CHAOTIC NEURAL NETWORK BASED MPEG-2 VIDEO ENCRYPTION FRAMEWORK OVER WIRELESS CHANNEL

by

TARIQ ADNAN FADIL
(1040210542)

A thesis submitted in fulfillment of the requirements for the degree of
Doctor of Philosophy

School of Computer and Communication Engineering
UNIVERSITI MALAYSIA PERLIS (UniMAP)

2014

ACKNOWLEDGMENT

Pursuing a doctoral degree is considered a hard and long journey that one cannot make it alone. First of all, my great thank is truly to My Lord (*Allah* ﷻ) who has awarded me all the health, strength, and belief to complete this work. I would like also to thank all those who have assisted me in my way to doctoral degree as follows:

My most special thanks are to my supervisors Dr. Shahrul Nizam Yaakob and Prof. Dr. R. Badlishah Ahmad, for their continuous, valuable and indispensable advices, their unlimited support, encouragement, and patience.

My special thanks for my lovely parents, brothers, and sisters in Iraq for their unlimited love, advice, motivation, and sacrifices.

I would like to acknowledge the Malaysian Ministry of Education and UniMAP for supporting me financially during my study.

Finally, thanks to all my friends. I am indebted to them and words will never express the gratitude I owe to them.

Tariq Adnan Fadil
University Malaysia Perlis (UniMAP)

TABLE OF CONTENTS

CHAPTER 3 CNN BASED VIDEO ENCRYPTION FRAMEWORK

CHAPTER 4 RESULTS AND ANALYSIS

CHAPTER 5 CONCLUSION AND FUTURE WORK

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

2G	Second Generation
3G	Third Generation
ATM	Asynchronous Transmission Mode
AVI	Audio/Video Interleaved
AWGN	Additive White Gaussian Noise
B-Frame	Bidirectional Prediction Frame
BER	Bite Error Rate
BMA	Block-Matching Algorithm
BPSK	Binary Phase Shift Keying
CBR	Constant Bit Rate
CCIR	International Radio Consultative Committee
CIF	Common International Format
CR	Compression Ratio
CNN	Chaotic Neural Network
CODEC	Coder/Decoder
CP	Cyclic Prefix
dB	Decibel
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DPCM	Differential Pulse Code Modulation
DVD	Digital Versatile Disk
DVB	Digital Video Broadcasting
EOB	End Of Block
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FEC	Foreword Error Control
FPS	Frame Per Second
FFT	Fast Fourier Transform
GOP	Group Of Picture
GSM	Global System Mobile
HDTV	High Definition Television

HTTP	Hyper Text Transfer Protocol
HVS	Human Visual System
H.263	A video coding standard
ICI	inter-carrier interference
I-Frame	Intra-Frame
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISI	Intersymbol Interference
ISO	International Standard Organization
LOS	Line OF Sight
ITU	International Telecommunication Union
MAD	Mean Absolute Difference
MB	Macro Block
M-JPEG	Motion-Joint Photographic Expert Group
MSD	Mean Square Difference
MPEG	Moving Picture Expert Group
MSE	Mean Square Error
MV	Motion Vector
OFDM	Orthogonal Frequency Division Multiplexing
P/S	Parallel to Serial
P-Frame	Prediction-Frame
PDF	Probability Density Function
PSNR	Peak Signal to Noise Ratio
PSTN	Public Switched Telephone Network
QCIF	Quarter Common International Format
QOS	Quality Of Services
RGB	Red, Green, Blue
RLC	Run Length Coding
S/P	Serial to Parallel
SNR	Signal-to-Noise Ratio
STD	Standard Deviation
TCP	Transmission Control Protocol
TSS	Three-Step Size

VBR	Variable Bit Rate
VLC	Variable Length Coding
WiMaX	Worldwide Interoperability for Microwave Acess
YC_bC_r	Color model, where Y is Luminance, C_b and C_r are chrominance (color) components.
ZP	Zero Padding
ZRL	Zero Run-Length
Mbps	Mega bit per second
QoS	Quality of Service
RF	Radio Frequency
VoD	Video-on Demand

LIST OF SYMBOLS

BW	Bandwidth
C_b	Blue Chrominance Signal
C_g	Green Chrominance Signal
C_r	Red Chrominance Signal
$\hat{d}_i$	Fourier Coefficients of the Signal
$\hat{d}(k)$	Compensated data symbols
$d_r(k)$	Received data symbols
$D_{m,n}$	Minimum Distortion of the candidate block
E_b/N_o	Bit energy to noise ratio
Δf	Sub-carrier Spacing
F(u,v)	DCT transformed coefficient at position (u,v)
f(x,y)	Inverse DCT transformed at position (x,y)
f_o	Frequency of the Source
f_i	Frequency of the i-th subcarrier
H	Number of Lines
$h(\tau - t)$	Impulse response of the radio channel
$I(r,c)$	pixel value of the original frame at the (r,c) location
$\hat{I}(r,c)$	Pixel value of the reconstructed frame at the location (r,c)
k	Positive integer
n(t)	Sample function of noise
N	Sub-carriers number
$p(\varphi)$	Probability Density Function
$P(r)$	Rayleigh distribution
$r(t)$	Received signal
s(t)	Digital information sent by transmitter
$s'(t)$	OFDM signal
τ	Delay Spread
T_U	Useful symbol duration
T_s	Symbol duration of the OFDM signal
T_g	Guard interval duration
T_{total}	Total symbol duration
W	Number of pixel per line
w_b	Weight factor blue color
w_g	Weight factor green color
w_r	Weight factor red color
x(n)	Transmitted sequence signal
y(n)	Received signal
Δf_d	Change in Frequency of the Source seen at the Receiver
Δf	Sub-Carrier Spacing
φ	Noise signal

$\delta(t)$	Pulse waveform of each of the symbol
$\delta'(t)$	Modified pulse waveform of each symbol
x	Initial Value of Logistic Map
μ	Control Parameter

Rangka Kerja Penyulitan Rangkaian Neural 'Chaotic' berasaskan MPEG-2 pada Saluran Tanpa Wayar

ABSTRAK

Perekabentuk kejuruteraan sistem menghadapi cabaran baharu daripada peningkatan permintaan terhadap aplikasi perkhidmatan multimedia yang selamat dan berkualiti tinggi melalui saluran jalur lebar untuk menyediakan penyelesaian yang cekap dan optima. Dalam tesis ini sifat teori 'chaos' digabungkan dengan rangkaian neural buatan untuk membina algoritma penyulitan 'cipher' yang dinamakan Rangkaian Neural 'Chaos' (CNN). Rangka Kerja model ini dibina dan dimodel dengan menggabungkan Rangkaian Neural 'Chaos' kedalam model 'codec' bagi menghasilkan 'bitstream' mampat yang selamat. Model ini direkabentuk dan dimodelkan berasaskan piawaian MPEG-2. Isyarat video 'bitstream' ini dihantar daripada sumber ke destinasi melalui teknik modulasi 'Orthogonal Frequency Division Multiplexing' (OFDM). Saiz isyarat video input yang diuji adalah 176 x 144 berpandukan format piawai QCIF. Rangka jujukan video dibahagikan kepada 30, 15, 10 dan 5 set yang di alirkan kepada model berkenaan. Rangka yang pertama dikenali sebagai Rangka-I bagi setiap Kumpulan Gambar (GOP) dimampat sebagai imej yang statik. Manakalan rangka-rangka yang lain dimampat menggunakan algoritma gerakan 'estimation' dan 'compensation' dan selanjutnya di kod semula seperti Rangka-I. Algoritma carian tiga langkah (TSS) digunakan dalam algoritma gerakan 'estimation' dan 'compensation'. Nilai Pemberat dan 'bias' bagi algoritma CNN didapati daripada jujukan binari yang dijana daripada peta logistik 'chaotic' pada setiap pusingan. Parameter kawalan dan nilai awal bagi peta logistik 'chaotic' digunakan sebagai kekunci rahsia untuk algoritma 'cipher'. CNN digunakan untuk sulitkan/nyahsulit data gerakan dan data statik dalam model video 'codec'. Algoritma CNN sangat sensitif terhadap pengubahsuaian kekunci dan teks biasa dengan mempamirkan nilai PSNR 18.363 dB dan nilai entropi 7.833. Rangka kerja model sistem mampu mengawal kualiti video, kadar bit, penyusunan rangka dan bilangan GOP. Hasil simulasi menunjukkan aliran bit yang dialirkan terlindung daripada serangan teks biasa yang diketahui. Pengukuran subjektif serta objektif telah digunakan untuk menentusahkan kebolehupayaan rangka kerja model sistem secara keseluruhan.

Chaotic Neural Network Based MPEG-2 Video Encryption Framework Over Wireless Channel

ABSTRACT

The increasing demand for retrieving secure and high quality of multimedia service applications corresponding to available bandwidth channel proposes new challenges for system engineering designers to implement efficient and optimum solution ideas. In this thesis, chaos theory property is combined with artificial neural network to construct a cipher cryptography algorithm called a Chaotic Neural Network (CNN). The proposed system model framework is developed and modelled by embedding CNN inside video codec model to produce a secure and a compress bitstream. The proposed video codec model is designed and implemented based on MPEG-2 standard. The resultant video signal bitstream is transmitted from source to destination by using Orthogonal Frequency Division Multiplexing (OFDM) modulation technique. The size of tested input video signal is 176 × 144 (QCIF standard format). The video sequence frames is divided into sets of 30, 15, 10, and 5 frames which are fed to the framework model. The first frame (I-Frame) for each Group of Pictures (GOP) is compressed as still image (i.e. by using DCT transform, Quantization, Zig-Zag scan, and Huffman entropy coding), while other frames are compressed by using motion estimation and compensation algorithm then encoded like (I-Frame). Three Step Search algorithm (TSS) is used as motion estimation and compensation algorithm in this thesis. Weights and biases of CNN algorithm are set based on binary sequence generated from the chaotic logistic map for each iterate. Control parameter and initial value of chaotic logistic map are used as secret keys of the cipher algorithm. CNN is used to encrypt/decrypt both of motion and quantized data vectors of video codec model. CNN algorithm shows high sensitivity behavior for both key and plaintext modification with low PSNR value of -18.363 dB and high entropy value of 7.833. OFDM model performance is investigated and simulated over AWGN and 2-path frequency selective Rayleigh fading channel. Mathematical formulation expression is given and software programming code implementation is written by using MATLAB to simulate and test the overall system model framework. The proposed system model framework has the ability to control the required video quality value factor, bit rate, frames arrangement, and GOP number. Results indicate that the transmitted bitstream has been protected from known plaintext attack. Perceptual encryption feature was satisfied and applied successfully. Finally, subjective and objective measurement metrics are used to verify the performance of overall system model framework.

CHAPTER 1

INTRODUCTION

1.1 Overview

Multimedia encryption techniques are closely related to some other techniques, such as encryption techniques (Mollin, 2006), multimedia compression (Sayood, 2005), multimedia communication (Rao, et al., 2006), and digital watermarking (Cox, J., Miller, M. L., & Bloom, J. A., 2002). First, multimedia encryption aims to encrypt multimedia content with encryption techniques, and thus, multimedia encryption is based on traditional encryption techniques. Second, multimedia content is often compressed before transmission or storage in order to save cost in space or bandwidth, and thus, multimedia encryption should consider the compression operations, for example, before compression, during compression or after compression. Third, multimedia content is often transmitted from the sender to the receiver through multimedia communication techniques, and thus, the multimedia encryption should satisfy different applications in multimedia communication.

Video compression and encryption are associated processes in secure multimedia systems and applications. Some video encryption algorithms are even fully embodied in a video codec. Standardized video compression technologies like MPEG-1 (ISO/IEC, 1993), MPEG-2 (ISO/IEC, 2000), H.261 (ITU-T, 1993), H.263 (ITU-T Recommendation H.263, 1998), and MPEG-4/ H.264 AVC (Advanced Video Coding) (ITU-T Recommendation H.264, 2007; ISO/IEC, 2005) are widely deployed for economically storing digital videos on storage constrained devices or efficiently transmitting them over bandwidth-limited networks. All video coding standards utilize the hybrid coding approach, i.e. they compress video data by using intra-frame and

inter-frame coding simultaneously (Salomon, 2004). Although there are differences in the concrete coding algorithms applied, the compression standards are built upon the same fundamental set of function elements.

The intra-frame coding is used to reduce spatial redundancy that exists within the frame. It compresses an entire video frame independently of any other frames. The resulting coded frame is denoted as I-frame. A video frame is divided into a number of macro blocks (16×16 pixels). The macro blocks can be further divided into distinct blocks (8×8 pixels). Each block is processed through three sequential procedures: DCT Discrete Cosine Transform) transformation, quantization, and entropy coding (Effelsberg & Steinmetz, 1998). The inter-frame coding encodes the differences between frames to reduce temporal redundancy that exists between successive frames.

Before encoding a block of pixels, the motion compensated prediction technique is used to search for a good match block in the reference frames. If such block is found, only the motion vector representing the motion of the block and the differences between the current and referred block need to be encoded. When no match block can be found in the reference frames, the block has to be compressed using the intra-frame coding method. The coded block is therefore called I-block. There are two kinds of frames using the motion compensated prediction: P (Predicted) frame, which is compressed using only previously decoded frames as reference frames, and B (Bi-directionally predicted) frame, which is predicted from past and future frames.

1.2 Problem Statement

Today, more information that include text, audio, image and other multimedia has been transmitted over wireless channel. Digital video signal applications are widely used in our daily life. Transmission of video signal consumes more time and occupies huge bandwidth channel due to the large size of video file compared with other multimedia types. Therefore, video data signal should be compressed before transmission to destination.

Video signal protection represents another important factor during transmission. Due to some inherent features of video, such as bulk data capacity and high correlation among pixels, traditional cryptographic techniques such as Data Encryption Standard (DES) and Rivest-Shamir-Adelman (RSA) are no longer suitable for practical image encryption. The aim of the traditional encryption algorithms is to shuffle the plain image, it make ciphers look like random. For the property of initial-value sensitivity, ergodicity or random similarity, chaos was used in data protection (Deng, 2005; Lian, et al., 2007). Chaos-based encryption has given a new and efficient way to deal with the intractable problem of highly secure image encryption due to the exceptionally desirable properties of mixing and sensitivity to initial condition and control parameter of chaotic map. As well as, artificial neural network can be used for data protection design schemes because it's complicated and time-varying structures (Bigdeli, et al., 2012). In this thesis, chaotic logistic map is combined with artificial neural network to construct a cipher cryptography algorithm called a chaotic neural network (CNN). In general, Symmetric cryptography algorithms show weakness to known plaintext attack, however, the transmitted video bitstream in this research is protected from this type of

attack, and the produced video signal satisfy high visual degradation which is enough for unauthorized people or attacker to understand the contents.

On the other hand, the ability to achieve low bit error rate is severely restricted by the frequency selectivity of the channel due to multiple paths propagation which leads to unacceptable degradation of system performance. This problem can be overcome by using Orthogonal Frequency Division Multiplexing (OFDM) modulation technique. The limitation of channel bandwidth problem is overcome by controlling the quality scale factor of resultant video signal. The aim of this research is to demonstrate the key problem emphasizes on video signal challenges of compression, encryption, and transmission from source to destination over wireless channel.

1.3 Research Questions

This thesis aims giving answers to following research questions:

(1) How to achieve acceptable video quality model with reasonable bitrate?

(2) How to achieve secure model algorithm for the delivered video signal?

(3) How to achieve robust and reliable video signal transmission over wireless channel?

1.4 Research Objective

The objectives of this research are as follows:

1- To compress the video signal using MPEG-2 standard. The proposed model has the ability to control the required quality factor and bitrate level corresponding to available variable bit rate (VBR) bandwidth channel.

2- To encrypt the resulting compressed video signal by using Chaotic Neural Network (CNN) cryptography algorithm, the developed algorithm is based on combining the chaos theory and artificial neural network.

3- To evaluate the performance of the above two objectives by transmitting it over wireless channel for both AWGN and multipath Rayleigh fading channel. OFDM modulation technique has been used for video bitstream transmission from source to destination.

1.5 Thesis Outline

The outline of this thesis as follows:

Chapter 1 presents overview, problem statement, methodology, research aim and objective, and thesis outline.

Chapter 2 presents literature review and describes different related research studies and their respective properties.

Chapter 3 focuses on research methodology of developed system model framework to investigate the performance of video compression, encryption, and transmission.

Chapter 4 presents results and discussion; analysis and performance investigation of the developed system model was done in this chapter as well as with comparison performance with other previous studies.

Chapter 5 presents the conclusion and suggestion for research future work.