A Scheme for Image Encryption And Decryption of Chaotic System Based on memristors

Honghu Hua, Xi Zhu and Haijun Liu*

School of Electronic Science, National University of Defense Technology, Changsha, Hunan Province, 410073, China.

*Corresponding author’s e-mail: liuhaijun@nudt.edu.cn

Abstract. In this paper, a scheme for image encryption and decryption of chaotic system based on memristors has been proposed. A memristor-based chaotic circuit is simulated and demonstrated it has chaotic characteristics. Then, a memristor-based XOR operation is introduced. At last, image encryption and decryption is presented based on these two structures. Simulation results indicate that chaotic system consisting of memristor-based chaotic circuit and memristor-based XOR operator can achieve image encryption and decryption.

1. Introduction
Memristor is a kind of nonlinear circuit element with memory characteristics apart from the capacitor C, the resistor R and the inductor L. As the fourth independent two-terminal circuit element, it was first mathematically predicted by Leon Chua in 1971 from symmetric principles without experimental observation [1]. Until 2008, the Hewlett-Packard (HP) laboratory team first successfully developed a memristor with typical memristive features [2]. Since then, the research on the memristor has received extensive and close attention of the society due to its prospective potential in many different fields, such as high-density memory [3-4], neuromorphic computation [5-7] and logic computation [8-9].

The theoretical design and hardware implementation of chaotic cryptosystem have been developed comprehensively in recent years [10-12]. Itoh and Leon Chua proposed chaotic circuit based on memristors [13]. After that, chaotic circuit based on memristors has gotten the rapid development[14-16]. Furthermore, memristor-based chaotic circuit for image encryption and decryption has been proposed [17-18]. However, their XOR operations in the encryption and the decryption are based on the traditional CMOS technology. In this paper, a scheme for image encryption and decryption of chaotic system based on full memristors has been proposed, whose chaotic circuit and the XOR operator are both based on the memristors.

The rest of this paper expands according to the following structure. Section II presents the memristor-based chaotic circuit and the XOR operation in detail. In Section III, the simulation results are provided. Finally, the conclusions are drawn in Section IV.

2. The cryptosystem of memristor-based chaotic circuit and XOR operation
In this section, a novel scheme with memristor-based chaotic circuit and the XOR operator has been proposed.

2.1. Memristor-based chaotic circuit
The chaotic circuit is presented in Figure 1 according to the Chua’s memristor-based chaotic circuit and
the HP memristor model. It consists of two inductors, a capacitor, a negative resistor and HP memristor model. And its state equation is obtained as equation (1) shows on the basis of the Kirchhoff’s Circuit Laws, where \( M(r) = rR_{on} + (1-r)R_{off} \) and the window function \( f(r) = 1 - (2r - 1)^2p \).

\[
\frac{di_1}{dt} = \left[ u - M(r)i_1 \right]/L_1, \quad \frac{dt}{dt} = (i_1 - i_2)/C, \quad \frac{di_2}{dt} = (Ri_2 - u)/L_2, \quad \frac{dr}{dt} = kf(r)i_1
\]

Given \( x = i_1, \ y = u, \ z = i_2, \ e = r, \ a = L_1/L_1, \ b = 1/C, \ c = 1/L_2, \ R/L_2 = 1, \ k = 2.5, \ M(e) = M(r) = 0.025e + 10(1 - e) \), equation (1) can be written as shown in dimensionless equation (2) [19].

\[
\frac{dx}{dt} = \left[ y - M(e)x \right]a, \quad \frac{dx}{dt} = (i_1 - i_2)b, \quad \frac{dx}{dt} = z - cy, \quad \frac{dx}{dt} = 2.5f(e)x
\]

When \( a = 2.9, \ b = 3.4, \ c = 0.79, \) and the initial state \( x_0 = 0, \ y_0 = 0.1, \ z_0 = 0, \ e_0 = 0.3 \), the projection of the chaotic attractor is shown in Figure 2.

The chaotic sequences \( \{x_t, y_t, z_t, e_t | t = 1, 2, \ldots, N\} \) with divergence, aperiodicity and the high sensitivity for initial state \( \{x_0, y_0, z_0, e_0\} \) are generated for the cryptosystem.

2.2. Memristor-based XOR operation

The memristors based on the crossbar array can realize complete binary boolean logic with optimized computation complexity [9]. Figure 3 shows the process of realizing binary boolean logic. And Table 1 indicates the meaning of the variables in Figure 3. Firstly, initialize the memristors in the crossbar array. \( W \) determines whether memristors are set or reset; Secondly, write the signals into the crossbar array, which consist of A, B and C. A and B represent the voltage \( V_{dd} \) or 0, and C determines the direction of the voltage applied across the terminals; Lastly, read out the logic computing results by a small voltage. Although it can realize complete binary boolean logic, XOR operation is what we need. Therefore, setting \( W = 0, \ A = p, \ B = q, \ C = p \), which \( p \) and \( q \) are the input values, can achieve XOR operation in the memristor-based crossbar array.

![Figure 1. Chua’s memristor-based chaotic circuit](image)

![Figure 2. The projection of the chaotic attractor. (a) x-y-z Spatial phase trajectory; (b) x-y plane phase trajectory](image)
Figure 3. Memristor-based logic computing in crossbar array. (a) Step 1: initialization. (b) Step 2: writing operation by input of the other three variables: A, B, and C. Step 3: reading operation by a small read voltage.

Table 1. Variable assignment

| Logic 1     | Logic 0     |
|-------------|-------------|
| W           | WL: V_{dd}; BL: 0 | WL: 0; BL: V_{dd} |
| A           | V_{dd}      | 0               |
| B           | V_{dd}      | 0               |
| C           | WL: A; BL: B | WL: B; BL: A    |

2.3. Cryptosystem scheme

A memristor-based chaotic cryptosystem scheme is shown in Figure 4. User key is the initial state of the memristor-based chaotic circuit. Once it is given, the chaotic sequences are generated, which are input into the memristor-based XOR operator with the plain image. And the output image is the cipher image. The decryption is the same as the encryption. Chaotic sequences are input into the memristor-based XOR operator with the cipher image, and the decrypted image is the operator’s output.

Figure 4. Cryptosystem scheme
According to the cryptosystem scheme in Figure 4, the process of the image encryption can be obtained as the following Table 2 shows. The process of the decryption is similar to the process of the encryption.

Table 2. The process for the image encryption

| Input: User key and plain image |
|---------------------------------|
| 1. generate the chaotic sequences \{x_t, y_t, z_t, e_t \mid t=1,2,\ldots,N,\ldots\} with User key \{x_0, y_0, z_0, e_0\}. |
| 2. get the transformed chaotic sequences \{x'_t, y'_t, z'_t, e'_t \mid t=k, k+l, \ldots, k+N^q\} whose values range from 0 to 255. |
| 3. get the output sequence of the bit-by-bit XOR operator whose inputs are the \(x'_t, y'_t, z'_t\) and \(e'_t\). |
| 4. turn the image into the sequence of length \(N\times N\). |
| 5. get the output sequence of the bit-by-bit XOR operator whose inputs are the transformed chaotic sequence and the sequence of the image. |
| 6. transform the output sequence into the cipher image. |

Output: cipher image

3. Simulation results and discussion

According to the cryptosystem scheme and the process of encryption and decryption, A simulation based on it has been carried out.

There are four state values \(\{x_t, y_t, z_t, e_t \mid t=1,2,\ldots,N,\ldots\}\). When the initial state values are set \(\{x_0=0, y_0=0.1, z_0=0, e_0=0.3\}\), the chaotic sequences will be generated according to the time sequence. Here state values are chosen as \(\{x'_t, y'_t, z'_t, e'_t \mid t=2,5,8,\ldots,145199\}\) randomly. And the chaotic sequence is \(x'_t \oplus y'_t \oplus z'_t \oplus e'_t\), which ‘\(\oplus\)’ represents bit-by-bit XOR operator.

Then the chaotic sequence is transformed in the light of above step 2 and 3 as shown in Figure 5(b). And Figure 5(a) is the plain image. These two images are input into the memristor-based XOR operator and Figure 5(c) is their output image, which, in other words, is the cipher image. Similarly, the cipher image and Figure 5(b) are input into the memristor-based XOR operator and the output is the plain image as shown in Figure 5(d).

The initial state is the key of the cryptosystem. If the initial state values have been wrong (e.g. \(\{x_0=0, y_0=0.1, z_0=0, e_0=0.32\}\)), the image of the chaotic sequence with wrong key is shown in Figure 5(e). And the decrypted image with the wrong key is shown in Figure 5(f). The cipher image can’t be decrypted correctly, although these two keys are very close.

The simulation results of the plain image encryption and decryption show that the scheme can work well. And it can work as an important way for encryption and decryption.
Figure 5. Simulation results of image encryption and decryption. (a) original image. (b) image of the chaotic sequence. (c) cipher image. (d) decrypted image with right key. (e) image of the chaotic sequence with wrong key. (f) decrypted image with wrong key.

4. Conclusion
In this paper, a scheme for image encryption and decryption of chaotic system based on full memristors has been proposed, whose chaotic circuit and the XOR operator are both based on the memristors. The performance of the chaotic circuit and the XOR logic operation based on the memristor run well. What’s more, a classic image has been encrypted and decrypted by this system, which demonstrates this scheme can work well and the memristors can be used as the key technology for the encryption and decryption of the chaotic system.

Acknowledgement
This work was supported by the National Natural Science Foundation of China (No. 61604177, 61471377, 61704191 and 61701509) and research funding of NUDT JC15-04-02.

Reference
[1] Chua, L. (1971) Memristor-The missing circuit element. IEEE Transactions on Circuit Theory, 18(5):507-519.
[2] Strukov D.B., Snider G.S., Stewart D.R., et al. (2008) The missing memristor found. Nature, 453(7191):80-83.
[3] Akinaga H., Shima H. (2010) Resistive Random Access Memory (ReRAM) Based on Metal Oxides. Proceedings of the IEEE, 98(12):2237-2251.
[4] Seo M.S., Park J.W., Lim K.S., et al. (2008) Transparent resistive random access memory and its characteristics for nonvolatile resistive switching. Applied Physics Letters, 93(22):2749.
[5] Covi E., Brivo S., Serb A., et al. (2016) HfO2-based memristors for neuromorphic applications. IEEE International Symposium in Circuits and System, Montreal. pp. 393-396.
[6] Jo S.H., Chang T., Ebong I., et al. (2010) Nanoscale Memristor Device as Synapse in Neuromorphic Systems. NANO LETTERS, 10(4):1297-1301.
[7] Indiveri G., Linares-Barranco B., Legenstein R., et al. (2013) Integration of nanoscale memristor synapses in neuromorphic computing architectures. Nanotechnology, 24(38):384010.
[8] Wong H.S.P., Salahuddin S. (2015) Memory leads the way to better computing. Nature Nanotechnology, 10(3):191-194.
[9] Li Y., Zhou Y.X., Xu L., et al. (2016) Realization of Functional Complete Stateful Boolean Logic in Memristive Crossbar. Acs Appl Mater Interfaces, 8(50):34559-34567.
[10] Qiao Z.W., Han Y., Wei X.Y. (2007) Design and Implementation of the File Encryption Algorithm Based on One Dimensional Chaos Method. Journal of North University of China, 28(6):37-50.

[11] Ansarmohammadi S.A., Shahinfar S., Nejatollahi H. (2016) Fast and area efficient implementation for chaotic image encryption algorithms. CSI International Symposium on Computer Architecture & Digital Systems. Tehran.

[12] Murilloescobar M.A., Cruzherández C., Abundizpérez F., et al. (2016) Implementation of an improved chaotic encryption algorithm for real-time embedded systems by using a 32-bit microcontroller. Microprocessors & Microsystems, 45:297-309.

[13] Itoh M., Chua L.O. (2008) MEMRISTOR OSCILLATORS. International Journal of Bifurcation and Chaos.

[14] Bao B., Zhenghua M.A., Jianping X.U., et al. (2014) A SIMPLE MEMRISTOR CHAOTIC CIRCUIT WITH COMPLEX DYNAMICS. International Journal of Bifurcation and Chaos, 21(09):1102999.

[15] Buscarino A., Fortuna L., Frasca M., et al. (2012) A chaotic circuit based on Hewlett-Packard memristor. Chaos: An Interdisciplinary Journal of Nonlinear Science, 22(2):023136.

[16] Lin Z.H., Wang H.X. (2009) Image encryption based on chaos with PWL memristor in Chua's circuit. 2009 International Conference on Communications, Circuits and Systems. Milpitas. 964-968.

[17] Yang C., Hu Q., Yu Y., et al. (2016) Memristor-Based Chaotic Circuit for Text/Image Encryption and Decryption. International Symposium on Computational Intelligence & Design. Hangzhou. pp. 447-450.

[18] Wang B., Zou F.C., Cheng J. (2017) A memristor-based chaotic system and its application in image encryption. Optik - International Journal for Light and Electron Optics.

[19] Zhang Y.H., Sun L.S. (2013) Simulations of Chaotic Circuit Based on Memristor. JOURNAL OF EEE, 35(2):54-57.