



Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa



IIUM PRESS

2011



Topics in Coding, Cryptography and Information Security

Editors:

**Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa**



**IIUM Press
2011**

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.

Perpustakaan Negara Malaysia

Cataloguing-in-Publication Data

Mohammad Umar Siddiqi, Sigit Puspito Wigati Jarot and Othman Omran
Khalifa: Topics in Coding, Cryptography and Information Security

ISBN: 978-967-418-169-7

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

Topics in Coding, Cryptography and Information Security

Contents

List of Contributors	ii
Editorial Introduction	vi

PART I: SOURCE CODING

1. Performance Analysis of Image Data Compression using Zero-Tree Wavelet Transform	2
<i>Othman O. Khalifa, Emir Tabakovic, Zlatko Memisevic and Aisha-Hassan Abdullah</i>	
2. Scalable and Robust Streaming Video System Challenges	12
<i>Othman O. Khalifa, Sinzobakwira Issa and Mohammad Umar Siddiqi</i>	

PART II: CHANNEL CODING

3. Golay Codec: An Overview	23
<i>Othman O. Khalifa</i>	
4. Reed-Muller Codes: An Overview	35
<i>Othman O. Khalifa</i>	
5. Viterbi Decoder: A Review and Implementation	42
<i>Noorainani Ainina Bt. Md Noor Albakri and Othman O. Khalifa</i>	

6.	Zigzag Codes: High Rate Low Complexity Iterative Codes <i>Sigit P.W. Jarot</i>	53
7.	Convolutional Coded OFDM in Broadband Mobile Communication <i>Sigit P.W. Jarot</i>	66
8.	Channel Coding Techniques in Mobile Communication Systems <i>Othman O. Khalifa and Rashid A. Saeed</i>	77
9.	Channel Coding in CDMA 2000 <i>Othman O. Khalifa</i>	85
10.	Channel Coding in Mobile WiMAX <i>Rashid A. Saeed and Othman O. Khalifa</i>	91
11.	Turbo Codes: An Error Correction Technique for 4G <i>Mosharraf Hussain Masud and Mohammad Umar Siddiqi</i>	99
12.	Combined Source Channel Decoding for Image Transmission over Noisy Channels <i>Jalel Chebil</i>	108

PART III: CRYPTOGRAPHY AND INFORMATION SECURITY

13.	Cryptographic Boolean Functions: Transform Domain Perspective <i>Hashim Mohamed Rafiq and Mohammad Umar Siddiqi</i>	120
14.	Implementation of RSA Algorithm <i>Hafizul Azizi Rasid, Mohd Azmi Jabar and Othman O. Khalifa</i>	141
15.	GSM Security: Problems and Solutions <i>Rashid A. Saeed and Othman O. Khalifa</i>	152
16.	Recent Approaches to Wireless Physical Layer Security <i>M. Tahir, Sigit P.W. Jarot and M.U. Siddiqi</i>	161
17.	Securing OFDM-based Systems from the Physical Layer <i>Sigit P.W. Jarot</i>	169
18.	Simulation of Artificial Noise based Physical Layer Security <i>Muhammad Izzat bin Zurkiple and Sigit Puspito Wigati Jarot</i>	174

19.	Secure IPv6 Address Generation	183
	<i>Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot</i>	
20.	Video Streaming and Encrypting Algorithms	190
	<i>Mohammed Abumualala, Othman O. Khalifa, and Aisha-Hassan A. Hashim</i>	
21.	Wireless IP Camera based on Motion Detection Surveillance System	217
	<i>Zeeshan Shahid and Khaizuran Abdullah</i>	
22.	Design of Mobile Phone Jammer	223
	<i>Fauzun Abdullah Asuhaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah</i>	

Index

Chapter 7

Convolutional Coded OFDM

in Broadband Mobile Communication¹

Sigit P.W. Jarot

7.1. Introduction

OFDM is one of the promising systems to support the generation broadband mobile communication system, due to its capability to mitigate inter-symbol interference in high bit rate transmission over mobile radio channel. OFDM based systems have been used in many applications of wired and wireless communication systems. OFDM is also the modulation scheme that has been official selected for the several new standards in broadband wireless such as LTE, 802.11 and WiMax.

Error correcting coding across OFDM subcarriers, in conjunction with frequency interleaving, is one of powerful methods in improving the performance of OFDM systems, by taking advantage of frequency diversity. The importance of channel coding and interleaving in an OFDM system is very well known, and there have been several studies for various applications, such as, DAB [3], [4], wireless ATM [5], satellite communication [6], wireless home link [7], and so forth. These varieties of study show that the coding strategy and its aspects very much depend on the applications and the channel environments of the system. Since convolutional coding is one of the error correction coding that is most widely used in OFDM systems so far, it is important to clarify the performance of the convolutional coding and the frequency diversity effect, in a broadband mobile radio channel. In this chapter, we present evaluations of the performance of convolutional coded OFDM system. Coding rate, delay interval, Doppler frequency, interleaving span and number of sub-carriers are used for evaluation parameters.

This chapter presents the performance evaluation of convolutional coding focusing on the frequency interleaving effects in OFDM over 80 MHz broadband mobile radio channel, for various coding rate, delay interval, Doppler frequency, and number of subcarriers. Computer simulation demonstrates that frequency interleaving span has to be changed when the path interval changes, in order to keep the system performance. This chapter is organized as follows. Section 7.2 gives explanation on system model, including the frequency interleaving method, and the channel model assumed for performance evaluation. Section 7.3 presents the

¹ Portions of the material have appeared previously in [1], [2] and [10].