ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 147

International Conference on Network, Communication, Computer Engineering (NCCE 2018)

Hopfield Neural Network and AES Combined with Hyperchaos Image Encryption Algorithm

Yong Wang, Shuo Chen [a)], Ying Wang

School of computers, Guangdong University of Technology, Guangzhou 510003, China

[a)] Corresponding author: 386817263@qq.com

Abstract. By analyzing the current image encryption algorithm based on a class of artificial neural network in recent years, this paper proposes a new hyperchaotic image encryption algorithm based on 4D of Hopfield-type neural network and AES(Advanced Encryption Standard) encryption algorithm, First, defines four number and a average value of plaintext image pixel as key, hyperchaos sequence generated by Hopfield-type neural network as the goal keys of AES algorithm; Then, the plaintext image and hyperchaos sequence to exclusive or processing; Finally, the goal key generation into the AES algorithm of triple encryption cipher. The simulation results show that the algorithm can effectively combines the advantages of two algorithms, achieve good encryption effect.

Key words: 4d of Hopfield-type neural network; AES; hyperchaotic.

INTRODUCTION

In the past ten years, chaos-based image encryption algorithm is the mainstream of image encryption technology. The chaotic system is a nonlinear dynamic system. It is sensitive to initial conditions and system parameters, and has white noise, pseudo-random sequence and interval ergodic chaos. Therefore, it is often used in the encryption algorithm. By changing some existing orders of the images, the pixels are arranged according to some operations to form a noise-like image to achieve the encryption effect [1]. The high-dimensional chaotic systems, especially the hyperchaotic systems, will increase the security of the cryptosystem by using the hyperchaotic system because the key space is large, with more than two positive Lyaponuv indices, more complex and unpredictable nonlinear behaviors. [2,3,4]. Among them, four-dimensional Hopfield neural network with nonlinear, associative memory, can directly generate a random matrix with good randomness to achieve the effect of hyperchaos, making 2D image encryption scheme design more reliable [5,6,7,8].

The key point of the AES encryption algorithm is too small and fixed. The four-dimensional Hopfield neural network can be fully utilized to generate a set of hyperchaotic sequences as the target keys for AES encryption. This will greatly enhance the AES algorithm Encryption security, and AES encryption algorithm S box transformation, row shift box column obfuscation has a very perfect encryption effect, the combination of both can make the image encryption security greatly improved. Accordingly, this paper presents a new four-dimensional Hopfield hyperchaotic neural network and AES algorithm combined with the encryption method.

ALGORITHM PRINCIPLE

The encryption algorithm proposed in this paper is closely related to the plaintext characteristics in the key selection process, and different plaintexts will generate different target keys. The algorithm first generates the chaotic sequence as the target key of the AES encryption algorithm through the neural network, and then performs the encryption of the three-cycle AES algorithm.

Four-Dimensional Hopfield Neural Network

The Hopfield neural network was first proposed by American physicist J.J. Hopfield in 1982. It is mainly used to simulate the biological neural network memory mechanism. Hopfield neural network is a fully connected neural network, for each neuron, its own output signal is fed back to itself through other neurons, so Hopfield neural network is a kind of feedback neural network. This paper cites the four-dimensional continuous Hopfield chaotic neural network model in [9]. The neural network consisting of four neurons is chosen. The maximum Lyapunov exponent of the model has reached 1.45, and two Lyapunov exponents are larger than 0 and are in a state of hyperchaos. This four-dimensional hopfield neural network is depicted by equations (1) and (2), where x is the state of the neuron, v is the transfer function, and W is the weight matrix.

$$x_i = -x_i + \sum_{j=1}^{4} w_{ij} v_i \tag{1}$$

$$v_i = \tanh(x_i) = \frac{e^{x_i} - e^{-x_i}}{e^{x_i} + e^{-x_i}}, i = 1,2,3,4 \tag{2}$$

Where W= (w_{ij}) is a 4×4 matrix, ie

$$\boldsymbol{w} = \begin{pmatrix} 1 & -6 & 4 & 1 \\ 980 & 3.5 & -1 & 0 \\ -1 & 4 & 1.5 & 1000 \\ 0 & 4 & -5 & 2 \end{pmatrix}$$

AES Encryption Algorithm

The triple AES algorithm adopted in this paper is a three-cycle encryption method. Each round of the AES algorithm is divided into four phases: (1) S-box transformation: the first four binary digits of each value are used as the row coordinates, and the last four are binary. Instead of querying the values in the S box for column coordinates, (2) Row shift operation: The nth row is shifted right by n bytes; (3) Column obfuscation operation: XOR operation is performed using a set of matrix and ciphertext The new column is replaced; (4) Round Key Addition: The ciphertext and the key are XORed.

Encryption and Decryption Principle

The size of an ordinary grayscale image is generally M×N. To facilitate the discussion of the algorithm, A is represented as a 256×256 grayscale image. If it is not a multiple of 8 pixels, 0-pixel values can be used to make the rows and columns into multiples of 8, Avg is the pixel average value, and the chaotic sequence only needs to obtain the corresponding size according to the image size. The encryption algorithm process is shown in Figure 3, and the steps are as follows:

Step 1: The plaintext image A is converted into a matrix p with a size of 256×256 in the order of row precedence, and the value range is [0,255].

Step 2: Add all the pixel values of the matrix p by 256×256 to get the pixel average value avg.

Step 3: Define the key as 4 random integers as the initial state of the four neurons of the Hopfield 4D neural network. A series of chaotic sequences are generated by the Hopfield four-dimensional neural network model. The chaotic sequence is composed of the four neurons recorded at each moment in time. We extract avg+256×2564+2563 chaotic data from the avg moment and perform the chaos. The data is rounded and divided by the 256-value obtained as the target key.

Step 4: Extract the avgth to the avg+256×256th target keys to generate a matrix and perform an XOR operation with the plaintext. Since the target key is 0-256, the number of bits in the binary digits does not exceed 8 bits, and the plaintext is performed. XOR bit processing does not exceed the 8-bit binary range.

Step 5: Perform the first part of the AES algorithm -S box transformation, extract the first avg+256×256th to the avg+256×256+256th AES loop number of times the target key is converted into a matrix of 1616, and the matrix is taken to be rounded The remaining numbers are numbered from 0 to 255 so that the number is the value of the original position of the target key of the segment as the S box, and the first 4 bits of each element value of the cipher text are taken as the number of rows of the S box. The last four digits are used as the number of columns of the S box, and this element value is replaced with the value of the corresponding position of the S box.

Step 6: Perform the second link of the AES algorithm - row shifting and scramble the cipher text matrix in the nth row to the right by n bits.

Step 7: Perform the third link of the AES algorithm - column obfuscation. Perform the sequential AND matrix with each of the four values of the ciphertext [02,03,01,01; 01,02,03,01; 01,01,02, 03;03,01,01,02] XOR operation according to row precedence respectively, for example (XOR of the first line [02,03,01,01] of the binary 10110101 and a value of the ciphertext), A value is XORed with the first line, the second value is XORed with the second line, the third value is XORed with the third line, the fourth value is XORed with the fourth line, and the ciphertext is Each of the four values performs an exclusive OR operation once in a loop.

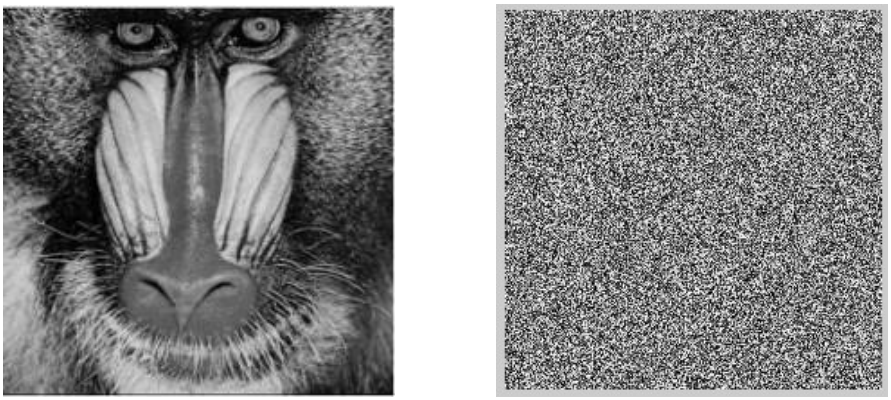
Step 8: Perform the fourth part of the AES algorithm - round key addition operation, extract the 256×256th target key of the first AES loop number from the first avg+256×256+256, round, take the absolute value and divide by 256 I, and XOR with ciphertext.

Step 9: Repeat Step 3 to Step 6 three times. The chaotic sequence of the S box and the round key is sequentially acquired according to the corresponding time, and the triple AES algorithm is performed to obtain the final ciphertext image C.

The decryption operation is the reverse of the encryption operation.

SIMULATION RESULTS

In order to facilitate the verification, the Lena grayscale image with a size of 256×256 is selected as the plaintext in the simulation process, but it is also suitable for image encryption of other size and size. As shown in Fig.1(a), the initial key is (1,1,1,1), and the plaintext parameter avg is rounded to 123. The experiment results in the encryption effect shown in Fig.1(b).



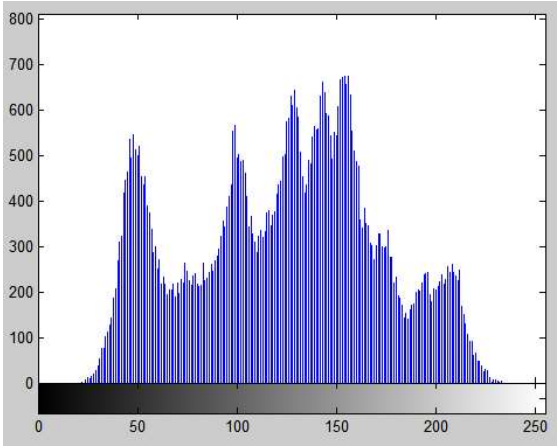
(a)Clear text images (b)Encrypt the image

FIGURE 1. Plain text images and encrypted images

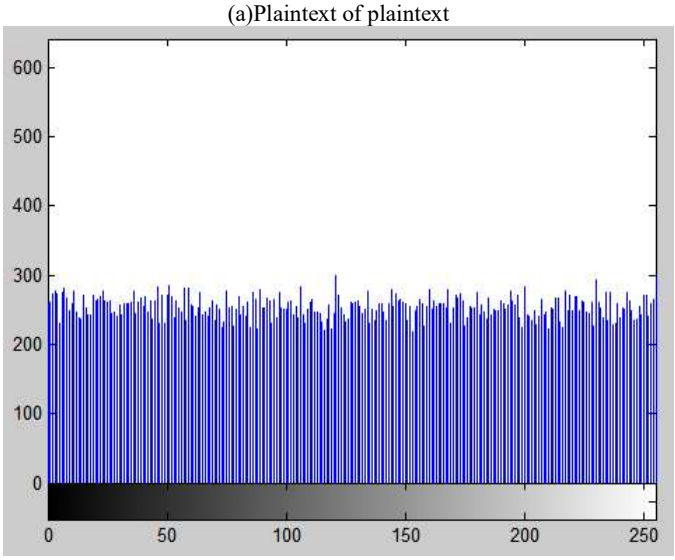
Histogram Analysis

The histogram of the degree image is the frequency at which each gray-scale pixel appears in the image, with the gray level as the abscissa, the ordinate as the gray-level frequency, and the plot of the plot frequency versus the gray level. The important feature is Reflects the gray distribution of the image. An ideal encrypted image should be a uniformly distributed histogram that prevents the cracker from extracting any meaningful information from the fluctuating ciphertext image histogram [21]. As seen from the grayscale histogram before and after encryption, as shown in Fig.2, the grayscale histogram of the plaintext image before encryption is not uniform, and the distribution

characteristics of the pixel values of the image are clearly exposed, and the grayscale of the encrypted ciphertext image is clearly exposed. The histogram is even and well concealing the distribution characteristics of the plaintext image.



(a)Plaintext of plaintext



(b)Ciphertext grayscale image histogram

FIGURE 2. Plaintext and ciphertext gray histogram

Algorithm Statistical Analysis

The adjacent pixel values are randomly selected for the horizontal, vertical, and diagonal directions of the image to calculate their respective correlation coefficients. Table 1 shows the correlation coefficients before and after encryption. It can be seen that the correlation of the adjacent pixels of the encrypted image is much smaller than that of the original plaintext image, indicating that this algorithm has a strong anti-statistical analysis capability.

TABLE 1. Before and after image encryption adjacent pixels correlation coefficient

Pixel Direction	Horizontal Direction	Vertical Direction	Diagonal Direction
The Original image	0.9808	0.9471	0.9284
Encrypt the Image	-0.0250	-0.0510	0.0028

CONCLUSION

Aiming at some problems existing in chaotic image encryption algorithms, a new image encryption algorithm is proposed in this paper. The algorithm mainly has the following two characteristics: First, using the plaintext parameter as the position of the chaotic sequence can be different with the plaintext image, effectively resisting the plaintext (ciphertext) image attack; secondly: the algorithm is introduced. The hyperchaotic sequence generated by the four-dimensional Hopfield neural network is used as the target key of the AES algorithm, which combines the advantages of the two algorithms, solves the shortcomings of the target key space of the AES encryption algorithm, and greatly enhances the difficulty of encryption. Experiments show that this algorithm not only has better encryption effect, but also has higher security.

ACKNOWLEDGMENTS

First of all, we want to thank Professor Wang. The teacher gave careful guidance in the selection of the thesis, the determination of the research plan and the specific implementation process. His rigorous attitude and systematic research ideas have given me a lifetime benefit. At the same time, I would also like to thank all the teachers who have given me great care and support during my studies as well as my classmates and friends who care about me.

REFERENCES

1. Chen Shu, Han Tailin. The status of image encryption algorithms [J]. China Science and Technology Information, 2012 (2): 78-78.
2. Zhang Xiaoqiang, Wang Mengmeng, Zhu Guiliang. Research progress of image encryption algorithm[J]. Computer Engineering and Science, 2012, 34(5):1-6.
3. ZHU Cong-xu, SUN Ke-hui. Cryptographic analysis of a class of hyperchaotic image encryption algorithms[J].Acta Physica Sinica,2012,61(12):1-11.
4. Xie Guobo, Jiang Xianyue. Double-chaotic image encryption algorithm based on two-dimensional discrete fractional Fourier transform[J]. Computer Engineering and Applications, 2017:1-9.
5. REN Xiaoxia, LIAO Xiaofeng, XIONG Yonghong. A new image encryption algorithm based on hyper-chaos feature of cellular neural network[J]. Computer Applications,2011,31(6):1528-1530+1535.
6. Lu Huibin, Wang Lijia.Color image chaos encryption algorithm based on Hopfield network[J]. Journal of Jilin University (Information Science Edition),2014,32(2):131-137.
7. Ding Qun, Lu Zheming, Sun Xiaojun. Image encryption based on neural network cryptography [J]. Chinese Journal of Electronics, 2004, 32(4): 677-679.
8. Liu Zhuhua, Zeng Gaorong, Xie Fangsen. Chaos Image Encryption Algorithm Based on Discrete Hopfield Network[J].Computer Engineering,2012,38(4):112-115.
9. Chen Pengfei, Chaos Modeling and Performance Analysis Based on Hopfield Neural Network[D]. Tianjin: Nankai University, 2010.