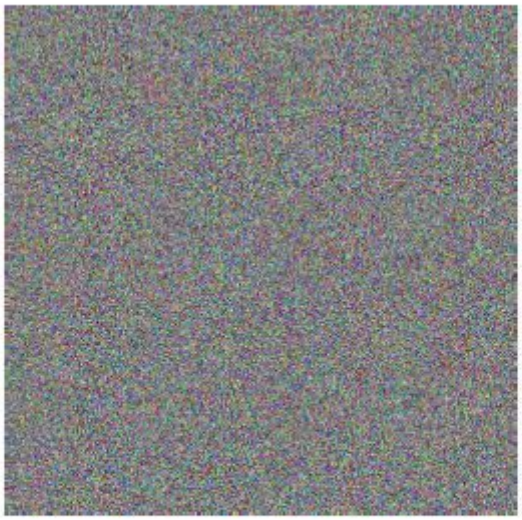


Figure 8

The flow chart of encryption algorithm.

(a)



(b)

Figure 9

Original image and encrypted image. (a) Original image. (b) Encrypted image.

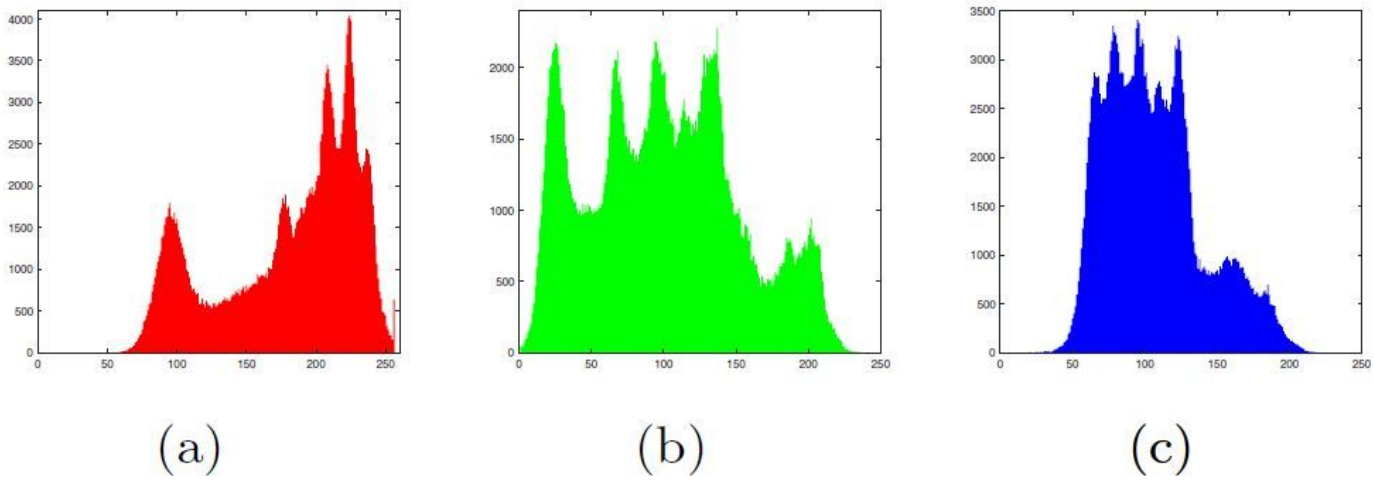


Figure 10

Histograms of original image. (a) Red channel. (b) Green channel. (c) Blue channel.

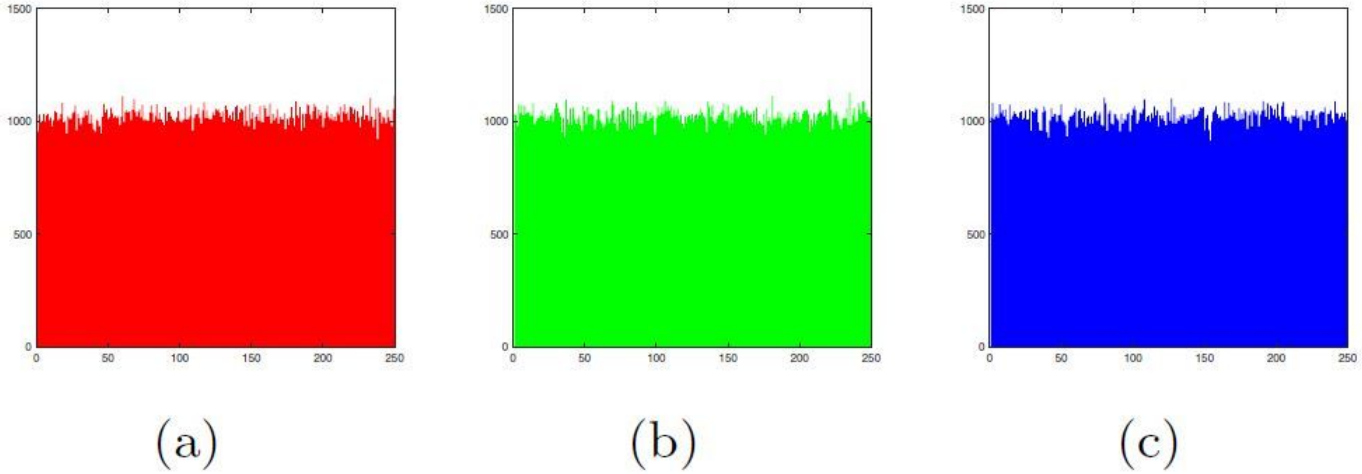


Figure 11

Histograms of encrypted image. (a) Red channel. (b) Green channel. (c) Blue channel.

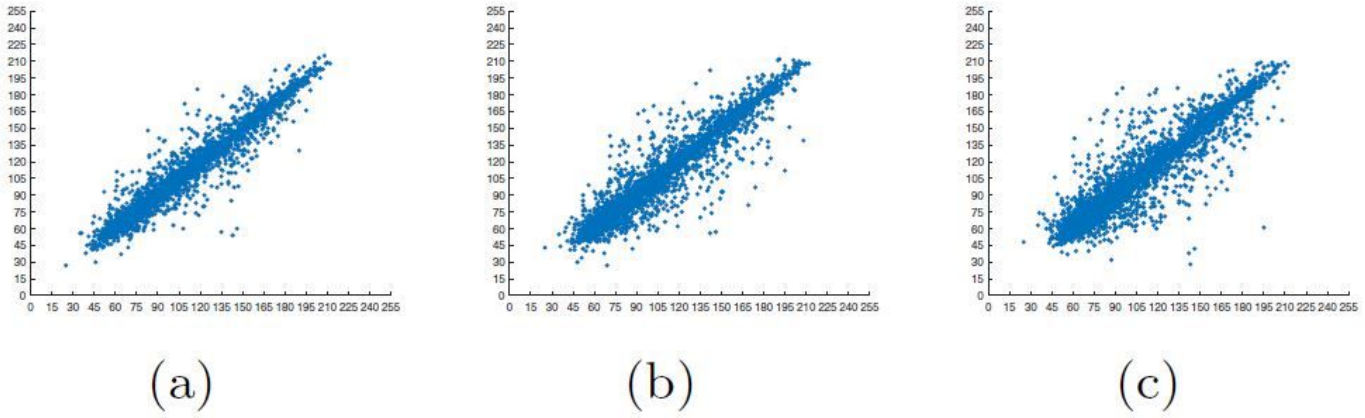


Figure 12

Correlation distributions in B channel of original image. (a) Horizontal direction. (b) Vertical direction. (c) Diagonal direction.

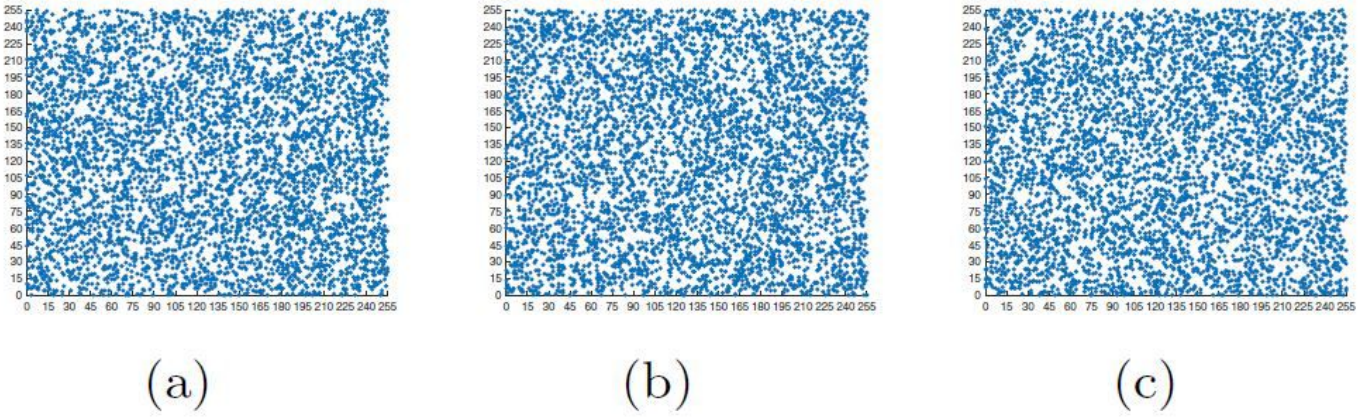


Figure 13

Correlation distributions in channel B of encrypted image. (a) Horizontal direction. (b) Vertical direction. (c) Diagonal direction.

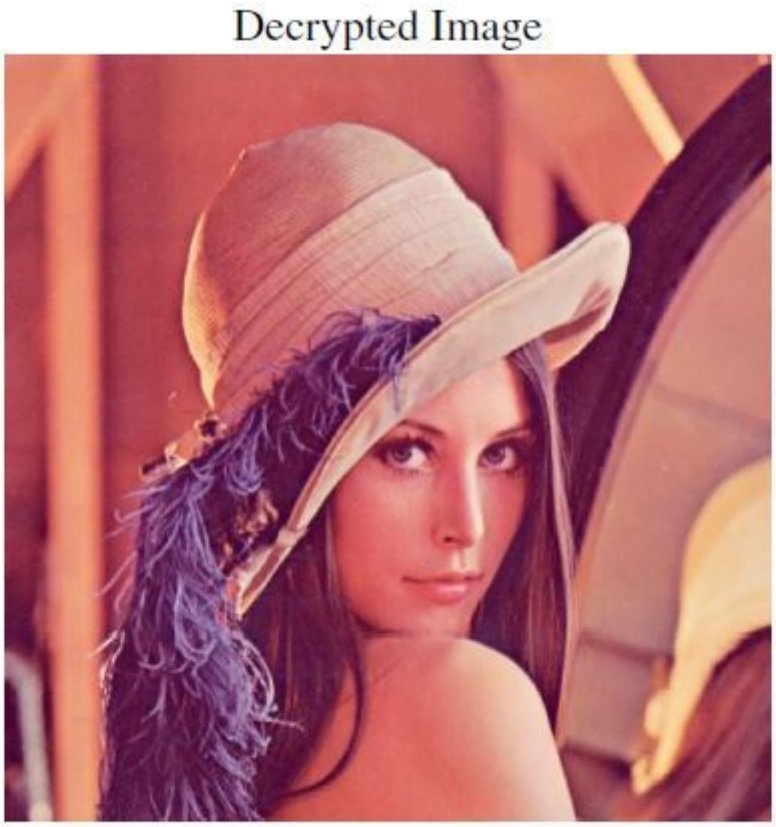


Figure 14

Decrypted image.

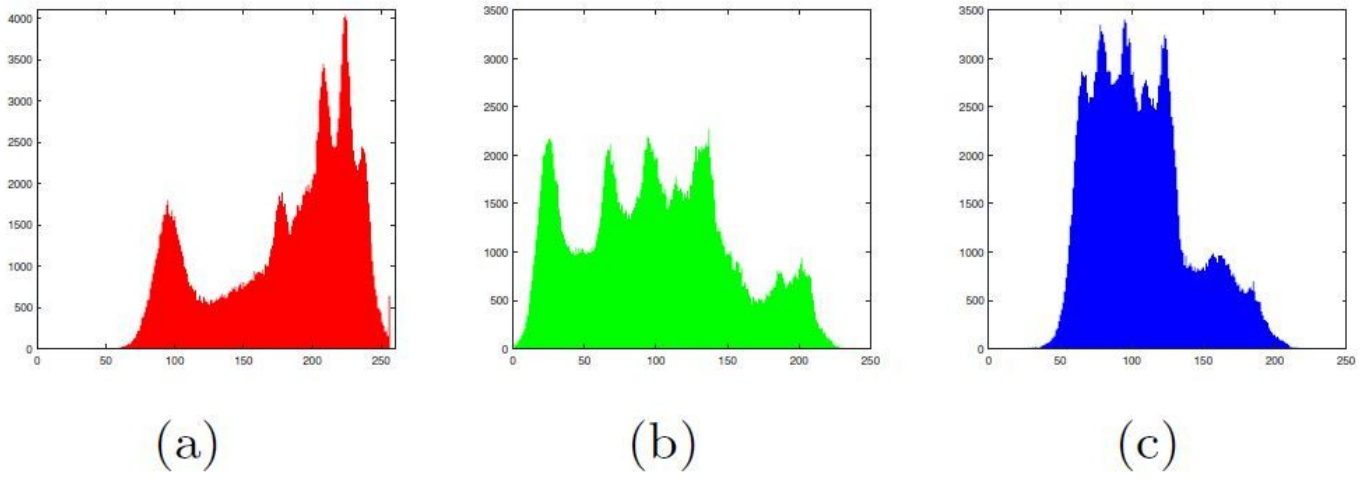


Figure 15

Histograms of decrypted image. (a) Red channel. (b) Green channel. (c) Blue channel.

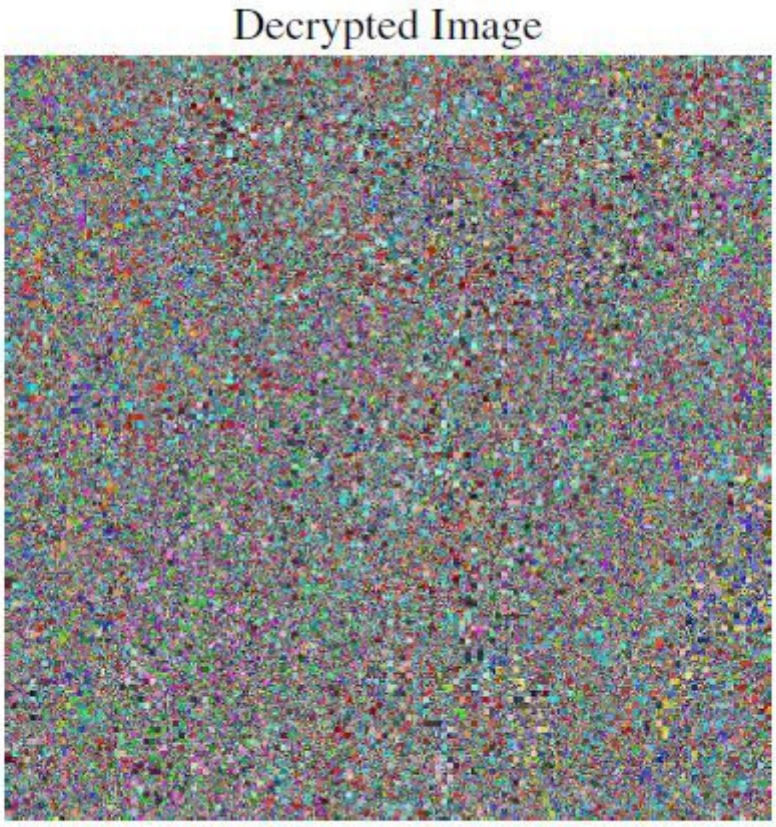


Figure 16

Decrypted image with keys slightly changed.