



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 11

Turbo Codes:

An Error Correction Technique for 4G

Mosharrof Hussain Masud and Mohammad Umar Siddiqi

11.1. Introduction

The first generation (1G) and second generation (2G) wireless mobile communication systems were designed primarily for voice transmission around in 1980 [1]. The 1G used analog frequency modulation technique where the subsequent generations have been using digital communication techniques for example, time division multiplexing (TDM), frequency division multiplexing (FDM) or the code division multiple access (CDMA). The recently introduced third generation (3G) wireless system has designed for high data transmission over the 2G systems that includes interactive multimedia services in the wireless networks. Mobile users and their demands are increasing dramatically over the globe day by day. However, the users are not satisfied with the coverage of 384 kbps peak rate in a wide area network (WAN) and limited coverage for 2 Mbps. Therefore, high data transmission is one of the design challenges for fourth generation (4G) that has been implemented in some countries in the world. The 4G will be the ultimate telecommunication solution for different technologies including GSM, UMTS, WiFi, WiMAX etc. that facilitates the heterogeneous environments. To provide enhanced QoS, turbo coding technique has been used in 4G networks. In this chapter it will be discussed briefly about 4G technology, the encoding and decoding methods of 4G technology by using Turbo Coding, and its performances as well.

11.2. Overview of 4G

4G (also known as Beyond 3G), an abbreviation for Fourth-Generation, is a term used to describe the next complete evolution in wireless communications. A 4G system will be a complete replacement for current networks and be able to provide a comprehensive and secure IP solution where voice, data, and streamed multimedia can be given to users on an "Anytime, Anywhere" basis, with a much higher data rates than previous generations [2].