A Dynamic AES Encryption Based on Memristive Chaos Neural Network

Y. A. Liu

University of Electronic Science and Technology of China

L. Chen

Beijing Microelectronics Technology Institute

X. W. Li

Beijing Microelectronics Technology Institute

Y. L. Liu

University of Electronic Science and Technology of China

S. G. Hu

University of Electronic Science and Technology of China

Q. Yu

University of Electronic Science and Technology of China

T. P. Chen

Nanyang Technological University

Y. Liu (✉ yliu1975@uestc.edu.cn)

University of Electronic Science and Technology of China

Research Article

Keywords: AES, memristive neural network, chaos, RSA

Posted Date: October 6th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-950992/v1>

License: This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

A Dynamic AES Encryption based on Memristive Chaos Neural Network

Y. A. Liu¹, L. Chen², X. W. Li², Y. L. Liu¹, S. G. Hu¹, Q. Yu¹, T. P. Chen³,
and Y. Liu^{1,a)}

¹State Key Laboratory of Electronic Thin Films and Integrated Devices,
University of Electronic Science and Technology of China, Chengdu
610054, P. R. China.

²Beijing Microelectronics Technology Institute (BMTI), Beijing 10076, P.
R. China.

³Nanyang Technological University, Singapore 639798.

^{a)}Corresponding author: Y. Liu (e-mail: yliu1975@uestc.edu.cn)

Abstract: This paper proposes an Advanced Encryption Standard (AES) encryption technique based on memristive neural network. A memristive chaotic neural network is constructed by the use of the nonlinear characteristics of the memristor. The chaotic sequence, which is sensitive to the initial value and has good random characteristics, is used as the initial key of AES grouping to realize "one-time-one-secret" dynamic encryption. Results show that the algorithm has higher security, larger key space and stronger robustness than the conventional AES. It can effectively resist the initial key fixed and exhaustive attacks.

Keywords: AES, memristive neural network, chaos, RSA.

I. Introduction

Advanced Encryption Standard (AES), a group symmetric encryption with variable key length, take advantages of good security, high efficiency, easy implementation and strong flexibility, and has become an international mainstream standard encryption system.¹⁻³ However, there are still some security problems in AES, such as the fixed initial key, key decoding, and limited key space.⁴⁻⁷ Chaotic systems were introduced to improve the AES encryption algorithm's security.⁸⁻¹² In 2004, A one-way coupled spatiotemporally chaotic map lattice was used to construct a new AES cryptosystem.⁸ in 2018, a novel chaos-based hybrid encryption algorithm design for secure and effective image encryption was presented.⁹ In 2019, an image encryption algorithm was proposed based on the combination of the chaos sequence and the modified AES.¹⁰ In 2020, A four-dimensional chaotic system was applied to generate key and improve advanced encryption standard.¹¹ In 2021, a modified AES cryptosystem with dynamic random keys based on chaos synchronization was presented.¹²

As the fourth fundamental circuit component, memristor has many advantages,¹³ such as non-linearity, memory properties, low power consumption, simple structure, and so on.¹⁴ There is also a lot of research on building chaotic systems and neural networks based on memristors.¹⁵⁻³⁰ For example, in 2008, it was derived that several nonlinear oscillators from

Chua's oscillators by replacing Chua's diodes with memristors.¹⁵ In 2012, delayed switching effect was used to control the switching of a memristor synapse between two neurons.¹⁷ In 2018, I. Boybat present a multi-memristive synaptic architecture with an efficient global counter-based arbitration scheme for a spiking neural network.¹⁹ A simple and effective method was given for designing the autonomous memristor chaotic systems of infinite chaotic attractors.²¹ In 2019, a chaotic memristor, which only contains meminductor, and memcapacitor models, was presented.²² In 2020, a class of electro-optical memristors was introduced, which can emulate the key properties of synapses and neurons.²⁵ A physical memristor based on the Muthuswamy – Chua chaotic system (circuit) was provided.²⁷

In this paper, based on the memristor-based transient chaotic neural network (MTCNN),³¹ the chaotic state for a long time is realized by the MTCNN. By MTCNN, AES initial key is dynamically generated to realize "one time one secret." Simultaneously, to improve the security, the Rivest-Shamir-Adleman(RSA) encryption is used to encrypt the initial parameters of the chaotic network. The sensitivity, key space, information entropy, correlation indexes, and poker test have been carried out and the capability and improvement of this proposed AES cryptosystem have been examined.

II . A dynamic AES encryption system

Fig. 1 shows the illustration of the encryption framework. The text is

encrypted with AES, and the parameters of the key generated by the chaotic neural network are encrypted with RSA. Taking a 128-bit key AES encryption as an example, AES algorithm needs ten rounds of encryption, and each round of encryption needs a different secret key. The chaotic sequence generated by MTCNN can be used as the key for each round of encryption and decryption.

The chaotic sequence generated by MTCNN realizes key generation through the following process. Fig.2 shows the 128-bit key generation process. Firstly, 16-bit floating-point digit in $[0,1]$ is generated by 16 iterations in the chaotic period. Then, 6 to 10 digits after the decimal point of 16 floating-point numbers are taken, and it is divided by 256 to obtain 16 integers in $[0, 255]$. By converting decimal system to binary system, each integer in the $[0, 255]$ is converted into an 8-bit binary digit to obtain 128-bit sequence, i.e., 128-bit key.

As a chaotic neural network is sensitive to the initial value, with the slight modification of the initial value each time, a different non-duplicate key sequence can be obtained, conforming to the key standard. The key generated from each initial value can be used for one round of AES encryption, and ten initial values can complete one AES block encryption.

III. Discussion

We examine the text encryption and decryption by the proposed

algorithm. The encryption and parameters of MTCNN were presented in Ref. 31.

As shown in Fig. 3, this system successfully realizes the encryption and decryption of classic picture. At the same time, through statistics of the encryption, slightly change of the key parameters (When y_0 in Ref. 31 is varied 1×10^{-16}), may result in the bit change rate of ciphertext for 51.03%. And the key avalanche phenomenon is apparent. This verifies the key dependence and effectiveness of the algorithm.

As shown in Fig. 4, the autocorrelation of the chaotic binary sequence generated by MTCNN is examined, fully conforming to random sequence characteristics. When $m = 0$, the autocorrelation function is equaled to 0.25; and when m is not equaled to 0, the autocorrelation function tends to be zero. The whole autocorrelation function is close to the δ function, being quasi-random. Moreover, by measuring the frequency of chaotic sequence, the average value of the balance degree of the chaotic sequence is 49.76%. That means that “0” and “1” sequences of chaotic sequence are evenly distributed. The balance degree of the chaotic sequence is good as shown in Fig. 4(a)-(d). It can also be seen that the values of autocorrelation sidelobe and cross-correlation function of ciphertext sequence are close to 0, indicating that the ciphertext encrypted by MTCNN shows good randomness and is not related to plaintext.

Theoretically, the key space of conventional “AES128” is $2^{128} \approx$

3.4×10^{38} . The memristive neural network used in this work can act as the parameter of the key taking the initial parameters Ref. 31 of M_0 for the memristor, damping factor k of neuron membrane, steepness parameter ε for output, initial current I_0 flowing through memristor, the initial state of the neuron y_0 , the characteristic parameter k_m , and the scaling parameters b and c . Parameters' type and range of the proposed MTCNN are presented in Table 1. The total key space size is equal to the product of all parameters' space: $K = K_{M_0} \times K_k \times K_\varepsilon \times K_{I_0} \times K_{y_0} \times K_{k_m} \times K_b \times K_c \approx 1.65 \times 10^{124}$ where K_{M_0} , K_k , K_ε , K_{I_0} , K_{y_0} , K_{k_m} , K_b and K_c are key space for parameters in Table 1, respectively.

Fig. 5 shows the frequency detection for encryption with the proposed MTCNN. It should be noted that no matter the plaintext has prominent statistical characteristics or randomness, the corresponding ciphertext shows good randomness. That means the ciphertext does not depend on the statistical characteristics of plaintext. The algorithm has good independence of plaintext and can effectively resist differential attacks. Furthermore, 20 times of poker test were carried out, and the test results are shown in Table 2. According to Ref. 32, The 20000-bit random ciphertext, encrypted by AES based on MTCNN is divided into 4-bit groups, and $f(i)$, the number represented by 4-bit group elements, is

counted respectively. The statistic X is calculated by Eq.1, which passes when $2.16 < X < 46.17$.

$$X = \frac{16}{5000} \times (\sum_{i=0}^{15} [f(i)^2]) - 5000 \quad [1]$$

The results show X all falls in the range $[8.46, 27.28]$, and the average values is $16.54 \in [2.16, 46.17]$. The ciphertext of this algorithm has good randomness and can resist attacks such as statistical analysis.

IV. Conclusion

In summary, this paper proposes an improved AES algorithm based on MTCNN. Based on the nonlinear characteristics of memristive chaotic neural network, the chaotic sequence, which has good random characteristics, is used as the initial key of AES grouping to realize "one-time-one-secret" dynamic encryption. The proposed AES algorithm can effectively improve the properties of seed key, key space, and anti-attack ability of AES algorithm.

References

- ¹ Daemen, J. The Design of Rijndael. *Information Security & Cryptography* 26, 137-139 (2001).
- ² Boukis, A. C., Reiter, K., Frlich, M., Hofheinz, D. & Meier, M. Multicomponent reactions provide key molecules for secret communication. *Nat Commun* 9 (2018).
- ³ Nair, R., Yuen, H. P., Corndorf, E., Eguchi, T. & Kumar, P. Quantum Noise Randomized Ciphers. *Phys Rev A* 74, (2006).
- ⁴ Zheng, S. H. et al. A Persistent Fault-Based Collision Analysis Against the Advanced Encryption Standard. *Ieee T Comput Aid D* 40, 1117-1129(2021).
- ⁵ Prabhakaran, V. & Kulandasamy, A. Hybrid semantic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection. *Neural Comput Appl* (2021).
- ⁶ El Batouty, A. S., Farag, H. H., Mokhtar, A. A., El-Badawy, E. A. & Aly, M. H. Improvement of Radio Frequency Identification Security Using New Hybrid Advanced Encryption Standard Substitution Box by Chaotic Maps. *Electronics-Switz* 9, (2020).
- ⁷ Sugawara, T., Li, Y. & Sakiyama, K. Probing attack of share-serial threshold implementation of advanced encryption standard. *Electron Lett* 55, 517-518(2019).
- ⁸ Ye, W. P. et al. Experimental realization of a highly secure chaos communication under strong channel noise. *Phys Lett A* 330, 75-84(2004).
- ⁹ avuolu, ü., Kaar, S., Zengin, A. & Pehlivan, I. A novel hybrid encryption algorithm based on chaos and S-AES algorithm. *Nonlinear Dynam* (2018).
- ¹⁰ Arab, A., Rostami, M. J. & Ghavami, B. An image encryption method based on chaos system and AES algorithm. *J Supercomput* 75, 6663-6682(2019).
- ¹¹ Yang, C. H. & Chien, Y. S. FPGA Implementation and Design of a Hybrid Chaos-AES Color Image Encryption Algorithm. *Symmetry-Basel* 12, (2020).
- ¹² Lin, C. H., Hu, G. H., Chan, C. Y. & Yan, J. J. Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm. *Appl Sci-Basel* 11, (2021).
- ¹³ Chua, L. O. Efficient Computer Algorithms for Piecewise-Linear Analysis of Resistive Nonlinear Networks. *IEEE Trans Circuit Theory* 18, 73-85 (1971).
- ¹⁴ Strukov, D. B., Snider, G. S., Stewart, D. R. & Williams, R. S. The missing memristor found. *Nature* (2008).

- ¹⁵ Itoh, M. & Chua, L. O. MEMRISTOR OSCILLATORS. *Int J Bifurcat Chaos* 18, 3183-3206 (2008).
- ¹⁶ Wang, F. Z. et al. Delayed switching applied to memristor neural networks. *J Appl Phys* 111 (2012).
- ¹⁷ Shen, J. X. et al. Mimicking Synaptic Plasticity and Neural Network Using Memtransistors. *Adv Mater* 30 (2018).
- ¹⁸ Fukami, S. & Ohno, H. Perspective: Spintronic synapse for artificial neural network. *J Appl Phys* 124 (2018).
- ¹⁹ Boybat, I. et al. Neuromorphic computing with multi-memristive synapses. *Nat Commun* 9 (2018).
- ²⁰ Wang, C. H., Zhou, L. & Wu, R. P. The Design and Realization of a Hyper-Chaotic Circuit Based on a Flux-Controlled Memristor with Linear Memductance. *J Circuit Syst Comp* 27, (2018).
- ²¹ Sun, J. W., Zhao, X. T., Fang, J. & Wang, Y. F. Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization. *Nonlinear Dynam* 94, 2879-2887 (2018).
- ²² Yuan, F. & Li, Y. X. A chaotic circuit constructed by a memristor, a memcapacitor and a meminductor. *Chaos* 29, (2019).
- ²³ Huang, H. M. et al. Implementation of Dropout Neuronal Units Based on Stochastic Memristive Devices in Neural Networks with High Classification Accuracy. *Adv Sci* 7 (2020).
- ²⁴ Chen, T., Wang, L. D. & Duan, S. K. Implementation of circuit for reconfigurable memristive chaotic neural network and its application in associative memory. *Neurocomputing* 380, 36-42 (2020).
- ²⁵ Emboras, A. et al. Opto-electronic memristors: Prospects and challenges in neuromorphic computing. *Appl Phys Lett* 117 (2020).
- ²⁶ Zhang, Y. et al. Brain-inspired computing with memristors: Challenges in devices, circuits, and systems. *Appl Phys Rev* 7 (2020).
- ²⁷ Ginoux, J. M., Muthuswamy, B., Meucci, R., Euzzor, S. & Ganesan, K. A physical memristor based Muthuswamy–Chua–Ginoux system. *Sci Rep-Uk* 10 (2020).
- ²⁸ Lin, P. et al. Three-dimensional memristor circuits as complex neural networks. *Nat Electron* 3, 225-232 (2020).
- ²⁹ Deng, Y. & Li, Y. X. A memristive conservative chaotic circuit consisting of a memristor and a capacitor. *Chaos* 30, (2020).
- ³⁰ Lai, Q., Wan, Z. Q., Kengne, L. K., Kuate, P. D. K. & Chen, C. Y. Two-Memristor-Based Chaotic System With Infinite Coexisting Attractors. *Ieee T Circuits-Ii* 68, 2197-2201(2021).

- ³¹ Liu, Y. A., Yu, Q., Hu, S. G., Qiao, G. C. & Liu, Y. A memristor-based transient chaotic neural network model and its application. *J Appl Phys* 126, (2019).
- ³² Murphy, S. The Power of NIST Statistical Testing of AES Candidates. (2000).

Acknowledgments

This work is supported by NSFC under project Nos. 61774028, 92064004 and 61771097.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Author information

State Key Laboratory of Electronic Thin Films and Integrated Devices,
University of Electronic Science and Technology of China, Chengdu
610054, P. R. China.

Y. A. Liu , Y. L. Liu, S. G. Hu, Q. Yu, and Y. Liu

Beijing Microelectronics Technology Institute (BMTI), Beijing 10076, P.
R. China.

L. Chen, X. W. Li

Nanyang Technological University, Singapore 639798.

T. P. Chen

Contributions

Y. A. Liu initiated the idea, designed the memristive chaotic neural network for AES. Y. L. Liu conducted the simulation experiments. L. Chen and X. W. Li discussed and analyzed the results. Y. Liu supervised the project, provided advices and technical guidance. S. G. Hu, Q. Yu and T. P. Chen gave necessary information for this study. Y. A. Liu and Y. Liu wrote the

main manuscript text, and other authors commented on the manuscript at all stages.

Corresponding author

Correspondence to Y. Liu (e-mail: yliu1975@uestc.edu.cn).

Competing interests

The authors declare no competing interests.

Table 1. List of parameter types and range of the proposed MTCNN

Parameter	Data type	Value range	Space size
M_0	double	[400,2000]	$K_{M_0} \approx 1600 \times 10^{16}$
k	double	[0.45,0.99]	$K_k \approx 0.54 \times 10^{16}$
$1/\varepsilon$	int	[400,1000]	$K_\varepsilon \approx 600$
I_0	double	[0.6,0.7]	$K_{I_0} \approx 0.1 \times 10^{16}$
y_0	double	[0.1,0.9]	$K_{y_0} \approx 0.8 \times 10^{16}$
k_m	double	$[1 \times 10^9, 20 \times 10^9]$	$K_{k_m} \approx 19 \times 10^9 \times 10^{16}$
b	double	[50,150]	$K_b \approx 100 \times 10^{16}$
c	double	$[9 \times 10^{-6}, 3 \times 10^{-5}]$	$K_c \approx 21 \times 10^{-6} \times 10^{16}$

Table 2. The Results of 20 times of Poker Test

Test Results of statistic X			
13.34	19.18	23.93	8.46
14.61	17.29	18.64	14.57
20.33	10.62	9.66	27.28
15.87	16.72	12.06	18.98
21.36	13.54	17.22	17.09

Fig. 1. Schematic illustration of the proposed AES encryption and decryption process based on MTCNN

Fig. 2. Schematic diagram of the 128-bit key generation by MTCNN

Fig. 3. Display of encryption and decryption based on the proposed MTCNN. (a) original image; (b) the image after MTCNN encryption; and (c) the image after decryption.

Fig. 4. Correlation detection of encryption algorithm based on MTCNN. The autocorrelation function for (a) the chaotic sequence, (b) the ciphertext, (c) the plaintext; and (d) the cross-correlation function values of plaintext and ciphertext.

Fig. 5. Frequency detection of the encryption algorithm based on the proposed MTCNN.