Multimedia Encryption, Transmission and Authentication

Edited by

Othman Omran Khalifa, B.Sc. ,M.Sc., Ph.D
International Islamic University Malaysia

Aisha-Hassan Abdulla, B.Sc., M.Sc., Ph.D.,
International Islamic University Malaysia

Teddy Surya Gunawan, B.Sc., M.Sc., Ph.D.,
International Islamic University Malaysia

IIUM PRESS

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

Multimedia Encryption, Transmission and Authentication

Edited by

Othman Omran Khalifa, B.Sc. ,M.Sc., Ph.D
International Islamic University Malaysia

Aisha-Hassan Abdulla, B.Sc., M.Sc., Ph.D.,
International Islamic University Malaysia

Teddy Surya Gunawan, B.Sc., M.Sc., Ph.D.,
International Islamic University Malaysia

IIUM Press

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011

Cataloguing-in-Publication Data Perpustakaan Negara Malaysia

ISBN: 978-967-418-160-4

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

Contents

Chapter 5

Video Encryption Using Computation between H.264/AVC and AES Encryption Algorithm

[1]Mohamed Abomhara Omar Zakaria and Othman O. Khalifa [2]

[1]University of Malaya

[2]Electrical and Computer Engineering

International Islamic University Malaysia

5.1. Introduction

With the advanced development of the Internet and multimedia, it is easier for digital data owners to transfer multimedia documents across the Internet. Therefore, multimedia security has become one of the most aspects of communications with the continuous increase in the use online transmission. Some applications, such as TV broadcast and military applications require a special and reliable secure storage or transmission to be completely secured against theft, alteration or misuse. Furthermore, videoconferencing has become a daily characteristic of financial businesses. As it saves time, effort, and travel expenses for large companies. In such applications, digital video is compressed to a low bit rate while it is stored or transmitted [1]. There are several important standards such as MPEG-1, MPEG-2/h.262 and MPEG-4 have been developed for video compression, but with the target to double the coding efficiency and high reliability in video transmission. The Moving Picture Expert Group (MPEG) and the Video Coding Expert Group (VCEG) have developed a new standard that promises to outperform the earlier MPEG-4 and H.263 standard. H.244/AVC provides the most current balance between the coding efficiency, implementation complexity and cost [2][3][4].

Communication security for multimedia can be accomplished by means of standard symmetric key cryptography, as such media can be treated as binary sequence and the whole data can be encrypted using a cryptosystem such as AES or DES [3][5].

In general, when the multimedia data is static (not a real-time streaming) it can be treated as regular binary data and use the conventional encryption techniques. In the past, encrypting the entire video data using standard encryption algorithms was referred to as a Naïve approach [6]. This method can provide substantially high security but it incurs huge