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.

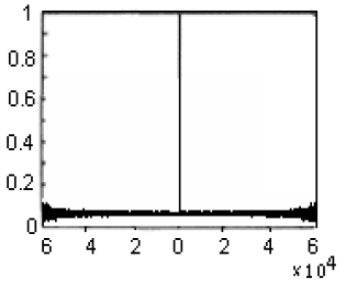

Fig.2.Secret-key sequence self-correlation function

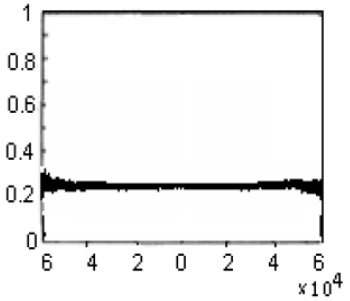

Fig.3. Cipher text cross-correlation function

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