

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
©IIUM Press, IIUM

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without any prior written permission of the publisher.

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

	Page No.
Part I- Multimedia Encryption and Transmission	
Chapter 1 Image and Video Coding Techniques <i>Sinzobakwira Issa and Othman O. Khalifa</i>	2
Chapter 2 Video Coding: MPEG standards <i>Othman O. Khalifa, Sinzobakwira Issa and Muhammad Umar Siddiqi</i>	7
Chapter 3 H.264/Advance Video Coding Standard <i>Othman O. Khalifa, Sinzobakwira Issa and Aisha-Hassan Abdulla</i>	16
Chapter 4 Development of Scalable Video Compression algorithm <i>Othman O. Khalifa, Sinzobakwira Issa and Mohamed Abomhara</i>	22
Chapter 5 Video Encryption Using Computation between H.264/AVC and AES Encryption Algorithm <i>Mohamed Abomhara Omar Zakaria and Othman O. Khalifa</i>	29
Chapter 6 Selective Video Encryption Algorithm Based on H.264/AVC and AES <i>Mohamed Abomhara Omar Zakaria and Othman O. Khalifa</i>	39
Chapter 7 Scalable Video Coding: A Review <i>Haris Al Qodri Maarif, Teddy Surya Gunawan, Othman O. Khalifa</i>	56
Chapter 8 JSVM Reference Software <i>Haris Al Qodri Maarif, Teddy Surya Gunawan, Othman O. Khalifa</i>	71
Chapter 9 Fast Mode Decision Algorithm <i>Haris Al Qodri Maarif, Teddy Surya Gunawan, Othman O. Khalifa</i>	78
Chapter 10 An Overview of Scalable Video Streaming <i>Mohammed Abumuala, Othman Khalifa and Aisha-Hassan A. Hashim</i>	88
Chapter 11 A Survey on Video Segmentation for Real-Time Applications <i>Haris Al Qodri Maarif, Sara Bilal, Teddy Surya Gunawan, Othman O. Khalifa</i>	100
Chapter 12 H.264/AVC Video Coding Tools and Functions <i>Sinzobakwira Issa, Othman O. Khalifa and Aisha-Hassan Abdulla</i>	107
Chapter 13 Speech Coding Techniques and Algorithms <i>Liban A. Kassim, Othman O. Khalifa, Teddy S. Gunawan</i>	116
Part II- Digital Watermarking	
Chapter 14 Digital Watermarking: An Overview <i>Othman O. Khalifa and Yusnita binti Yusof</i>	135
Chapter 15 Digital Watermarking : Related work <i>Othman O. Khalifa and Yusnita binti Yusof</i>	143
Chapter 16 Digital Watermarking Techniques and Methodologies <i>Othman O. Khalifa and Yusnita binti Yusof</i>	150
Chapter 17 Wavelet Transform for Digital Images Watermarking <i>Othman O. Khalifa, Yusnita Yusof</i>	156
Chapter 18 Wavelet Digital Watermarking System Design and Performance Evaluation <i>Othman O. Khalifa and Yusnita binti Yusof</i>	166
Chapter 19 An Improved Wavelet Digital Watermarking Software Implementation <i>Othman O. Khalifa and Yusnita binti Yusof</i>	175

Chapter 20	Adaptive Digital Watermarking System for Authentication of Intellectual Properties <i>Rashidah F. Olanrewaju, Azizah Abd Manaf and Akram Zeki</i>	182
Chapter 21	An Evaluation of Transform Domain Watermarking and its application to Intellectual Properties of images <i>Rashidah F. Olanrewaju, Othman O Khalifa, Aisha Hassan Hashim, A.A. Aburas and Akram Zeki</i>	192
Chapter 22	Applications of Digital Watermarking: Current and Future Trends <i>Othman O. Khalifa and Yusnita binti Yusof</i>	198
Chapter 23	State-Of-The-Art Digital Watermarking Attacks <i>Othman O. Khalifa and Yusnita binti Yusof</i>	204
Chapter 24	Performance evaluations of Digital Watermarking System <i>Yusnita binti Yusof and Othman O. Khalifa</i>	215
Part-III Multicast Transmission		
Chapter 25	Classifications Of Multicast Routing In Mobile Ad Hoc Networks <i>Mohammad Qabajeh, Aisha-Hassan A. Hashim, Othman O. Khalifa and Liana Qabajeh</i>	221
Chapter 26	Qualitive study on Multicast Routing Protocols In Manets <i>Mohammad Qabajeh, Aisha-Hassan A. Hashim, Othman O. Khalifa and Liana Qabajeh</i>	228
Chapter 27	Issues In Location-Based Multicast Routing In Manets <i>Mohammad Qabajeh, Aisha-Hassan A. Hashim, Othman O. Khalifa and Liana Qabajeh</i>	235
Chapter 28	Multicasting Challenges In Wireless Mesh Networks <i>M. L. Sanni, A. A. Hashim, F. Anwar and J. I. Daoud</i>	241
Chapter 29	Mobility Management In Multicast Environment <i>M. L. Sanni, A. A. Hashim, A. W. Naji and G. S. M. Ahmed</i>	249
Chapter 30	<i>Multicast Security</i> : Issues and Solutions <i>Mohammad Qabajeh, Aisha-Hassan A. Hashim and Othman O. Khalifa</i>	257
Chapter 31	Real-time MPEG-4 transmission over Wireless LAN <i>Abdirisag Mohammed Jama and Othman O. Khalifa</i>	263

Chapter 30

Multicast Security: *Issues and Solutions*

MOHAMMAD QABAJEH¹, AISHA-HASSAN A. HASHIM², OTHMAN O. KHALIF³

*ECE Dept, Fac. of Eng., International Islamic Univ. Malaysia (IIUM), Jalan Gombak, 53100
Kuala Lumpur, Malaysia.*

m_qabajeh@yahoo.com¹, aisha@iiu.edu.my², Khalifa@iiu.edu.my³, liana_tamimi@ppu.edu⁴

30.1. Introduction

The rapid growth of multicast communications has lead to wide use of the Internet for both individual and commercial distributed applications. Multicast communication is defined as an efficient way to distribute rich media to multiple users or participants simultaneously over the Internet. This is efficient in many applications including Internet video transmissions, news feeds, stock quotes, software updates, live multiparty conferencing, on-line video games and shared whiteboards. Thus, the need for secure transmission of multicast streams is considered as an important issue. However, potential security threats to multicast communications are similar to those encountered in unicast transmissions. These threats include the unauthorized creation, alteration ,destruction and illegitimate use of data. In case of multicast traffic, the inherent broad scope of a multicast session, the potential for attacks may be greater than that countered in unicast traffic. It is required to secure these services while maintaining the trade-off between efficiency and performance.

The field of multicast networking and related security issues is an important issue, which requires more efforts from research community. Multicast communication is becoming the basis for a growing number of applications. Therefore, it is important to provide security mechanisms for this type of applications. Various techniques to support multicast security have been proposed. The most common types of encryption are conventional (symmetric or single key) and public-key (asymmetric or two-key) encryption. The most popular symmetric encryption algorithms are data encryption standard (DES) and triple data encryption. The public-key encryption algorithms provide message authentication and integrity in addition to message confidentiality. The most popular public-key encryption algorithms are the RSA, Diffie-Hellman, digital signature standard (DSS) and the elliptic curve algorithms. In this chapter, a brief background about security threats facing multicast technology is provided.