Networks Security & Distrubuted Systems (NSDS'2015)
25 - 26 November , Baghdad IRAQ

SECURE VIDEO CODED SYSTEM MODEL

Tariq Adnan Fadil*
Department of Computer Engineering Techniques
Dijla College University, Baghdad, Iraq
*Corresponding Author Email: tariq.adnan@duc.edu.iq

***Abstract*— In this paper, overall system model, shown in Figure (1), of video compression-encryption-transmitter/decompression-dencryption-receiver was designed and implemented. The modified video codec system has used and in addition to compression/decompression, the encryption/decryption video signal by using chaotic neural network (CNN) algorithm was done. Both of quantized vector data and motion vector data have been encrypted by CNN. The compressed and encrypted video data stream has been sent to receiver by using orthogonal frequency division multiplexing (OFDM) modulation technique. The system model was designed according to video signal sample size of 176 × 144 (QCIF standard format) with rate of 30 frames per second. Overall system model integrates and operates successfully with acceptable performance results.**

***Keywords*— Video, Compression, Encryption, Transmission, CNN, OFDM.**

1. INTRODUCTION

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 users also is important, especially in applications that require 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 unsafe channel while keeping the privacy of the transmitted data [1], [2]. Due to some essential features of images, like high data capacity and high profile links among pixels, classical encryption methods are improper for workable image encryption [3]. Neural network can be used for data security schema design due to its complexity and time-varying structure [4]. Due to the desired features of mixing neural and the sensitively of initial value conditions of chaotic maps, a chaos-based neural network combination will produce a model called a chaotic neural network (CNN) which is given a new promising and efficient way for data encryption [3], [5].

Real-time digital video transmission has another demanding requirement; it needs a high transmission bandwidth; it must be transmitted with minimal delay, and it cannot tolerate a high error rate [6]. Visual communication is an important part of multimedia services for third and fourth generations of personal communication services. The concept of the next generation includes a small handset, which allows users to communicate with each other from anywhere in the world, and by various data formats (e.g., voice, text, images, video, and sound). Many technical problems remain to be solved in order to make this imagination a reality. However, wireless video communication is particularly in great demand. Powerful compression algorithms must be used to deliver digital video since the available is limited [7]. The data rate requirements are aggravated if multiple terminals demand video transmission from a signal access point, serving a given wireless cell. The high data rate requirements of such applications require wireless transmission technologies that can support them.

One especially promising approach here is the Orthogonal Frequency Division Multiplexing (OFDM) which does not only provide high data rates over wireless channel, but also supports a notion of resources sharing between multiple wireless terminals by dividing the wireless bandwidth into so-called "subcarriers", which can be individually assigned to different terminals [8]. The rest of the paper is organized as follows; system model design was described in section 2. Result analysis and performance were described in section 3. Finally section 4, concludes the whole work.

2. SYSTEM MODEL DESIGN

In this section, a modified video compression system is used together with OFDM transceiver system to transmit a secure video signal as shown in Figure (1). Video quality measure performance is developed by performing an objective fidelity measure like PSNR. The overall system model is tested by using a video sample size of 176 × 144 (QCIF standard format) with rate of 30 frames per second. This system model also is used to simulate the transmission of compressed video signal over wireless radio channel by using OFDM modulation technique.

In this system model, the input video signal is compressed then encrypted by CNN algorithm then the

resultant bit stream is transmitted using OFDM transmitter. At the receiver side the received signal is demodulated using OFDM receiver to reconstruct the received encoded bit stream, which then passes through modified video decompression to reconstruct the resultant video signal. More details on System model parts are described on the following subsections:

2.1 VIDEO CODEC/ CRYPTOGRAPHY

Video codec / cryptography system model has been developed to support a wide range of digital video applications, including home entertainment and broadcast applications. It was illustrated as shown in Figure (1).

● Video Compression/Encryption

As shown in Figure (1), the frame store contains a reconstructed copy of the previous encoded frame: this is used as a reference for temporal prediction. The motion estimator calculates motion vectors for each block of the current frame. A motion-compensated version of the previous frame is subtracted from the current frame to create a difference or error frame. Each block of this difference frame is then transformed using Discrete Cosine Transform DCT and the coefficients are quantized and, together with the motion vectors, are encrypted by CNN algorithm and then entropy coded. At the same time, the quantized coefficients are rescaled (the IQuant block) and inverse transformed (IDCT) to create a local copy of the encoded and decoded frame. This is used as the prediction reference for the next frame. (This ensures that the encoder and decoder use identical reference frames for motion compensation).

● Video Decompression/Decryption

The coded data is entropy decoded then decrypted by CNN algorithm and the coefficients are rescaled ("inverse quantization") and inverse transformed to recreate the difference frame. A motion-compensated reference frame is created using the previous decoded frame and the decrypted motion vectors for the current frame. The current frame is reconstructed by adding the difference frame to this reference frame. This frame is displayed and is also stored in the decoder frame store.

2.2 CNN CIPHER ALGORITHM

Chaotic system is rich in its importance because of sensitivity to initial conditions, ergodicity, random behavior and unsteady periodic orbits with long periods. Features of diffusion and confusion are required in conventional cryptography algorithms, and they are achieved through iterative processing. The significant difference between chaos-based and traditional cryptography algorithms is that encryption transformations are defined in finite sets, while chaos is meaningful only on real numbers [9]. The logistic map is a chaotic map analysis in [10] and is used with neural network to produce a combination of CNN. Logistic map defined as: $f(x, \mu) = \mu x (1 - x)$, the system works in chaotic area for control parameter values μ (s_∞, 4], where $s_\infty \approx 3.57$ – Feigenbaum's constant, see bifurcation diagram Figure (2). The system exhibits strong chaotic behavior when a control parameter μ is close to 4 [11]. If not, then the logistic map has a negative Lyapunov exponent value, and the system does not reveal chaotic behavior, which can lead to a cryptanalytical vulnerability of the cipher [12]. To ensure the security of the cipher; Lyapunov exponent value should be always positive even the control parameter μ value is changed. If it is negative, then a new value should be chosen.

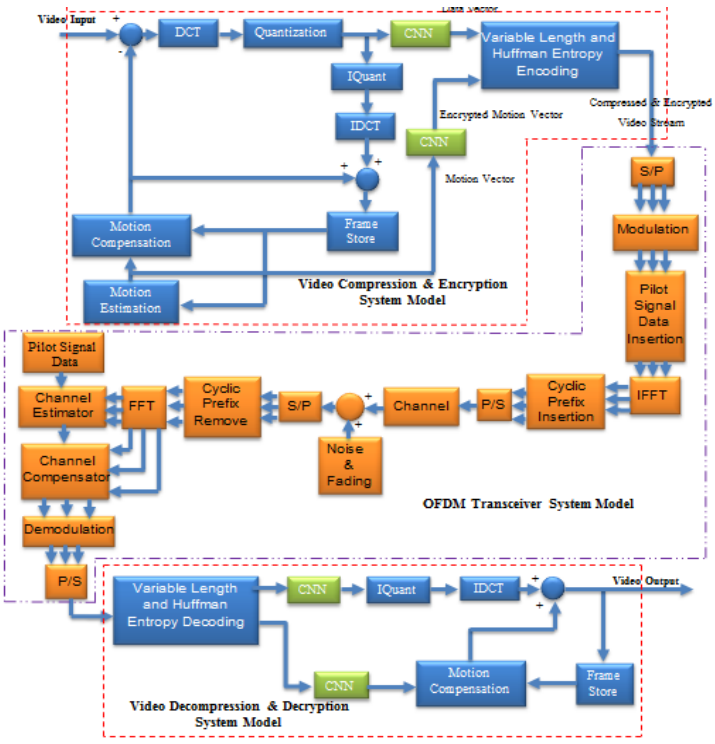

Fig. (1) Overall System Model

The cipher algorithm belongs to a category of value transformation algorithm. A neural network is called a CNN if its weights and biases are determined by a chaotic sequence. Based on binary sequence generated from the logistic map, biases and weights of neurons

are set in each iteration. The control parameter μ = 3.9712356378087541 and the initial value x = 0.7519649922109873 of the chaotic logistic map are represent the secret keys of the system.

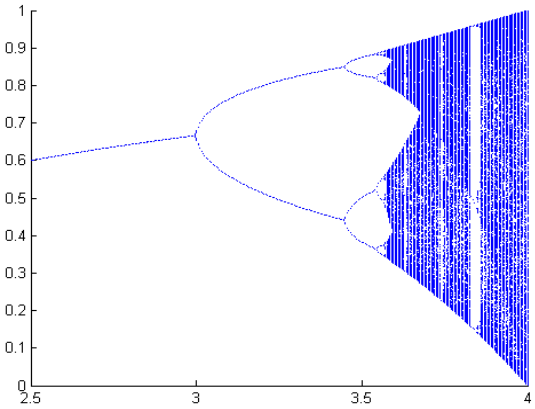

Fig. (2) Bifurcation Diagram of a logistic map

2.3 OFDM MODULATION TECHNIQUE

OFDM is a modulation scheme that allows digital data to be efficiently and reliably transmitted over radio channel, even with presence of multipath environments. OFDM transmits data by using a large number of narrow bandwidth carriers. The frequency spacing and time synchronization of these carriers are chosen in such a way that these carriers are orthogonal, meaning that they do not interfere to each other. The name "OFDM" is delivered from the fact that the digital data is sent by using many carriers, each of different frequency (Frequency Division Multiplexing) and these carriers are orthogonal to each other, hence Orthogonal Frequency Division Multiplexing. Figure (3) shows the comparison between conventional multicarrier technique and orthogonal multicarrier technique. OFDM has been adopted in wide band digital communication applications, like digital audio and video broadcasting DAB and DVB [13].

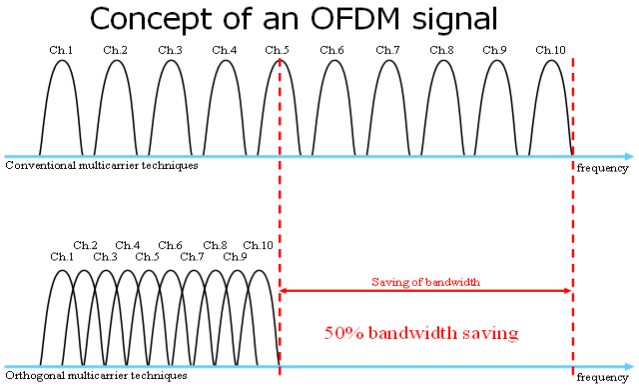

Fig. (3) Comparison between Conventional Multicarrier and Orthogonal Multicarrier technique

3. RESULT ANALYSIS AND PERFORMANCE

3.1 VIDEO CODEC

The video signal is compressed with constant quality for all video sequence so that the output bit rate is variable with time. This system model ability to specify the number of frames to be performed, in this paper four successive frames are used with quality values of (90, 70, 50, 30, 10, and 5) as shown in Table (1).

Table (1) Testing Table for Overall System Model

Uncompressed Data Rate (Mb\s)	Quality	Compressed Bit Rate (Mb\s)	Compression Ratio	PSNR(dB)
2.433024	90	0.19291	12.6124	44.25915
	70	0.111008	21.9176	39.32305
	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

3.2 CNN CIPHER ALGORITHM

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 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, with minor key different at CNN decryption such as μ1 = 3.9000000000000002 and x2 = 0.7500000000000002, then the resultant output video is unclear as shown in Figure (4), and its PSNR is very low (-18.700925).

The entropy value of an encrypted cipher is 7.833. It has been shown 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 [14].

Original input video Resultant output video

Fig. (4) Sensitivity to Key Effect

3.3 OFDM TRASMISSION TECHNIQUE

The radio channel is assumed to be an AWGN channel. The modulation type used is BPSK modulation scheme. In this test, different values of signal to noise ratio (E_b/N_o) are used and the PSNR value for each E_b/N_o is measured. Investigating these results highlight the following: the PSNR approaches the target of acceptable video quality when E_b/N_o become on or above 12 dB as shown in Table (2). The BER is estimated here by comparing the transmitted bit stream with the received bit stream.

Table (2) Variation of PSNR and BER for different values of E_b/N_o through AWGN Channel

E_b/N_o (dB)	PSNR(dB)	BER
10	7.3211	5.6078e-05
11	10.24	6.9137e-06
11.5	12.8646	3.0728e-06
12	32.6432	7.6819e-07

4. CONCLUSION

In this paper, an integrated system model of video compression-encryption-trasmitter/decompression-decryption-receiver have been designed and implemented successfully. Cryptography algorithm was performed by using combination of chaos theory and neural network. User has ability to control quality level value in this system model, with quality level value of 50; this value renders both high compression and excellent decompression video quality. CNN algorithm shows sensitivity to key modification and high entropy value of an encrypted cipher. At wireless channel, PSNR approaches acceptable video quality value when Eb/No becomes on or above 12 dB.

REFERENCES

[1] R. Stinson. "Cryptography, Theory and Practice", second edition, CRC Press, 2002.
[2] A. Menezes, P.C. Oorschot, and S. Vanstone. "Handbook of Applied Cryptography", CRC Press, 1997.
[3] S. Deng, "Image Encryption Scheme Based on Chaotic Neural System", LNCS 3497, pp. 868-872, Springer-Verlag Berlin Heidelberg 2005.
[4] D. Guo, L. Cheng, L. Cheng, "A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks", Applied Intelligence 10 (1) (1999).
[5] S. Lian, J. Sun, J. Wang, Z. Wang, "A chaotic stream cipher and the usage in video protection", Chaos, Solutions and Fractals 34 (3) (2007) 851–859.
[6] M. J. Riley, "Digital Video Communications", Artech House, Boston, London, ISBN 0-89006-890-9, 1997.
[7] A. H. Sadka, "Compressed Video Communication" John Wiley and Sons, England, ISBN 0-470-84312-8, 2002.
[8] J. Gross, J. Klaue, H. Karl and A. Wolisz, "Cross-Layer Optimization of OFDM Transmission Systems for MPEG-4 Video Streaming", Telecommunication Networks Group, Technical University of Berlin, 2004.
[9] Jiang, Z. P., "A Note on Chaotic Secure Communication Systems". IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications. vol. 49, no. 1, pp. 92-96, January 2002.
[10] Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li, "A new chaotic algorithm for image encryption", Chaos, Solitons and Fractals, pp. 393-399, July 2006.

[11] Hao Bai-Lin. Starting with Parabolas: An Introduction to Chaotic Dynamics. Shanghai Scientific and Technological Education Publishing House, Shanghai, China, 1993.
[12] G. Álvarez, F. Montoya, M. Romera, G. Pastor: Cryptanalysis of a discrete chaotic cryptosystem using external key, Phys. Lett. A 319, 334–339, (2003).
[13] Y. Sun, "Bandwidth-Efficient Wireless OFDM", IEEE Journal on Selected Areas in Communication, Vol. 19, No. 11, pp. 2267-2278, November 2001.
[14] A. Akhavan, A. Samsudin, A. Akhshani, "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, 2011.