



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>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 3

Golay Codec: An overview

Othman O. Khalifa

3.1. Introduction

There are different types of codes in coding theory. One category of codes is linear codes. One manipulates these codes via the theorems and methods of linear algebra. Two other codes worth noting are Hamming codes and Golay codes. Hamming codes are designed to correct any single error, while Golay codes corrects three or fewer errors. The Golay code was used to encode pictures from Jupiter and Saturn. The idea of Error Correcting Codes came with the onslaught of computer technology. In the late 1930s Bell Telephone Laboratories built one of the first mechanical relay computers. This computer is unlike anything currently in use. However, the mechanical relay computer while executing a program was prone to errors like today computers. In fact, in 1947 Hamming conducted calculations on the mechanical relay computer at Bell Telephone Laboratories and found himself constantly re-running his programs due to computer halts. Error-correcting codes were discovered in mid-20th century after Richard W. Hamming got irritated by his computer stopping when it encountered an error, causing him to realize that if his computer could detect errors it should be able to locate and correct them. He devised ways to encode the input so that the computer could correct isolated errors and continue running, and his inquiries led him to discover what are now called Hamming codes. Another key player in the birth of Error-Correcting Codes is Marcel J. E. Golay. Golay was an engineer at Signal Corps Engineering Laboratories at Fort Monmouth. He became interested in Error-Correcting Codes after reading a paper published by Shannon on the (7,4) Hamming Code. This publication sparked Golay's interest: Shannon's paper gave Golay an entirely new perspective: a geometric perspective of information and coding theory. Golay set out to find perfect single-error-correcting-codes. Codes that have every word associated to a codeword. Therefore these codes correct single errors without any "extra" redundancy. Golay started out to prove first that a perfect code exists. In 1958 Golay stated a necessary condition for the existence of a perfect code:

$$n = ((p^m)^k - 1)/(p^m - 1) \tag{3.1}$$

of length n using p^m symbols for some integer k .

In 1948, Marcel Golay introduced some linear codes, denoted by G_{23} , G_{24} , G_{11} , G_{12} that are now called Golay codes. The codes G_{24} is a binary linear (24,4096,8)