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 14

Digital Watermarking: An Overview

Othman O. Khalifa and Yusnita binti Yusof
Electrical and Computer Engineering
International Islamic University Malaysia
yusnita@ucti.edu.my, khalifa@iium.edu.my

14.1 Introduction

Digital watermarking has been inspired from security concerns over multimedia contents due to the advances of computer technology. Nowadays, it is easy to obtain, manipulate, distribute and store these contents due to evolution of Internet, excellent multimedia tools and low-cost storage devices. Research community and industry has shown extensive interests in developing and implementing possible solutions via digital watermarking. Digital watermarking can be defined as the process of embedding a certain piece of information (technically known as watermark) into multimedia content including text documents, images, audio or video streams, where the watermark can be detected or extracted later to make an assertion about the data [1]. A generalized watermark model consists of watermark encoding and detection processes as shown in Figure 14.1 and Figure 14.2 [2]. The inputs to the embedding process are the watermark, the cover object and a secret key. The key is used to enforce security and to protect the watermark. The output of the watermarking scheme is the watermarked data. The channel for the watermarked data could be a lossy, noisy, unreliable channel. Thus the received data may be different from the original watermarked data. The inputs for extraction are the received watermarked data and the key corresponding to the embedding key. The output of the watermark recovery process is the recovered watermark [1][2][3].