Stream Cipher Method Based on Neural Network

Haiyan Long
City College
Dongguan University of Technology
Dongguan, China
Long_haiyan@126.com

***Abstract*—A new stream cipher algorithm based on one-way function of neural network is proposed. The nonlinear system comprised of such neural network is used to transform a group of LFSRs for key stream generation. As a result, the complexity of sequences is increased with period expanding. The produced cipher sequence has high randomness and has passed the standard tests of SP800-22. The experimental results show that the proposed encryption method is safe and has a higher performance of encryption and decryption speed by parallel computation structure. It can meet the need of stream cipher technology. The work has some values for deeper research on its theory and hardware application on secret communication. It is expected to attract more researchers in this field.**

Keywords- neural network; stream cipher; LFSR

I. INTRODUCTION

Hastad et al. [1] pointed out that a necessary and sufficient condition for the existence of pseudo-random generators is the existence of one way function, which are easy to compute but hard to invert. Chaotic system is characterized by sensitive dependence on initial conditions, pseudo-randomness and ergodicity. In addition, it has a good feature of confusion and diffusion. So pseudo-random sequence is with good randomness, non-relevance and complexity provided by chaotic system is quite suitable for protecting information security [2-5]. Although one-dimensional chaotic maps are advantageous considering the high-level efficiency and simplicity aspects, but most existing chaotic cryptosystems still suffer from fundamental draw-backs such as small key space, slow performance speed and weak security function[6,7]. To solves the problem of short cycle and low precision of one-dimensional chaotic function, many researchers have used higher-dimensional chaotic systems, coupled chaotic map to enhance the cryptosystem security [8-10] at a cost of speed.

Cryptography employing neural network especially discrete Hopfield Neural Network (HNN) becomes a new research field recently because its nonlinearity is very fit to the requirement of complex computing in cryptography [11-13].The chaotic dynamics of recurrent HNN is regarded as the extremely complex and unpredictable nonlinearity that can be used to generate unpredictable stream [14, 15]. Moreover, discrete HNN is a kind of network that can be carried out by high speed parallel calculation networks and suits for parallel hardware in real-time applications [16]. As a combination of neural networks and chaos, chaotic neural networks (CNN) are expected to be more suitable for data encryption. A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks is proposed in [12]. In [17] it showed that some weak keys exist in the scheme from [12]. The cipher is vulnerable to cipher text-only and chosen-cipher text attack. Due to three problems found in Guo et al.'s scheme, Leung et al. proposed a modified cryptographic scheme based on Clipped HNN [13]. Their scheme solves the problems in the original scheme [12]. However, the memory size is huge when the network size is reasonably large because the coding matrix in the scheme [13] is the same as that in [12]. The mathematical proof whether the counter value is unique is difficult, not to mention an adequate solution. Thus, we propose a new fast scheme which uses one-way function of HNN without coding matrix and data expansion.

The rest of the paper is organized as follows. Section 2 gives a description of cryptographic scheme. The security and performance are analyzed in Section 3 and the conclusion is given in the last section.

II. STREAM CIPHER ALGORITHM FROM ONE-WAY FUNCTION

A. Hopfield Neural Network Model

Assume a fully interconnected synchronous neural network of *N* neurons labeled from 0 to *N*-1. The state of a neuron *i* at the time *t* is denoted $S_i(t)$, which is either 0 or 1. The next state of neuron *i* , i.e. $S_i(t+1)$ depends on the current states of all neurons as follows:

$$S_i(t+1) = \sigma(\sum_{j=0}^{N-1} T_{ij} S_j(t) + \theta_i), i = 0,1,\cdots, N-1 \quad (1)$$

Where T_{ij} is the synaptic strength between neurons *i* and *j*, θ_i is the threshold value of the neuron *i*; $\sigma(x)$ is any non-linear function, can be realized by a sign function:

$$\sigma(x) = \begin{cases} 1, x \geq 0 \\ 0, x < 0 \end{cases} \quad (2)$$

The HNN can be a neural network with zero neuron threshold and a symmetric matrix T_{ij}. Hopfield proved that the energy function of such network is monotonically decreasing during state evolution [18]. Therefore, any initial state of the network will converge to a stable state, i.e., chaotic attractor. The relationship between message states in the domain for each attractor are unpredictable. If the neural synaptic matrix *T* is changed, these attractors and their attraction domain will be also altered. After a random permutation matrix *H* is selected, the original initial state S and corresponding attractor S_μ turns into new initial state $\hat{S}$ and attractor $\hat{S}_\mu$, which can be calculated by $\hat{S} = HS$ and $\hat{S}_\mu = HS_\mu$ [12].

B. *Convergent Property of HNN*

Chan first presented a modified HNN named clipped HNN [19]. Under some conditions, the clipped HNN is capable of storing a set of desired patterns as stable points of the network. In the parallel updating mode, the network will always converge to these 2*n* stable points for most of the state vectors. These stable points can be further divided into two groups, group α and β, each with *n* stable points. It is shown that the attraction basins of the stable points in group α and β are uniformly distributed.

C. *Proposed Stream Cipher Algorithm*

There exists a One-way function in the HNN. When neural synaptic matrix T is an $n \times n$ singular matrix, the singular matrix $\hat{T} = H * T * H'$ can be easily obtained under the condition that H is an $n \times n$ random diagonalizable matrix and kept secretly. But it is hard to obtain the secret key H directly, especially for a sufficiently large number of *n* [4].

Based on the nonlinear dynamics and the convergence properties of the HNN, a new design of key stream generator is proposed, which is able to produce sequences with large period and linear complexity. In Fig.1, several m-sequences are chosen as the driven source of the sequence generator, and discrete HNN as the nonlinear function to select the output.

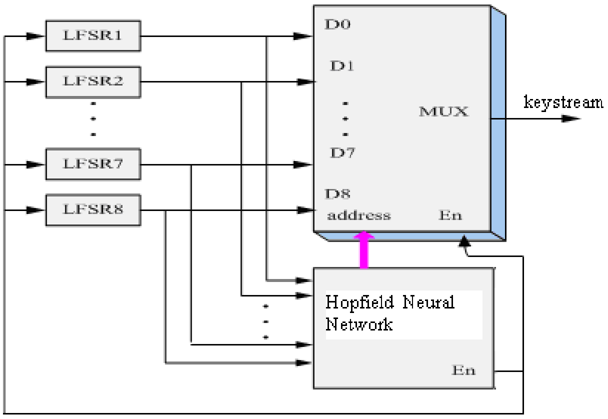

Fig. 1 Keystream sequence generator (n=8)

In the parallel updating mode, the network will always converge to two attractor groups for most of the state vectors, each with *n* attractors [19]. Because *n* attractors are evenly distributed in both groups, we can randomly map D_i to LFSR$_i$ for each group. Therefore, the fine statistics property of m-sequence is reserved, and its complexity and period are also improved in this way.

Based on the above analysis, the operation of the nonlinear filter generator can be summarized as follows:

STEP1: Both sides of the communication should randomly select the same $n \times n$ diagonalizable matrix H and the same initial values of LFSRs, which must be set secret keys.

STEP2: At each time unit, the states of m-LFSRs are input the network for iteration. Due to the convergence property of the HNN, the input probe will eventually converge to one of the attractors of the network.

STEP3: The generated attractors can be divided into two groups. In one group, the number of '0' and '1' is equal; whereas, the number of '1' is more than '0' in another group. Since the numbers of attractors in both groups are equal to *n* and every attractor happens in the same possibility, the attractors in both groups can be ordered from 1 to *n* according to their appeared sequence. As is shown in Fig.1, the attractors generated from HNN are used as address signal of the multiplexer to select one of the *n* LFSRs to connect to output. To avoid the coding matrix, we consecutively encode LFSRi, rather than use Table 1 in [13] for encoding the input stream.

The key stream obtained from the above procedure is used to exclusive-or (XOR) text message for encryption. On the other hand, decryption can be done by XORing the ciphered text with key stream. This scheme can generate stream ciphers in a simple way, which is easy to be implemented by hardware and leads to high-speed encryption and decryption.

III. Security Analysis

A. *Proof of One-way Property*

For a nonsingular matrix A, there exists one and only one inverse A^{-1}. Therefore, $x = A^{-1}b$ is the unique solution of the linear equation $Ax = b$. Usually, A is a singular or rectangular matrix, so the linear equation has no solution, or multiple solutions. However, with the theorem of generalized inverse matrix, $x = Gb$ is denoted as one of solutions of the linear equation $Ax = b$. For every finite matrix A (square or rectangular) of real or complex elements, there exists a unique matrix X satisfying the Penrose equations:

$$AXA = A \tag{3}$$

$$XAX = A \tag{4}$$

$$(AX)^* = AX \tag{5}$$

$$(XA)^* = XA \tag{6}$$

where A^* denotes the conjugate transpose of A. The unique solution is commonly called Moore-Penrose inverses, denoted by A^+. The generalized inverse matrices are still uncertain for one or several formulas. Let $C^{m\times n}$ denotes the class of $m \times n$ complex matrices, definition is given as follows:

Definition: For any $A \in C^{m \times n}$, let $A(i, j, \cdots, k)$ denote the set of matrices $X \in C^{m \times n}$ which satisfy equations $(i), (j), \cdots, (k)$ from (1)–(4). A matrix $X \in A(i, j, \cdots, k)$ is called an $(i, j, \cdots, k)$ –inverse of **A**, denoted by $A(i, j, \cdots, k)$.

So a matrix X satisfying (1) is called the equation solving generalized inverse for $AXA = A$ or $\{1\}$ inverse of A, and is denoted by $X = A(1)$ or $X \in A\{1\}$, where $A\{1\}$ denotes the set of all $\{1\}$ inverses of A. $\{1\}$-inverse is one of the most basic and important generalized inverses. One of its significant applications is about expressing the solutions when solving the matrix equations and linear equations, and plays a similar role as the common inverse.

Theorem: For $A \in C^{m \times n}$, $B \in C^{p \times q}$, if and only if there exist $A^{(1)}$ and $B^{(1)}$ satisfying equation $X = B'A'B^{(1)} + Y(I - BB^{(1)})$ where Y is any $n \times p$ matrix, then solutions of $B = XAX'$ are consistent.

Proof: If A is a singular matrix, and X satisfy (1), then $B = XAX'$ can be transformed to

$$AB = AXAX' = AX' \tag{7}$$

Make a transposition simultaneously on both sides

$$X'A = B'A', \tag{8}$$

Rewrite (8) into a common form:

$$AXB = D, \tag{9}$$

Where $A \in C^{m \times n}$, $B \in C^{p \times q}$, $D \in C^{m \times q}$, if and only if there exists some $A^{(1)}$ and $B^{(1)}$ satisfying

$$AA^{(1)}DB^{(1)}B = D \tag{10}$$

Equation (9) is consistent [19] and for arbitrary $Y \in C^{p \times q}$, its general solution is given by

$$X = A^{(1)}DB^{(1)} + Y - A^{(1)}AYBB^{(1)}. \tag{11}$$

Let $A = I, D = B'A'$. According to (11), for arbitrary $Y \in C^{p \times q}$, the general solution of (8) is

$$X = B'A'B^{(1)} + Y(I - BB^{(1)}). \tag{12}$$

Since equation $B = XAX'$ has infinite solutions, which is corresponding to $\hat{T} = H * T_0 * H'$ in stream cipher algorithm. Therefore, it is easy to calculate $\hat{T}$ by T_0 and H, but it is nearly impossible to get H by $\hat{T}$. So we can make a conclusion that the transformation function of neural synaptic matrix is a trapdoor one-way function.

B. *Complexity Analysis*

HNN with $N = 8$ is used for analysis. Assuming that cipher circuit contains eight LFSR, chaotic sequence generator and data MUX, the order of the LFSR is denoted by $D_i(1,2,\cdots,8)$, which are different from each other. The output of LFSR is $d_i(1,2,\cdots,8)$; $a_0a_1a_2$ is the output of chaotic sequence generator. Then the output of MUX is given by:

$$\begin{aligned} C = {} & d_1\overline{a_2}\,\overline{a_1}\,\overline{a_0} + d_2\overline{a_2}\,\overline{a_1}a_0 + d_3\overline{a_2}a_1\overline{a_0} + d_4\overline{a_2}a_1a_0 \\ & + d_5a_2\overline{a_1}\,\overline{a_0} + d_6a_2\overline{a_1}a_0 + d_7a_2a_1\overline{a_0} + d_8a_2a_1a_0 \end{aligned} \tag{13}$$

According to the complexity principles, the linear complexity, L, is given by:

$$L = A^n \sum_{i=1}^{2^n} D_i \tag{14}$$

where A and $D_i(1,2,\cdots,8)$ are the complexity of every chaotic sequence output and each LFSR respectively; the number of LFSRs are 2^n. It can be seen that the complexity of the circuit is dominated by the number of LFSR, and shows an exponential relation with *n*.

C. *Random Test*

In this paper, the randomness test for secret-key sequences generated by the proposed algorithm is carried out according to SP800-22 set by the National Institute of Standards and Technology (NIST) [20]. SP800 contains 100 groups of test samples, each group having 106 data in our experiment data. Test results in Table 1 show that the random-bit sequences generated by the algorithm are quite stochastic.

TABLE 1. CORRELATION TEST USING SP800-22

Test	Pass %	Results
Frequency	1.0000	Successful
Block Frequency	0.9505	Successful
Cumulative Sums	0.9134	Successful
Runs	0.1364	Successful
Longest Run	0.7948	Successful
Rank	0.9772	Successful
FFT	0.9458	Successful
Non Overlapping Template	0.9917	Successful
Overlapping Template	0.3753	Successful
Universal	0.3508	Successful
Approximate Entropy	0.0392	Successful
Random Excursions	0.9123	Successful
Random Excursions Variant	0.9037	Successful
Serial	0.9736	Successful
Linear Complexity	0.2163	Successful

D. Correlation Test

Chosen 2k repeated plaintext for encoding, the self-correlation function of the cipher text sequence is shown in Fig.2, which presents as a function of δ without any repeated periods. The self-correlation is virtually impulse like. This figure clearly indicates that the cipher text will not respond to the repeated plaintext. When any element in the permutation matrix *H* is altered, the cross-correlation function of the former and the latter cipher text is shown in Fig.3. It shows that any slight alterations in secret-key can make the cipher text completely change, which meets the Avalanche Effect.

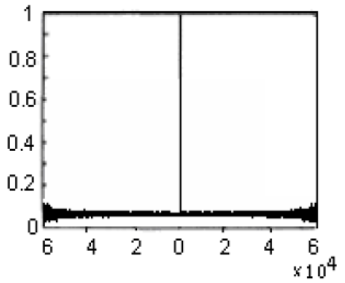

Fig.2.Secret-key sequence self-correlation function

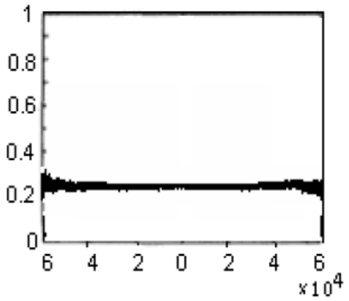

Fig.3. Cipher text cross-correlation function

E. Analysis of Speed and Information Rate

In practical program, we adopt the LFSRs with *n*=16 as input, and D_i =11, 13, 17, 19, 21, 25, 29, 31, 37, 39, 41, 43, 47, 53, 59, 61 for *i*=1, 2… 16. Primitive plynomials are listed as following: (11,2,0), (13, 4,3,1,0), (17,6,0), (19,5,2,1,0), (21,2,0), (25,3,0), (29,2,0), (31,13,0), (37,6,4,1,0), (39,4,0), (41,3,0), (43,6,4,3,0), (47,5,0), (53,6,2,1,0), (59,7,4,2,0), (61,5,2,1,0) .

The algorithm proposed in [12] is improved by symmetrical encryption algorithm which avoids the exhaustive search and data expansion. If we use the algorithm in [13] to encrypt 4-bit information, the chaotic attractors should compute 9 times on average. However, encrypting 1-bit information only needs once for our algorithm. Test shows that the average speed is over 7 times faster than that of [13]. With such a speed, the proposed encryption scheme is suitable for internet applications over broadband networks, where the encryption and decryption time should be short relative to the transmission time.

IV. Conclusion

A new scheme is proposed to generate pseudorandom number from one-way function of neural networks that provides high security and high speed. The new scheme has no exhaustive search, thus improves the efficiency of producing pseudorandom numbers. Moreover, our scheme keeps no data expansion so that it is suitable for large file transfer.

References

[1] J. Hastad, R. Impagliazzo, L. Levin and M. Luby, “Pseudo-random generator from one-way functions," SIAM J. Comput., vol. 28, no. 4, pp.1364-1396, 2010.

[2] R. Matthew, "One the derivation of a chaotic encryption algorithm", Cryptologia, vol. 8, pp. 29-42, 2011.

[3] Y. Wang, X. Liao, D Xiao and K. W. Wong, "One-way hash function construction based on coupled map lattices," Information Sciences, vol. 178, pp.1391-1406, 2010.

[4] N. K. Pareek, V. Patidar and K. K. Sud, "Cryptography using multiple one- dimensional chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 10, pp. 715-723, 2011.

[5] N. K. Pareek, V. Patidar and K. K. Sud, "Image encryption using chaotic logistic map,” Image and Vision Computing, vol. 24, pp.926-934, 2011.

[6] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," Chaos, Solitons & Fractals, vol. 42, issue 3, pp. 1745-1754, 2009.

[7] G. Alvarez, F. Montoya, M. Romera and G. Pastor. "Cryptanalysis of a discrete chaotic cryptosystem using external key," Phys Lett. A, vol. 319, issues 3-4, pp. 334-339, 2003.

[8] A. N. Pisarchik and M. Zanin, "Image encryption with chaotically coupled chaotic maps," Physica D: Nonlinear Phenomena, vol. 237, pp. 2638-2648, 2008.

[9] Y. Wang, K. W. Wong, X. Liao, T. Xiang and G.Chen, "A chaos-based image encryption algorithm with variable control parameters," Chaos, Solitons& Fractals, vol. 4, pp. 1773-1783, 2010.

[10] X. Tong and M. Cui, "Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator," Signal Processing, vol. 89, pp. 480-491, 2011.

[11] M. Arvandi, S. Wu and A. Sadeghian, "On the use of recurrent neural networks to design symmetric ciphers," IEEE Comput. Intell. Mag, vol. 3, no. 2, pp. 42-53, 2010.

[12] D. Guo, L. M. Cheng and L. L. Cheng, "A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks," Applied Intelligence, vol 10, no. 1, pp. 71-84, 2008.

[13] K. C. Leung, S. L. Li, L. M. Cheng and C. K. Chan. "A symmetric probabilistic encryption scheme based on CHNN without data expansion," Neural Processing Letters, vol. 24, no. 2, pp. 93-105, 2009.

[14] L. Chen and K. Aihara, "Chaotic Simulated Annealing by Network Model with Transient Chaos". Neural Networks, 2007, 8(6), pp. 915-930.

[15] D. Karras and V. Zorkadis, "On neural network techniques in the secure management of communication systems through improving and quality assessing pseudorandom stream generators," Neural Networks, vol. 16, no. 5, pp. 899–905, 2006.

[16] D. H. Guo, X. J. He and C. S. Chen, "ASIC design of chaotic encryption based on neural networks," Chinese J. of Computers, vol. 23, no. 11, pp.1230-1232, 2007.

[17] L. Chen and K. Aihara, "Strange attractor in chaotic neural networks," IEEE Tran. on Circuits and System, vol. 47, no. 2, pp. 1455-1468, 2007.

[18] J. J. Hopfield, “Neurons, dynamics and computation," Physics Today, vol. 47, no. 2, pp. 40-46, 1994.

[19] C. K. Chan and L. M. Cheng, "The convergence properties of a clipped Hopfield network and its application in the design of keystream generator," IEEE Trans. on Neural Networks, vol. 12, no. 2, pp. 340-348, 2001.

[20] http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf