ENCRYPTION OF MPEG-2 VIDEO SIGNAL BASED ON CHAOTIC NEURAL NETWORK

Tariq A. Fadil[1], Shahrul N. Yaakob[2], Badlishah Ahmad[3], Abid Yahya[4]

[1,2,3,4]School of Computer & Communication Engineering, UniMAP, Perlis, Malaysia

Email: [1,2,3,4]eng_tariq_adnan@yahoo.com

ABSTRACT

In this paper, a cipher system based on chaotic neural network (CNN) is used to encrypt and construct a stream cipher of compressed MPEG-2 video signal. The symmetric cipher algorithm transforms the plaintext (compressed video data) into the unintelligible form under the control of key; this algorithm has high security and simple architecture with low cost hardware. However, if the size of neural network is increased, the required execution time for CNN encryption and decryption process will be decreased. The whole system model can keep the original file and provide good video quality and reduce the required bit rate which is very suitable to limited bandwidth channel. The proposed system - is also suitable for secure video transmission applications and wireless multimedia communication.

KEYWORDS*: Chaos, Neural Network, Video Compression, Video Encryption.*

1.0 INTRODUCTION

Transmission of Modern multimedia communication technology such as image, audio and video becomes more widely used in our daily life. Compression of digital video signal becomes very important in video transmission applications because the amount of data associated especially for video signal is very huge to be handled by a limited bandwidth channel, in addition to compression providing a secure level of the transmitted data against unauthorized people also is important especially in applications that required a high level of protection such as medical, military, and entertainment applications. Cryptography is the study of information security and the feasibility of communication over an insecure channel while preserving the secrecy of the information transmitted [1], [2]. Due to some intrinsic features of images, such as bulk data capacity

and high correlation among pixels, traditional encryption algorithms are not suitable for practical image encryption [3]. Neural network can be used to design data protection schemes because of its complicated and time-varying structures [4]. Due to the desirable properties of mixing neural and the sensitively to initial value conditions and parameters of chaotic maps, a chaos –based neural encryption produced a combination called a chaotic neural network (CNN) which is given a new and efficient way for data encryption [3], [5].

A number of research works have sought a link between chaotic neural networks (CNN) and increased security in cryptosystems. Author in work [6] has proposed to use unpredictable outputs of CNN together with dedicated hardware to encrypt digital signals. The randomness of the output of the system, built using a specific VLSI architecture, determines whether the encrypted data is predictable or not. Xiao and Liao have reported a combined hash and encryption scheme by CNN where the weights of the neural network are distributed with random chaotic sequences [7]. Bose has proposed a public key encryption using multiple chaotic systems and a set of linear functions for key exchange over an insecure channel [8]. Lian has proposed a block cipher based on neural network, the chaotic neural layer realizes data diffusion also he uses a linear neuron layer for realizing data confusion [9]. This paper presents an algorithm coupled with chaotic neural network to encrypt MPEG-2 video codec system. The algorithm supports quality and bit rate control that is required by many video transmission applications, which is considered a new promising field related to video protection and compression. The rest of the paper is organized as follows, in section 2, a chaotic neural network based cipher is proposed. In section 3, the performance and security analyses are described in detail. Finally section 4, concludes the whole work.

2.0 A CIPHER BASED ON CHAOTIC NEURAL NETWORK (CNN)

The chaotic system is rich in significance or implication because it has sensitivity to change initial conditions and parameters, ergodicity [1], random behavior and unstable periodic orbits with long periods. The properties of diffusion, dispersion, disorder, and confusion required in conventional cryptography algorithms are achieved through iterative processing. The important difference between chaos-based and

conventional cryptography algorithms is that encryption transformations are defined on finite sets, while chaos has meaning only on real numbers [10]. A chaotic neural network (CNN)-based cipher which is a modification of the one developed in [6] was proposed, with respect to key size and neural network size. The encryption scheme belongs to the category of value transformation algorithm[2].

The logistics map is a chaos map analysis in [11] used with neural network to produce a combination of CNN, based on a binary sequence generated from the logistic map, the biases and weights of neurons are set in each iteration. A neural network is called a chaotic neural network if its weights and biases are determined by a chaotic sequence.
The logistic map is defined as:

$$f(x) = \mu\, x(1 - x) \tag{1}$$

The control parameter μ = 3.9712356378087541 and initial value x(0) = 0.7519649922109873 of the logistic map are represent the secret key of the system. The logistic map can exhibit strong chaotic behavior when μ is close to 4 [12]. Su in [6] has used 64 weights and 8 biases for neural network; however, if the size of neural network is increased to 256 weights and 16 biases the required execution time for CNN encryption and decryption process will be decreased as shown in Table 1.

By setting the length of input bit stream of the compressed stream M to encryption algorithm and evolving the chaotic sequence x(1), x(2), …, x(M) by x(n+1) = μ x(n)(1-x(n)), and generating a chaotic bit sequences b(0), b(1), …, b(16M-1) from x(1), x(2),…, x(M) by the generating scheme that 0.b(16m-16)b(16m-15)…b(16m-2)b(16m-l)… is the binary representation of x(m) for m = 1, 2, …, M. The encryption procedure: for the m-th plain-element $f(m)= \sum_{i=0}^{15} di(n).2^i$, the corresponding cipher-element $f'(m)= \sum_{i=0}^{15} \boldsymbol{d'i(n).2^i}$ is determined by the following process:

For i = 0 to15 and j = 0 to 15, 256 weights *wji* are calculated as follows:

$$wji = \begin{cases} 0 \; if \; j = i \; and \; b(16 \times m + i) = 0, \\ 1 \; if \; j = i \; and \; b(16 \times m + i) = 0, \\ -1 \; if \; j \neq i, \end{cases} \tag{2}$$

[1] A system that tends in probability to a limiting form that is independent of the initial conditions.
[2] Value transformation algorithms transform the data value of the original signal.

For $i = 0$ to 15, 16 biases θ_i are calculated as follows:

$$\theta_i = \begin{cases} -0.5 \; if \; b(16 \times m + i) = 0, \\ 0.5 \; if \; b(16 \times m + i) = 1, \end{cases} \quad (3)$$

Then the *i-th* cipher-bit $d'_i(n)$ is calculated as follows:

$$d'_i(n) = sign(\sum_{j=0}^{15} wji \times di + \theta_i) \quad (4)$$

Where $sign(\cdot)$ denotes the sign function, i.e.,

$$sign(x) = \begin{cases} 1, x \geq 0, \\ 0, x < 0, \end{cases} \quad (5)$$

The decryption procedure is the same as the above one.

Table 1 Comparison between two algorithms with respect to time execution and entropy for 4 successive frames.

Algorithm Type	Required Time for Encryption in S.	Required Time for Decryption in S.	Ciphertext Entropy
CNN algorithm [6]	475.3963	468.1908	7.8330
Enhanced CNN algorithm of [6]	304.7432	304.7352	7.7701

3.0 PERFORMANCE ANALYSES

3.1 MPEG-2 performance with respect to CNN

In this paper, MPEG-2 video compression system together with CNN cipher is employed. A video quality measure performance is developed by performing an objective fidelity measures such as PSNR. The whole system model shown in Figure 1 is tested by using a video sample with frame size 176 × 144 (QCIF standard format) with 30 frames per second. This video sample is compressed with constant quality for all video sequence so that the output bit rate is variable with time. The system has the ability to specify the number of frames to be performed, this work tested by using a sample of 4 successive frames with quality values of (90,

70, 50, 30, 10, and 5) depending on the bandwidth and channel condition as shown in Table 2. It has been also concluded from the results that CNN encryption and decryption have no effect on the quality of resultant output video as shown in Figure 2.

Table 2 Testing Table for Whole System Model

Uncompressed data rate (Mb\s)	Quality	Compressed Bit rate (Mb\s)	Compression ratio	PSNR(dB)
	90	0.19291	12.6124	44.25915
	70	0.111008	21.9176	39.32305
2.433024	50	0.086976	27.9735	36.64307
	30	0.063605	38.2519	33.146
	10	0.046869	51.9108	29.29482
	5	0.038624	62.9925	26.76662

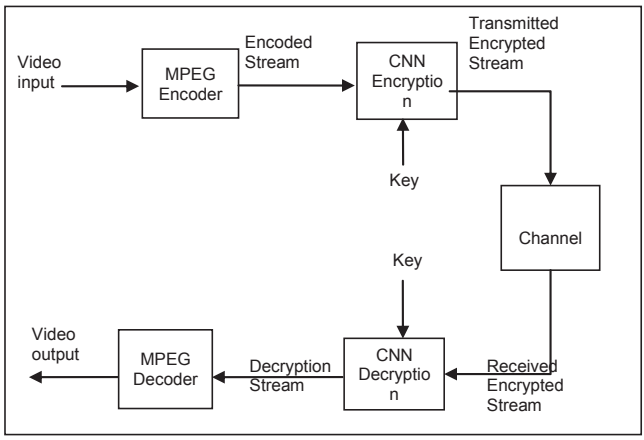

Figure 1 Whole System Model

3.2 Security Analysis

CNN algorithm is so much sensitive to the plaintext and keys, such that a very small change in the plain-image or the keys would lead to a totally different cipher data. The secret key of the system is control parameter μ = 3.9712356378087541 and initial value x(0)= 0.7519649922109873 of the logistic map, the key size is too long and its very difficult to guess by the attacker. The algorithm is very sensitive to the key, a small key

modification will result totally different unclear video results. To test the sensitivity of the ciphertext to the keys, the proposed work performed the following test, the key of the CNN encryption system is μ = 3.9000000000000001 and x = 0.7500000000000001, even with very small different in key in CNN decryption such as μ1 = 3.9000000000000002 and x2 = 0.7500000000000002 the resultant output video is unclear as shown in figure (3), and its PSNR is very low (-18.700925).

The entropy value of an encrypted cipher is shown in table (1). It has been shown from the result that the entropy of the encrypted image is close to the ideal entropy value, which is 8; this indicates that the rate of information leakage from the proposed image encryption algorithm is close to zero [13].

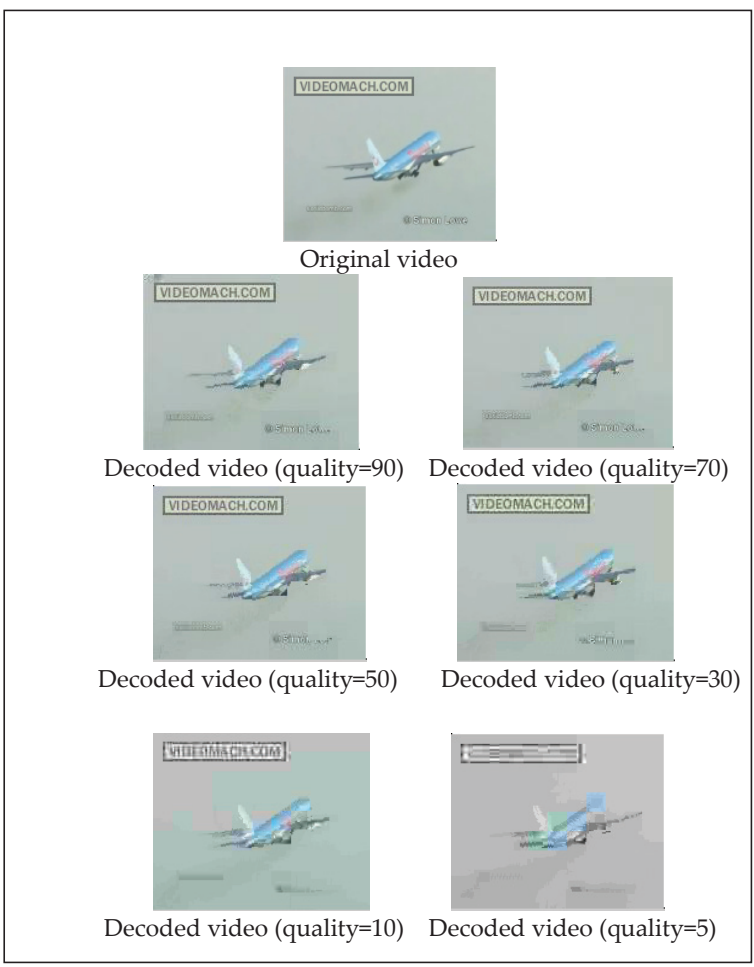

Figure 2 Original and decoded video for different qualities

Comparing the histogram of the plaintext, as shown in figure (4) and histogram of the ciphertext as shown in figure (5), it can be observed that the ciphertext has a good uniform distribution against original input video data. Accordingly, from the statistical analysis, it is observed that the proposed algorithm is secure against the statistical attacks mentioned in [14].

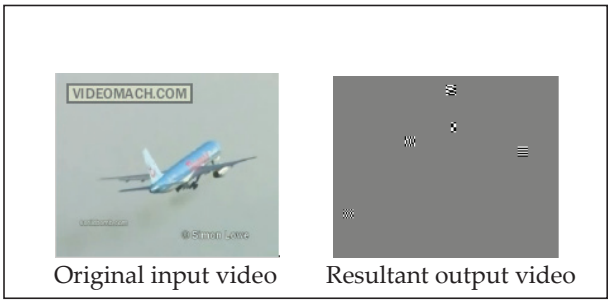

Figure 3 Sensitivity to Key Effect

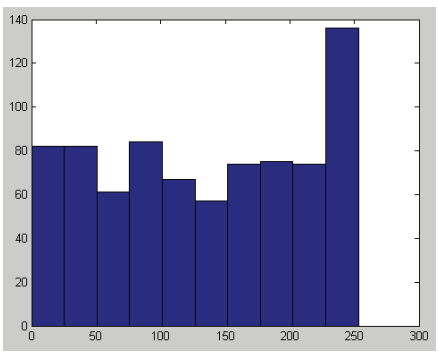

Figure 4 Ciphertext Histogram

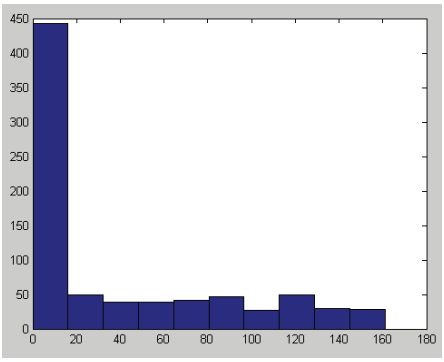

Figure 5 Original Plaintext Histogram

4.0 CONCLUSIONS

In this paper, a system model containing MPEG-2 for video compression and a Chaotic Neural Network (CNN) for ciphering and deciphering have been used. However, to reduce the required time for CNN encryption and decryption algorithm, it is proposed to increase the size of neural network. It has been shown from analysis results that the proposed algorithm has high security with low cost, and also supports quality and bit rate control. Hardware implementation and more security analysis and investigation are left for future work.

5.0 REFERENCES

A. Akhavan, A. Samsudin, A. Akhshani. 2011. A Symmetric Image Encryption Scheme Based on Combination of Nonlinear Chaotic Maps. Journal of the Franklin Institute. doi:10.1016/j.jfranklin.2011.05.001.

A. J. Menezes, P.C. Van Oorschot, S.A. Vanstone. 1997. Handbook of Applied Cryptography. CRC Press.

D. Guo, L. Cheng, L. Cheng. 1999. A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks. Applied Intelligence. Volume 10.

D. Xiao, X. Liao. 2004. A Combined Hash and Encryption Scheme by Chaotic Neural Network. Proc. Int'l Sym. Neural Nets. Volume 2. pp. 633–638.

G. Haojiang , Z. Yisheng, L. Shuyun, L.Dequn. 2006. A New Chaotic Algorithm for Image Encryption. Chaos, Solitons and Fractals. pp. 393-399.

H. Bai-Lin. 1993. Starting with Parabolas: An Introduction to Chaotic Dynamics. Shanghai Scientific and Technological Education Publishing House, Shanghai, China.

L. Shiguo. 2009. A Block Cipher on Chaotic Neural Network. Neurocomputing Elsevier, ScienceDirect. Volume 72. pp. 1296-1301.

R. Bose. 2005. Novel Public Key Encryption Technique Based on Multiple Chaotic Systems. Phys. Rew. Lett. Volume 95.

R. Stinson. 2002. Cryptography, Theory and Practice 2nd edition. CRC Press.

S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan. 2007. A Fast Chaotic Encryption Scheme Based on Piecewise Nonlinear Chaotic Maps. Phys. Lett. A 366. pp. 391-396.

S. Deng. 2005. Image Encryption Scheme Based on Chaotic Neural System. Springer-Verlag Berlin Heidelberg. LNCS 3497. pp. 868-872.

S. Lian, J. Sun, J. Wang, Z. Wang. 2007. A Chaotic Stream Cipher and The Usage in Video Protection. Chaos, Solitons and Fractals. Volume 34. pp. 851–859.

S. Su, A. Lin, J. Yen. 2000. Design and Realization of a New Chaotic Neural Encryption/Decryption Network. IEEE Asia-Pacific Conf. Cir. & Syst. pp. 335–338.

Z. P. Jiang. 2002. A Note on Chaotic Secure Communication Systems. IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications. Volume 49. pp. 92-96.