



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 8

Channel Coding Techniques in Mobile Communication Systems

Othman O. Khalifa and Rashid A. Saeed

8.1. Introduction

The aim of any communication schemes is to provide error-free data transmission. In a communication system, information can be transmitted by analog or digital signals. In a wireless communication channel, the signals transmitted by the terminals suffer from a variety of degradations, such as additive white Gaussian noise (AWGN), shadowing, and multi-path fading and can be altered or lost during transmission due to channel noise. In all wireless systems would be impossible without channel coding. Therefore, an Error control is required to detect and possibly correct errors by introducing redundancy to the stream of bits to be sent to the channel. The Channel Encoder will add bits to the message bits to be transmitted systematically. After passing through the channel, the Channel decoder will detect and correct the errors [1][2][3].

8.2. Common Communications Channels

Various communication channels can provide a connection between a transmitter and its destination. Common Communications channels are to receiver with a wire such as coaxial cables, ethernet cables, and twisted-pair wires and optical. Wireline channels are more private and much less prone to interference. Simple wireline channels connect a single transmitter to a single receiver: a point-to-point connection as with the telephone. Listening in on a conversation requires that the wire be tapped and the voltage measured. Some wireline channels operate in broadcast modes: one or more transmitter is connected to several receivers. One simple example of this situation is cable television. Computer networks can be found that operate in point-to-point or in broadcast modes. Wireless channels are much more public, with a transmitter's antenna radiating a signal that can be received by any antenna sufficiently close enough such as mobiles, Wi-Fi Technology, Bluetooth, etc. In contrast to wireline channels where the receiver takes in only the transmitter's signal, the receiver's antenna will react to electromagnetic radiation coming from any source. This feature has two faces: The smiley face says that a receiver can take in transmissions from any source, letting receiver electronics select wanted signals and disregarding others, thereby allowing portable transmission and reception, while the frowny face says that interference and