A Sequential Cipher Algorithm Based on Feedback Discrete Hopfield Neural Network and Logistic Chaotic Sequence

Shoulin Yin, Jie Liu, and Lin Teng
(Corresponding author: Jie Liu)

Software College, Shenyang Normal University
Shenyang, Liaoning 110034, China

(Received Dec. 22, 2018; Revised and Accepted June 24, 2019; First Online Feb. 26, 2020)

Abstract

The traditional Logistic chaotic sequence is easy to be reconstructed and when using it to encrypt data, it is easily to leak sensitive information. Therefore, an external key is introduced to encrypt the initial value and parameters of the Logistic equation. Then we conduct sensitive and diffusion process for feedback discrete Hopfield neural network based on the Logistic sequence sensitivity to the initial value. And by updating the control parameters, it produces good sequence key with random chaos iterative operation. The final algorithm analysis and simulation experiments show that the key of the algorithm has a good sensitivity, the generated random sequence has good randomness, which satisfies the requirement of cryptography. The pseudo-random sequences constructed by the algorithm are characterized by good randomness and complexity.

Keywords: Feedback Discrete Hopfield Neural Network; Logistic Chaotic Sequence; Sensitive and Diffusion Process

1 Introduction

With the rapid development of computer technology and multimedia technology, multimedia communication has gradually become an important way for people communicating with each other [2, 3, 9]. Information security has been an important issue that is closely related to our lives [7, 8, 17]. The most important way to protect information security is data encryption. The discrete Hopfield neural network was proposed by Liu [10], so the combination of chaos and neural networks for data encryption has been continuously developed. At present, the main research methods are as follows:

1) Using a known chaotic sequence to train the neural network model, so that the neural network can approximate the same chaotic sequence, then use the known chaotic sequence as the public key, and the trained neural network weight and threshold parameters are as the private key to implement data encryption;

2) Using the chaotic attraction of the discrete Hopfield network and the unidirectional mapping of the initial state and the attractor, the stable attractor of the discrete Hopfield network can be encrypted as a key.

The neural network mutual learning model and the chaotic system were mutually interfered, and a new composite stream cipher was proposed in reference [15]. A novel chaos-based hybrid encryption algorithm design for secure and effective image encryption was presented. To design the algorithm, the Zhongtang chaotic system had been selected because of its rich dynamic features and its dynamical analysis was performed. On the base of this system, a new chaos-based random number generator (RNG) was developed and usefulness of the designed RNG in an encryption process was shown over NIST 800-22 randomness tests in reference [21]. In reference [11], the Hermite orthogonal polynomial was introduced into the neural network excitation layer, and the "one-time-one-density" asynchronous encryption algorithm was realized. Pareek [12] proposed a chaotic encryption scheme by combining the chaotic attraction of Hopfield network with the linear feedback shift register. The most important thing to apply chaos and neural network to data encryption was that it used the chaotic characteristics of chaotic sequences. However, Zhang [19] also pointed out that there are defects in the sequence reconstruction of chaotic sequences in data encryption. Moreover, the reference [4] completely reconstructed the four-point and sixteen-point sequence fragments of the Logistic equation. Therefore, the simple chaotic sequence encryption method is the risk of being cracked. Aiming at this problem, this paper introduces an external key to encrypt the Logistic equation, and proposes a piecewise discrete Hopfield neural network model. Through a sensitive and diffusion process, the chaotic network model also has good sensitivity and good random generation sequence.

The rests of the paper are organized as follows. Section 2 introduces the Logistic mapping. Discrete Hopfield neural network Model is illustrated in Section 3. Section 4 and Section 5 outline the quantitative processing and new algorithm analysis. Section 6 finally concludes this paper.

2 Logistic Mapping

Logistic mapping [5,16,18,20] is a classic chaotic sequence mapping. Because of its simple implementation method, it is easy to be reconstructed by the thief using phase space to construct the form of chaotic equation. Therefore, in order to enhance the confidentiality of the Logistic mapping, this paper introduces an external key to encrypt the initial values and parameters of the Logistic map.

The 24-bit binary number K_1 is used as an external key to initialize the initial values and parameters of the Logistic map. Let K_1 be expressed in hexadecimal as $K1 = k_1k_2k_3k_4k_5k_6$, and "$k_1k_2k_3k_4k_5k_6$" is an external key. Where "$k_1k_2k_3$" is used to generate the input control parameter r of the Logistic mapping. "$k_4k_5k_6$" is used to generate the initial value X_0 of the Logistic mapping.

In this article, the Logistic mapping is as follows:

$$X_{n+1} = r \times X_n(1 - X_n), X_n \in (0, 1).$$

Where r is the input control parameter and X_0 is the initial value of the Logistic mapping. They are generated by an operation of an external key. During the operation, "$k_1k_2k_3k_4k_5k_6$" is converted into a corresponding decimal number for operation. Therefore, we can get,

$$\begin{aligned} r &= 4 + \frac{k_1/16^2 + k_2/16 + k_3}{16^2}. \\ X_0 &= \frac{k_4/16^2 + k_5/16 + k_6}{16^3}. \end{aligned} \quad (1)$$

3 Discrete Hopfield Neural Network Model

Assuming that each Neuron state is 0 or 1, the next state $S_i(t + 1)$ depends on current state $S_i(t)$. So

$$S_i(t + 1) = \sigma(\Sigma_{j=0}^{N-1} T_{i,j} S_i(t) + \theta_j), i = 0, 1, \cdots, N - 1,$$

where the threshold of neuron i is θ_j, and the connection weight between neuron j and i is $T_{i,j}$. $\sigma(x)$ is any nonlinear function, is set as the unit step function. Then the energy function of the system at time t is:

$$E(t) = 0.5 \sum_{i,j} T_{i,j} S_i(t) S_j(t).$$

Hopfield has proved that Equation (1) decreases monotonically with the evolution of system state, and eventually it will reach a stable state, namely chaos attractor. And there is an unpredictable relationship between the state messages contained in its attraction domain. If the join weight matrix T is changed, the attractor and its corresponding attraction domain will change too. After the introduction of random transformation matrix H, the initial state S and attractor S_μ will be updated by $\hat{S} = SH$ and $\hat{S}_\mu = S_\mu H$ and get new initial state S and attractor $\hat{S}_\mu$, and this process is unilateral, irreversible [14].

4 Quantitative Processing

In order to apply the random sequence generated by discrete Hopfield neural network into data encryption, this paper introduces the conversion function $T(x)$ to convert the generated random sequence into a $0 - 1$ random sequence. $T(x)$ is defined as follows:

$$T(x) = 0, x \in [2n/N, (2n + 1)/N].$$

Where N is an integer in interval $[10, +\infty]$, n is an integer in interval $[0, \tilde{N}]$, $\tilde{N} = \lfloor N/2 \rfloor$. Since the random value generated by the network is in the interval $(0, 1)$, this paper divides the interval $(0, 1)$ into N equal parts. The larger the N value is, the finer the interval division is and the data precision is higher.

4.1 Generating a $0 - 1$ Random Sequence

1) Input the key K_1 to initialize the Logistic mapping and iteratively calculate the Logistic mapping 200 times. Let $X = [x_{101}x_{102}x_{103}, \cdots, x_{199}x_{200}]$ be used to store the next 100 chaotic values.

2) Use X to initialize the weight, threshold of the diffusion matrix W and the discrete Hopfield neural network. W is a 4×4 matrix, W_1 is a 2×4 matrix, B_1 is a 2×1 matrix, W_2 is a 1×2 matrix, and B_2 is a 1×1 matrix.Extract elements from X to initialize W, W_1, B_1, W_2, and B_2, respectively.

3) Input the key K_2 and obtain $\tilde{D}_1$ through initial grouping and transformation.

4) Input $\tilde{D}_1$ to the discrete Hopfield neural network, and a random value D_3 is obtained through network operation; then the values of the control parameters Q_1 and Q_2 are continuously updated until a random sequence of the desired length is obtained.

5) The generated random sequence is converted to a corresponding binary random sequence by a quantization function $T(x)$.

5 New Algorithm Analysis

This paper analyzes the key space size of the new algorithm, the number of 0/1 statistics, the correlation of random sequences and the sensitivity of the key through theoretical analysis and experimental simulation, and draws

Table 1: Statistical analysis results

Testing parameter	Sequence 1	Sequence 2
n_0	128	130
n_1	129	127
r	129	131
y_1	5.37e^{-4}	5.98e^{-5}
y_2	1.3214	-6.7892
y_3	-0.1179	0.1225

corresponding conclusions. The simulation experiment data is as follows: $n_0 = 120$, $n_1 = 8$, $n_2 = 10$, $\alpha = 2$, $N = 128$, $Q_1 = [0.5, 0.5]^T$, $Q_2 = 0.5$.

5.1 Key Space Analysis

In this paper, the encryption key consists of K_1 and K_2, and the key space is determined by the length of K_1 and K_2. Let their lengths be L_1 and L_2, respectively. The key space is $2^{(L_1+L_2)}$. The larger $L_1 + L_2$ is, the larger the key space is. In this paper, $L_1 = 24$, $L_2 = 16$, and the key space size is 2^{40}. Obviously, the length of L_2 is variable. Increasing the length of L_2 can increase the size of the key space. However, when the length of the key L_2 is increased, the number of inputs of the discrete Hopfield neural network will also increase. The number of corresponding discrete Hopfield neural network layers will increase too, the time overhead of the network iterative operation will increase. When the generated random sequence is very large, the time overhead of running the entire network will be very large too.

5.2 Statistical Analysis

A valid binary random sequence must satisfy the 0/1 ratio. Therefore, the purpose of this test is to determine if the ratio of 0/1 in the sequence is approximately equal to the ratio of 0/1 in the true random sequence. At the same time, this paper refers to the method of [13] for the frequency test, sequence test and run test of the generated random sequence. Therefore, two random sequences of length 256 are randomly selected for statistical analysis. The analysis results are shown in Table 1.

In Table 3, n_0 denotes a number of 0, n_1 is number of 1, r is total number of run test, y_1 is frequency test value, y_2 is sequence test value, y_3 is run test value.

It can be seen from Table 1 that the number of "0" and "1" in sequence 1 and sequence 2 are nearly equal, satisfying the requirements of random sequence. At the same time, the frequency test value y_1 is less than 3.84, which can pass the frequency test. The sequence test value y_2 is less than 5.99, which can pass the sequence test. The run test value y_3 is much less than 1.96, which can pass the run test. Therefore, the generated random sequence has good randomness.

Table 2: Statistical analysis result of LET

Testing parameter	Sequence 1	Sequence 2
n_0	127	126
n_1	129	132
r	130	128
y_1	6.18e^{-5}	2.51e^{-4}
y_2	-0.972	-0.864
y_3	0.259	-0.397

Table 3: Statistical analysis result of RBC

Testing parameter	Sequence 1	Sequence 2
n_0	135	140
n_1	121	116
r	140	135
y_1	5.34e^{-3}	1.23e^{-2}
y_2	1.467	2.132
y_3	1.792	1.235

In order to further verify the randomness of the generated sequences, the above two randomly selected random sequences are compared with the statistical analysis results in the reference LET [6] and RBC [1]. The statistical analysis results of the LET and RBC are shown in Table 2.

From Table 2, it can be seen that the difference between "0" and "1" in the random sequence generated by new algorithm is smaller than the difference between "0" and "1" in the literature [13]. Therefore, the 0/1 sequence generated in this paper is more random. At the same time, the frequency test value y_1, the sequence test value y_2 and the run test value y_3 are all smaller than the corresponding values in [6]. Therefore, the 0/1 sequence cant better pass the frequency test, sequence test and run test. Compared with the literature [6], the difference between "0" and "1" in the random sequence in this paper is close to the difference between "0" and "1" in the literature [6]. And, the frequency test value y_1 and the run test value y_3 in this paper are smaller than the corresponding values in the literature [6] in some cases, which indicates that the 0/1 sequence can better pass the frequency test and the run test in some cases. However, the sequence test value y_2 in this paper is larger than the corresponding value in [6], which indicates that the 0/1 sequence generated in [6] can pass the sequence test better. In general, the proposed algorithm outperforms the literature in frequency test, sequence test and run test [1], and in some cases is superior to the literature [6].

5.3 Correlation Analysis

The change in the autocorrelation function of the sequence is smaller, the better the randomness of the sequence is. The cross-correlation function of the sequence is close to zero, the more unrelated the two sequences are. Figure 1 is the autocorrelation function of the 0/1 sequence generated when the initial keys are K_1 and K_2. Figure 2 is a comparison of the 0/1 sequence generated when the key K_1 or K_2 is randomly changed by one bit. The solid line represents the original sequence and the dotted line represents the new sequence. Figure 3 is a cross-correlation function diagram of two sequences.

5.4 Key Sensitivity Analysis

The chaotic sequence generated by the Logistic map has good sensitivity to the initial value. Since the key K_1 is used to generate the initial value of the Logistic equation, K_1 also has good sensitivity. At the same time, this paper uses Logistic map to sensitive and diffuse the key K_2, which makes K_2 also have good sensitivity. In order to verify the sensitivities of the keys K_1 and K_2, one of the keys is changed, and the percentage of the difference between the new random sequence and the original random sequence is counted. Let i denote the position number corresponding to each of K_1 and K_2, then $1 \leq i \leq \vartheta$, ϑ is the sum of the lengths of the keys K_1 and K_2. In this paper, $\vartheta = 40$. NP represents the percentage of the new random sequence and the original random sequence as the percentage of the total number of sequences. The formula of NP is:

$$\begin{aligned} NP(i) &= (\sum_{n=1}^{NK}(A(n)))/(NK) \times 100\%. \\ A(n) &= \begin{cases} 0 & D(n) = D'(n) \\ 1 & D(n) \neq D'(n). \end{cases} \end{aligned}$$

Where $D(n)$ and $D'(n)$ represent the original random sequence and the new random sequence, respectively. NK represents the total number of bits of the sequence $D(n)$. $NP(i)$ represents the percentage corresponding to the change of the $i-th$ bit.

Depending on the strict avalanche criterion in the block cipher measure, changing any bit in the key should result in a change of approximately 50% of the bits in the ciphertext. Figure 4 shows the percentage statistics obtained for the key length $\vartheta = 40$ and the sequence length $NK = 20000$.

It can be seen that the percentage of the sequence generated when the key changes by one bit is close to 50%, which satisfies the strict avalanche criterion.Therefore, both keys K1 and K2 are sensitive.

In summary, the 0/1 sequence generated by the algorithm has good randomness and the key has strong sensitivity.In addition, this paper uses a 24-bit external key to generate chaotic initial values and control parameters. Compared with the literature [16] directly using chaotic initial values and control parameters as keys, the key of this paper is more convenient to manage. At the same time, it solves the problem that the Logistic sequence proposed in [15] is easy to be reconstructed, which makes the security of the key better.

5.5 Anti-Matrix Analysis and Difference Analysis

If using a public key encryption system, from the orthogonal decomposition, the singular value decomposition and triangular decomposition, they demonstrate that the HNN network's safety is reliable. Because the entire password system is irregular in the process of encryption, even if the same clear sequence encrypted, the obtained ciphertext sequence cannot be the same. Moreover, in the decryption process using the attracting method, the differential cryptanalysis for the algorithm is invalid.

6 Conclusion

In this paper, we propose a sequential cipher algorithm based on feedback discrete Hopfield neural network and logistic chaotic sequence. The key is processed with sensitive and diffused to enhance its sensitivity. After experiment demonstration, the new algorithm has reliable security and high efficiency than other methods.

Acknowledgments

This work is supported by Science & Technology Planning Project of Gansu Province under Grant No. 1610RJZE135.

References

[1] S. A. K. Albermany, F. R. Hamade, G. A. Safdar, "New random block cipher algorithm," in *International Conference on Current Research in Computer Science & Information Technology*, 2017. DOI: 10.1109/CRCSIT.2017.7965555.

[2] J. Gao, P. Li, Z. Chen, "A canonical polyadic deep convolutional computation model for big data feature learning in Internet of Things," *Future Generation Computer Systems*, vol. 99, pp. 508-516, Oct. 2019.

[3] J. Gao, J. Li and Y. Li, "Approximate event detection over multi-modal sensing data," *Journal of Combinatorial Optimization*, vol. 32, pp. 1002-1016, 2016.

[4] J. S. Gao, B. Y. Sun, W. Han, "Construction of the control orbit function based on the chaos theory," *Electric Machines & Control*, 2002-02, 2002.

[5] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves," *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73-84, Mar. 2004.

[6] R. Karmakar, S. Chatopadhyay, R. Kapur, "Encrypt flip-flop: A novel logic encryption technique for sequential circuits," *Computer Science*, 2018. (https://arxiv.org/pdf/1801.04961.pdf)

[7] S. Khatoon, T. Thakur, B. Singh, "A provable secure and escrow-able authenticated group key agreement

protocol without NAXOS trick," *International Journal of Computer Applications*, vol. 171, no. 3, pp. 1-8, 2017.

[8] M. Liu and F. Long, "Stream cipher algorithm based on piecewise linear chaotic networks," *Computer Applications and Software*, vol. 33, no. 9, pp. 306-309, 2016.

[9] J. Liu, S. L. Yin, H. Li and L. Teng, "A density-based clustering method for k-anonymity privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 8, no. 1, pp. 12-18, Jan. 2017.

[10] Z. Liu, L. Zhang, L. V. Xue, *et al.*, "Evaluation method about bus scheduling based on discrete hopfield neural network," *Journal of Transportation Systems Engineering & Information Technology*, vol. 11, no. 2, pp. 77-83, 2011.

[11] Q. Meng, S. Yu, H. Liu, *et al.*, "A novel blind detection algorithm based on improved compound sine chaotic neural networks," in *IEEE International Conference on Communication Technology*, 2016. DOI: 10.1109/ICCT.2015.7399973.

[12] N. K. Pareek, "Design and analysis of a novel digital image encryption scheme," *International Journal of Network Security & Its Applications*, vol. 4, no. 2, 2012.

[13] L. Teng, H. Li, J. Liu and S. Yin, "An efficient and secure cipher-text retrieval scheme based on mixed homomorphic encryption and multi-attribute sorting method," *International Journal of Network Security*, vol. 20, no. 5, pp. 872-878, 2018.

[14] L. Teng, H. Li, S. Yin, "A multi-keyword search algorithm based on polynomial function and safety inner-product method in secure cloud environment," *International Journal of Network Security*, vol. 8, no. 2, 2017.

[15] C. Tie-Ming, J. Rong-Rong, "New hybrid stream cipher based on chaos and neural networks," *Acta Physica Sinica*, vol. 62, no. 4, pp. 191-201, 2013.

[16] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem," *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61-71, Mar. 2004.

[17] S. L. Yin and J. Liu, "A k-means approach for mapreduce model and social network privacy protection," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 7, no. 6, pp. 1215-1221, Nov. 2016.

[18] S. Yin, L. Teng, J. Liu, "Distributed searchable asymmetric encryption," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 4, no. 3, pp. 684-694, 2016.

[19] X. Zhang, F. Han, Y. Niu, "Chaotic image encryption algorithm based on bit permutation and dynamic DNA encoding," *Computational Intelligence and Neuroscience*, vol. 2017, pp. 11, 2017. (`https://doi.org/10.1155/2017/6919675`)

[20] Q. Zhang, L. T. Yang, X. Liu, Z. Chen, and P. Li, "A tucker deep computation model for mobile multimedia feature learning," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 13, no. 3, pp. 1-39:18, 2017.

[21] U. Cavu?o?lu, S. Kacar, A. Zengin, I. Pehlivan, "A novel hybrid encryption algorithm based on chaos and S-AES algorithm," *Nonlinear Dynamics*, vol. 92, no. 4, pp. 1745-1759, 2018.

Biography

Shoulin Yin received the B.Eng. and M.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016 and 2013 respectively. Now, he is a doctor in Harbin Institute of Technology. His research interests include Multimedia Security, Network Security, Filter Algorithm, image processing and Data Mining. Email:352720214@qq.com.

Jie Liu is a full professor in Software College, Shenyang Normal University. He received his B.S. and M.S. degrees from Harbin Institute of Technology. He is also a master's supervisor. He has research interests in wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Professor Liu had published more than 30 international journal papers (SCI or EI journals) on the above research fields. Email:ljnan127@163.com.

Lin Teng received the B.Eng. degree from Shenyang Normal University, Shenyang , Liaoning province, China in 2016. Now, she is a laboratory assistant in Software College, Shenyang Normal University. Her research interests include Multimedia Security, Network Security, Filter Algorithm and Data Mining. Email:910675024@qq.com.