



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 <i>Othman O. Khalifa, Emir Tabakovic, Zlatko Memisevic and Aisha-Hassan Abdullah</i>	2
2. Scalable and Robust Streaming Video System Challenges <i>Othman O. Khalifa, Sinzobakwira Issa and Mohammad Umar Siddiqi</i>	12

PART II: CHANNEL CODING

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

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>Hashum 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
Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot
20. Video Streaming and Encrypting Algorithms 190
Mohammed Abumuala, Othman O. Khalifa, and Aisha-Hassan A. Hashim
21. Wireless IP Camera based on Motion Detection Surveillance System 217
Zeeshan Shahid and Khaizuran Abdullah
22. Design of Mobile Phone Jammer 223
Fauzum Abdullah Asuhaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah

Index

Chapter 9

Channel Coding in CDMA2000

Othman O. Khalifa

9.1. Introduction

Today it is necessary to have powerful coding scheme that gives reliable data and multimedia service and bi-transmission in mobile communication systems. Wireless communication systems are making a rapid variety of communication services to everybody, anywhere, anytime. Peoples want multimedia facilities from their mobile handset. But it requires high data rate, hi efficiency and many more technical things, which are available in third generation. (CDMA) so the CDMA technology makes existing mobile handset more efficient and attractive. In wireless systems there are two categories, frequency and time. Division by frequency, where each pair of communicators is allocated a part of the spectrum for all of the time, this called Division Multiple Access (FDMA). While Division by time, where each pair of communicators is allocated all or at least a large part of the spectrum for part of the time and that called Time Division Multiple Access (TDMA). However, in Code Division Multiple Access (CDMA), each communicator will be allocated the entire spectrum all of the time.

9.2. Overview of CDMA Coding

The world's first CDMA2000 networks were introduced in Korea in October 2000, with 144kbit/s data rates to subscribing customers and delivering nearly twice the voice capacity that operators experienced with their cdmaOne (IS-95) systems. The success of the CDMA2000 1X system has encouraged many providers in the Americas and Asia to use it in their plans. In CDMA a unique spreading codes to spread the baseband data before transmission is used. The signal is transmitted through a channel, which is below noise level. The receiver able to despread the wanted signal, which is passed through a narrow bandpass filter using a correlator. Therefore, unwanted signals will not be despread and will not pass through the filter. Codes take the form of a carefully designed one/zero sequence produced at a much higher rate than that of the baseband data [1] The rate of a spreading code is referred to as chip rate rather than bit rate. The CDMA2000 Network Architecture is shown in Figure 9.1