UNIVERSITI PUTRA MALAYSIA

JPEG IMAGE ENCRYPTION USING COMBINED REVERSED AND NORMAL DIRECTION-DISTORTED DC PERMUTATION WITH KEY SCHEDULING ALGORITHM-BASED PERMUTATION

AHMAD ZAIDEE BIN ABU

JPEG IMAGE ENCRYPTION USING COMBINED REVERSED AND NORMAL DIRECTION-DISTORTED DC PERMUTATION WITH KEY SCHEDULING ALGORITHM-BASED PERMUTATION

By

AHMAD ZAIDEE BIN ABU

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for Degree of Master of Science

January 2008

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirements for the degree of Master of Science

JPEG IMAGE ENCRYPTION USING COMBINED REVERSED AND NORMAL DIRECTION-DISTORTED DC PERMUTATION WITH KEY SCHEDULING ALGORITHM-BASED PERMUTATION

By

AHMAD ZAIDEE ABU

January 2008

Chairman: Associate Professor Adznan bin Jantan, PhD

Faculty: Engineering

This thesis work studied on digital image encryption algorithms performed towards JPEG images. With image encryption algorithms, JPEG images can be securely scrambled or encrypted prior to distribution. The intended recipient will be given a decryption key in which only with this key the receiver can received and decrypt the media for viewing. The proposed approach uses a frequency domain combinational framework of coefficients scrambling with Key Scheduling Algorithm based (KSA-based) permutation. This novel algorithm applies coefficients scrambling using Combined-Reverse-and-Normal-Direction (CRND) scanning together with Distorted DC permutation (DDP). This encryption algorithm involved the manipulation of JPEG zigzag scanning table according to 10 different scanning tables which was derived by reversing the existing zigzag scanning directions. With the same compression properties, this encryption algorithm was shown to be able to produce average file size smaller than baseline JPEG and other encryption. It was also shown that the average decoding speed for this technique outperform most of other existing techniques and the same time able

to maintain image quality (PSNR) as other techniques. It terms of security, with the combination of Distorted DC permutation (DDP), it was considered to be having medium security based on some basic attack analysis that was carried out. It is also shown that this technique is fully format compliance as most of other techniques do. Based on the simple nature of CRND, this technique is easy to be implemented on existing system and thus should be able reduce the cost of implementing a new encryption system.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

ENKRIPSYEN IMEJ JPEG MENGGUNAKAN GABUNGAN ARAH BERTENTANGAN DAN NORMAL-PERMUTASI PERENCATAN DC DENGAN PERMUTASI BERSANDARKAN ALGORITMA JADUAL KEKUNCI

Oleh

AHMAD ZAIDEE ABU

Januari 2008

Pengerusi: Profesor Madya Adznan bin Jantan, PhD

Fakulti: Kejuruteraan

Tesis in mengkaji tentang enkripsyen bagi digital imej yang dilakukan terhadap imej JPEG. Dengan adanya algorithm-algoritma enkripsyen bagi imej, imej JPEG dapat di selerakkan atau dienkrip sebelum disebarkan. Penerima tertentu akan diberikan kata kunci dekripsyen yang mana hanya dengan kata kunci ini sahaja penerima tersebut boleh menukarkan semula media yang diterima kepada bentuk yang asal. Pendekatan yang dicadangkan ini menggunakan kombinasi rangka-kerja koefisien dalam domain frekuensi berasaskan algoritma Permutasi Kekunci Berjadual. Algoritma novel ini mengaplikasikan penyelerakan koefisien menggunakan Kombinasi-Arah-Berlawanan-dan-Normal (CRND) bersama-sama dengan Permutasi Perencatan DC (DDP). Algoritma enkripsyen ini melibatkan manipulasi pengimbasan 'zigzag' bagi JPEG dengan menggunakan 10 kombinasi pengimbasan 'zigzag' yang berbeza menggunakan CRND. Dengan menggunakan sifat-sifat pemampatan yang sama, enkripsyen ini telah ditunjukkan berkemampuan untuk menghasilkan purata saiz fail image yang lebih kecil daripada yang terhasil daripada 'Baseline JPEG' dan teknik-teknik enkripsyen yang lain. Telah ditunjukkan juga bahawa purata masa yang diambil untuk mengdekrip lebih baik

daripada teknik-teknik enkripsyen lain. Di dalam masa yang sama juga teknik ini mampu memelihara kualiti (PSNR) imej sebagaimana teknik-teknik lain. Dari segi jaminan keselamatan pula, dengan kombinasi DDP, ia boleh dikategorikan sebagai keselamatan tahap pertengahan yang mana telah dibuktikan melalui analisis serangan asas. Telah ditunjukkan juga bahawa teknik ini juga adalah mengikut piawaian penuh format JPEG sebagaimana juga teknik-teknik lain. Berdasarkan sifat CRND yang lurus dan mudah difahami, teknik ini mudah untuk diaplikasikan pada sistem yang sedia ada dan sekaligus mampu mengurangkan kos bagi mengaplikasikan sistem enkripsyen baru.

ACKNOWLEDGEMENTS

I would like to express my gratitude to:

My beloved parents, whose keep reminding me to finish my MSc.

My beloved wife, Fazdliana Samat for her help, patience, guidance and support and my beloved son Ahmad Darwisy bin Ahmad Zaidee who also gave me the strength to complete this dissertation.

My supervisor, Prof. Madya Dr. Adznan bin Jantan for his guidance and patience waiting for this dissertation.

ABJ Research group members for their guidance and supports even though I couldn’t always be there for group meeting.

And last but not least, everyone who had been supportive, encouraging and helpful through my long MSc Journey.

I certify that an Examination Committee has met on 3rd January 2008 to conduct the final examination of Ahmad Zaidee bin Abu on his Master of Science thesis entitled "JPEG Image Encryption Using Combined Reversed and Normal Direction-Distorted DC Permutation with Key Scheduling Algorithm-Based Permutation" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the student be awarded the degree of Master of Science.

Members of the Examination Committee were as follows:

Mohamad Khazani Abdullah, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Raja Syamsul Azmir Raja Abdullah, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

M. Iqbal Saripan, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Khairuddin Omar, PhD
Associate Professor
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia
(External Examiner)

HASANAH MOHD. GHAZALI, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 1 April 2008

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Adznan bin Jantan, PhD
Associate Professor
Faculty of Engineering
University Putra Malaysia
(Chairman)

Khairi Yusof, PhD
Lecturer
Faculty of Engineering
University Putra Malaysia
(Member)

AINI IDERIS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 10 April 2008

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declared that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.

AHMAD ZAIDEE ABU

Date:

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AC	ac coefficients of an image block
ARPA	Advanced Research Projects Agency
ARPANET	ARPA Network, developed by ARPA
ASCII	American Standard Code for Information Interchange
CODEC	Encoder and Decoder / Compressor and Decompressor
CRND	Combined-Reverse-and-Normal-Direction scanning
$CRND^{-1}$	Inverse CRND
DC	dc coefficients of an image block
DCT	Discrete Cosine Transform
DCT^{-1}	Inverse DCT
DC DIFF	DC Differential
DC $DIFF^{-1}$	Inverse DC DIFF
DDP	Distorted DC Permutation
DDP^{-1}	Inverse DDP
DES	Data Encryption Standard
DWT	Discrete Wavelet Transform
HUFF DEC	Huffman Decoding
HUFF ENC	Huffman Encoding
HVS	Human Visual System
IJG	Independent JPEG Group
IPR	Intellectual Property Rights
JPEG	Joint Photographic Expert Group

PSNR	Peak Signal to Noise Ratio, A measurement of Quality
Quant	Quantization
$Quant^{-1}$	Inverse Quantization
RC4	A Stream Cipher designed by Ron Rivest of RSA Security of EMC Corporation
RGB	Red, Green, Blue color scheme
RLC	Run Length Coding
RLD	Run Length Decoding
RLE	Run Length Encoding
RSA	Public Key Encryption algorithm by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman
VLC	Variable Length Coding
YCbCr	A color scheme derived from RGB. Luminance, chrominance (blue) and chrominanace (red).
Zigzag	A coefficient scanning used in JPEG Encoding

CHAPTER 1

INTRODUCTION

1.1 Overview of Encryption Technology

Since the invention of ARPANET in 1967 until today, the use of open network for data transmission has been increasing as more individuals and companies get connected to the global networks. Today, with the availability of Broadband Internet and advancement in compression technology, huge digital media was now able to be transferred from one point to another in a very short time. This had also increased the number of internet usage for personal and business communication.

In business communication such as e-commerce, the data transfer needs to be secure enough to make sure that no unknown entities can actually peek the data before it arrived to the destination. In a very simple case, logging into a websites might give this unknown entity a capability to get the password and later on logging into the system and making inappropriate changes. This is one of the situations where the need for encryption takes place.

In the earlier days, encryption technologies were focusing more towards encrypting text messages. Today, encryption was able to be done towards rich multimedia content such as images, audio and videos. These rich multimedia are distributed widely especially in multimedia commerce applications such as Digital Library, Video on Demand, Video Conferencing and IPTV. Due to the popularity of these applications, the Intellectual

Property Rights (IPR) and secrecy of communication protections have become a very important issue. In order to cater this issue, two approaches were usually used. The first approach is by using Digital Watermarking and the second approach is by using Digital Encryption.

In digital watermarking, each media is assigned with a 'fingerprint' indicating the owner of the media, while in digital encryption the media is encrypted in such a way that the actual data is scrambled/ represented with non-actual value, which can be reversed in a decryption process. Digital Watermarking normally can be tampered or processed so that the 'fingerprint' can be removed. The copying of the media also could not be control, i.e. the viewer might not care where a video was copied from even the 'fingerprint' exist. While digital watermarking would be a good choice to protect IPR, digital encryption works better in protecting the secrecy of the media while being transferred or viewed by unintended recipient.

For images/videos, Block-based DCT compression was used widely in many photographic (real world) images and videos distribution. This technology was first used in JPEG [2] image compression and later in H.26x [6, 7, 8, 9] and MPEG-x [3, 4, 5] video compression. In video compression, intra-frame (I-Frame) is used to describe an image that was spatially compressed while inter-frame (P or B-Frame) is used to describe the temporally compressed image. The basic of I-Frame compression uses the same technique as in JPEG image compression. Based on this similarity, it is expected that encryption algorithm applied to JPEG image compression should also be able to be applied into MPEG-x and H.26x.