



**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**

**FK 2008 38**



**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 ini mengkaji tentang enkripsiyen bagi digital imej yang dilakukan terhadap imej JPEG. Dengan adanya algorithm-algoritma enkripsiyen bagi imej, imej JPEG dapat di selerakkan atau dienkríp sebelum disembarkan. Penerima tertentu akan diberikan kata kunci dekripsiyen 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 enkripsiyen ini melibatkan manipulasi pengimbasan 'zigzag' bagi JPEG dengan menggunakan 10 kombinasi pengimbasan 'zigzag' yang berbeza menggunakan CRND. Dengan menggunakan sifat-sifat pemampatan yang sama, enkripsiyen ini telah ditunjukkan berkemampuan untuk menghasilkan purata saiz fail image yang lebih kecil daripada yang terhasil daripada 'Baseline JPEG' dan teknik-teknik enkripsiyen yang lain. Telah ditunjukkan juga bahawa purata masa yang diambil untuk mengdekríp 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 3<sup>rd</sup> 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

	<b>Page</b>
<b>ABSTRACT</b>	iii
<b>ABSTRAK</b>	iv
<b>ACKNOWLEDGEMENT</b>	vi
<b>APPROVAL</b>	vii
<b>DECLARATION</b>	ix
<b>LIST OF TABLES</b>	xiii
<b>LIST OF FIGURES</b>	xiv
<b>LIST OF ABBREVIATIONS</b>	xxi
<b>CHAPTER</b>	
<b>I</b>	<b>INTRODUCTION</b> 1
	Overview of Encryption Technology 1
	Motivation & Research Problems 3
	Goal and Objectives 5
	Research Scopes 6
	Contribution and Dissertation Outline 7
<b>II</b>	<b>LITERATURE REVIEW</b> 9
	Overview of Digital Image Encryption 9
	Spatial Domain Image Encryption 12
	Frequency Domain Image Encryption 13
	Compressed Bitstream Domain 14
	Combinational Approach 15
	Summary of Comparison between Different Techniques 16
<b>III</b>	<b>METHODOLOGY</b> 20
	Overview on Digital Image and Color Spaces 21
	RGB Color Space 24
	YCbCr Color Space 25
	Jpeg Baseline Basic Operations 28
	Discrete Cosine Transform (DCT) 32
	Coefficients Quantization 33
	Zigzag Coefficients Scanning 34
	DC Differential 35
	Run-Length & Huffman Coding 36
	Method of Analysis 40



	JPEG Format Properties	41
	JPEG Data Input	42
	Comparison Metrics	43
	Development and Analysis of Existing Techniques	48
	Scanline Dispersal / Permutation	48
	Bit Scrambling	51
	Block Rotation	53
	Block Shuffling	56
	Coefficient Shuffling	59
	Coefficient Shuffling with Different Plane	63
	DC Coefficient Shuffling	65
	Naïve Algorithm	68
	Sign Encryption	70
	The Proposed Algorithms	74
	Combined Reverse and Normal Direction (CRND) Scanning	74
	Distorted DC Permutation	77
	Key Scheduling Algorithm	79
	CRND-DDP with KSA-based Permutation	80
	Simulator GUI Design	84
<b>IV</b>	<b>RESULTS AND DISCUSSION</b>	<b>86</b>
	Scanline Dispersal / Permutation	86
	Bit Scrambling	91
	Block Rotation	96
	Block Shuffling	101
	Coefficient Shuffling	106
	Coefficient Shuffling with Different Plane	110
	DC Coefficient Shuffling	114
	Naïve Algorithm	118
	Sign Encryption	122
	Combined Reverse and Normal Direction (CRND)	127
	Distorted DC Permutation	132
	CRND-DDP with KSA-based Permutation	137
	Overall Results Comparison	142
	Level of Degradation	144
	Encoding/ Encryption Speed	144
	Decoding/ Decryption Speed	145
	Encoded/ Encrypted File size	145
	Encoded/ Encrypted Image Quality	146
	Format Compliance	146
	Security Level	150
	Basic Attack Analysis	150



<b>V</b>	<b>CONCLUSION AND FUTURE WORKS</b>	155
	Conclusion	155
	Future Works	155
	<b>REFERENCES</b>	157
	<b>APPENDICES</b>	162
	<b>BIODATA OF THE AUTHOR</b>	249



## LIST OF TABLES

<b>Table</b>		<b>Page</b>
1	Comparison Table of Existing Techniques based on Literature	18
2	Luminance DC Coefficient Difference Huffman Codewords	38
3	Luminance AC Coefficients Huffman Codewords	39
4	Images used for simulations	42
5	Line Dispersal Encryption Results	90
6	Bit Scrambling Encryption Results	95
7	Block Rotation Encryption Results	100
8	Block Shuffling Encryption Results	105
9	Coefficient Shuffling Encryption Results	109
10	Coefficient Shuffling with Different Plane Encryption Results	113
11	DC Coefficients Shuffling Encryption Results	117
12	Naïve Algorithm Encryption Results	121
13	Sign Encryption Results	126
14	Combined-Reverse-and-Normal-Direction (CRND) Scanning Encryption Results	131
15	Distorted DC Permutation (DDP) Encryption Results	136
16	CRND-DDP with KSA-based Permutation Encryption Results	141
17	Average Percentage of Difference for Different Techniques	142
18	Format Compliance Comparison for the Proposed and Existing Techniques	147
19	Full Comparison Table between the Proposed and Existing Techniques	153



## LIST OF FIGURES

Figure		Page
1	Basic Image Encryption Illustration	11
2	Basic Image Decryption Illustration	11
3	Research Methodology Flow	20
4	Digital image representation example (a) Luminance image plane (b) 8x8 pixels image (c) 8x8 pixels values of “kids.jpg” at hair area.	23
5	RGB Color Cube	24
6	Image “kid.jpg” in (a) RBG color plane (b) R color plane (c) G color plane (d) B color plane	25
7	Image “kid.jpg” in (a) YCbCr color plane (b) Y color plane (c) Cb color plane (d) Cr color plane	27
8	JPEG Encoder Block Diagram	28
9	JPEG Decoder Block Diagram	29
10	JPEG Compression Illustration for an 8x8 block of “kid.jpg”	31
11	DCT Coefficients frequency distributions	33
12	Coefficient scanning with zigzag order	35
13	Run-Length Coding Illustration	36
14	Scanline Dispersal Illustration	48
15	Block Diagram for JPEG Encoding with Scanline Dispersal Encryption	49
16	Scanline Dispersal vs. Baseline JPEG with QF=65 for (a) “kid.jpg” (b) “lena.jpg”	50
17	Bit Scrambling process illustration	51
18	Block Diagram for JPEG Encoding with Bit Scrambling Encryption	52

19	Bit Scrambling Encryption with QF=65 for (a) “kid.jpg” (b) “lena.jpg”	53
20	Block Rotation with 90, 180 and 270 degree clockwise	54
21	Block Diagram for Block Rotation Encryption	55
22	Block Rotation Encrypted Image for (a) “kid.jpg” (b) “lena.jpg”	56
23	Block Shuffling process Illustration	57
24	Block Shuffling Encryption Block Diagram	58
25	Block Shuffling Encrypted Image (a) “kid.jpg” (b) “lena.jpg”	59
26	Coefficient Shuffling Technique Illustration	60
27	Coefficient Shuffling Encryption Block Diagram	62
28	Coefficient Shuffling Encryption for (a) “kid.jpg” (b) “lena.jpg”	62
29	Coefficient Shuffling with Different Plane Illustration	63
30	Coefficient Shuffling with Different Plane Block Diagram	64
31	Coefficient Shuffling with Different Plane Encrypted images for (a) “kid.jpg” (b) “lena.jpg”	65
32	DC Coefficient Shuffling Illustration	66
33	Block Diagram for DC Coefficient Shuffling	66
34	DC Shuffling Encrypted images for (a) “kid.jpg” (b) “lena.jpg”	67
35	Huffman Bitstream Naïve Encryption Illustration	68
36	Naïve Encryption of JPEG Huffman Bitstream Block Diagram	69
37	Naïve (RC4) Encrypted Images for (a) “kid.jpg” (b) “lena.jpg”	70
38	Sign Encryption Illustration	71
39	Sign Encryption of JPEG Images Block Diagram	72
40	Sign Encrypted image for (a) “kid.jpg” (b) “lena.jpg”	73





41	CRND Coefficients Scanning Illustrations	75
42	CRND Encryption & Decryption Block Diagram	75
43	CRND Encrypted image for (a) “kid.jpg” (b) “lena.jpg”	76
44	Illustration for DDP and Reconstruction of DC Differential without Inverse DDP	78
45	DDP Encrypted image for (a) “kid.jpg” (c) “lena.jpg”	79
46	The proposed JPEG Encryption using CRND-DDP with KSA-based Permutation Block Diagram	82
47	The proposed JPEG Decryption using CRND-DDP with KSA-based Permutation Block Diagram	82
48	CRND-DDP Encrypted Images for (a) “kid.jpg” (b) “lena.jpg”	83
49	GUI for Encryption Comparison Simulator	85
50	Fully Format Compliance Line Dispersal Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	87
51	Encryption/ Encoding Speed Comparison between Line Dispersal Algorithm and Baseline JPEG for QF=65	88
52	Decryption/ Decoding Speed Comparison between Line Dispersal Algorithm and Baseline JPEG for QF=65	88
53	Encrypted/ Encoded Filesize Comparison between Line Dispersal Algorithm and Baseline JPEG for QF=65	89
54	Decrypted/ Decoded Image Quality (PSNR) Comparison between Line Dispersal Algorithm and Baseline JPEG for QF=65	89
55	Partially Format Compliance Bit Scrambling Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	92
56	Encryption/ Encoding Speed Comparison between Bit Scrambling Algorithm and Baseline JPEG for QF=65	93
57	Decryption Speed Comparison between Bit Scrambling Algorithm and Baseline JPEG for QF=65	93



58	Encrypted/ Encoded Image File size Comparison between Bit Scrambling Algorithm and Baseline JPEG for QF=65	94
59	Decrypted Image Quality Comparison between Bit Scrambling Algorithm and Baseline JPEG for QF=65	94
60	Fully Format Compliance Block Rotation Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	96
61	Encryption/ Encoding Speed Comparison between Block Rotation Algorithm and Baseline JPEG for QF=65	97
62	Decryption/ Decoding Speed Comparison between Block Rotation Algorithm and Baseline JPEG for QF=65	98
63	Encrypted/ Encoded File size Comparison between Block Rotation Algorithm and Baseline JPEG for QF=65	98
64	Decrypted/ Decoded Image Quality (PSNR) Comparison between Block Rotation Algorithm and Baseline JPEG for QF=65	99
65	Fully Format Compliance Block Shuffling Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	101
66	Encryption/ Encoding Speed Comparison between Block Shuffling Algorithm and Baseline JPEG for QF=65	102
67	Decryption/ Decoding Speed Comparison between Block Shuffling Algorithm and Baseline JPEG for QF=65	103
68	Encrypted/ Encoded Image File size Comparison between Block Shuffling Algorithm and Baseline JPEG for QF=65	103
69	Decrypted/ Decoded Image Quality Comparison between Block Shuffling Algorithm and Baseline JPEG for QF=65	104
70	Fully Format Compliance Coefficient Shuffling Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	106
71	Encryption/ Encoding Speed Comparison between Coefficient Shuffling Algorithm and Baseline JPEG for QF=65	107
72	Decryption/ Decoding Speed Comparison between Coefficient Shuffling Algorithm and Baseline JPEG for QF=65	107



73	Decryption/ Decoding Speed Comparison between Coefficient Shuffling Algorithm and Baseline JPEG for QF=65	108
74	Decrypted/ Decoded Image Quality Comparison between Coefficient Shuffling Algorithm and Baseline JPEG for QF=65	108
75	Fully Format Compliance Coefficient Shuffling with Different Plane Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	110
76	Encryption/ Encoding Speed Comparison between Coefficient Shuffling with Different Plane and Baseline JPEG for QF=65	111
77	Decryption/ Encoding Speed Comparison between Coefficient Shuffling with Different Plane and Baseline JPEG for QF=65	111
78	Encrypted/ Encoded Image File size Comparison between Coefficient Shuffling with Different Plane Algorithm and Baseline JPEG for QF=65	112
79	Decrypted/ Decoded Image Quality (PSNR) Comparison between Coefficient Shuffling with Different Plane Algorithm and Baseline JPEG for QF=65	112
80	Fully Format Compliance DC Shuffling Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	114
81	Encryption/ Encoding Speed Comparison between DC Coefficient Shuffling Algorithm and Baseline JPEG for QF=65	115
82	Decryption/ Decoding Speed Comparison between DC Coefficient Shuffling Algorithm and Baseline JPEG for QF=65	115
83	Encrypted/ Encoded Image File size Comparison between DC Coefficient Shuffling Algorithm and Baseline JPEG for QF=65	116
84	Decrypted/ Decoded Image Quality (PSNR) Comparison between DC Coefficient Shuffling Algorithm and Baseline JPEG for QF=65	116
85	Partially Format Compliance Naïve (RC4) Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	118
86	Encryption/ Encoding Speed Comparison between Naïve (RC4) Algorithm and Baseline JPEG for QF=65	119



87	Decryption/ Decoding Speed Comparison between Naïve (RC4) Algorithm and Baseline JPEG for QF=65	119
88	Encrypted/ Encoded Image File size Comparison between Naïve (RC4) Algorithm and Baseline JPEG for QF=65	120
89	Decrypted/ Decoded Image Quality Comparison between Naïve (RC4) Algorithm and Baseline JPEG for QF=65	120
90	Fully Format Compliance Sign Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	122
91	Encryption/ Encoding Speed Comparison between Sign Encryption Algorithm and Baseline JPEG for QF=65	123
92	Decryption/ Decoding Speed Comparison between Sign Encryption Algorithm and Baseline JPEG for QF=65	124
93	Encrypted/ Encoded Image File size Comparison between Sign Encryption Algorithm and Baseline JPEG for QF=65	124
94	Decrypted/ Decoded Image Quality Comparison between Sign Encryption Algorithm and Baseline JPEG for QF=65	125
95	Fully Format Compliance CRND Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	127
96	Encryption/ Encoding Speed Comparison between CRND Algorithm and Baseline JPEG for QF=65	128
97	Decryption/ Decoding Speed Comparison between CRND Algorithm and Baseline JPEG for QF=65	129
98	Encrypted/ Encoded File size Comparison between CRND Algorithm and Baseline JPEG for QF=65	129
99	Decrypted/ Decoded Image Quality Comparison between CRND Algorithm and Baseline JPEG for QF=65	130
100	Fully Format Compliance DDP Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	133
101	Encryption/ Encoding Speed Comparison between DDP Algorithm and Baseline JPEG for QF=65	133
102	Decryption/ Decoding Speed Comparison between DDP Algorithm and Baseline JPEG for QF=65	134



103	Encrypted/ Encoded Image File size Comparison between DDP Algorithm and Baseline JPEG for QF=65	134
104	Encrypted/ Decoded Image Quality (PSNR) Comparison between DDP Algorithm and Baseline JPEG for QF=65	135
105	Fully Format Compliance CRND-DDP Encrypted Image of “lena.jpg” opened with Windows Picture and Fax Viewer	138
106	Encryption/ Encoding Speed Comparison between CRND-DDP Algorithm and Baseline JPEG for QF=65	138
107	Decryption/ Decoding Speed Comparison between CRND-DDP Algorithm and Baseline JPEG for QF=65	139
108	Encrypted/ Encoded Image File size Comparison between CRND-DDP Algorithm and Baseline JPEG for QF=65	139
109	Decrypted/ Decoded Image Quality Comparison between CRND-DDP Algorithm and Baseline JPEG for QF=65	140
110	Comparison Average of Percentage Difference between Different Techniques and Proposed Techniques in term of Encryption and Decryption Speed and File size	143
111	Encrypted Images for the Proposed Algorithms Compared to other Existing Algorithm for “lena.jpg”	149



## 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 <sup>-1</sup>	Inverse CRND
DC	dc coefficients of an image block
DCT	Discrete Cosine Transform
DCT <sup>-1</sup>	Inverse DCT
DC DIFF	DC Differential
DC DIFF <sup>-1</sup>	Inverse DC DIFF
DDP	Distorted DC Permutation
DDP <sup>-1</sup>	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 <sup>-1</sup>	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 Rivest, Adi Shamir and Leonard Adleman
VLC	Variable Length Coding
YCbCr	A color scheme derived from RGB. Luminance, chrominance (blue) and chrominance (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.

