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

©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


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
   Othman O. Khalifa, Emir Tabakovic, Zlatko Memisevic and Aisha-Hassan Abdullah 2

2. Scalable and Robust Streaming Video System Challenges
   Othman O. Khalifa, Sinzobakwira Issa and Mohammad Umar Siddiqi 12

PART II: CHANNEL CODING

3. Golay Codec: An Overview
   Othman O. Khalifa 23

4. Reed-Muller Codes: An Overview
   Othman O. Khalifa 35

5. Viterbi Decoder: A Review and Implementation
   Noorainani Aminah Binti Md Noor Albakri and Othman O. Khalifa 42
6. Zigzag Codes: High Rate Low Complexity Iterative Codes
   Sigit P.W. Jarot
   53

7. Convolutional Coded OFDM in Broadband Mobile Communication
   Sigit P.W. Jarot
   66

8. Channel Coding Techniques in Mobile Communication Systems
   Othman O. Khalifa and Rashid A. Saeed
   77

9. Channel Coding in CDMA 2000
   Othman O. Khalifa
   85

10. Channel Coding in Mobile WiMAX
    Rashid A. Saeed and Othman O. Khalifa
    91

11. Turbo Codes: An Error Correction Technique for 4G
    Mosharraf Hussain Masud and Mohammad Umar Siddiqi
    99

12. Combined Source Channel Decoding for Image Transmission over Noisy Channels
    Jalel Chebil
    108

PART III: CRYPTOGRAPHY AND INFORMATION SECURITY

13. Cryptographic Boolean Functions: Transform Domain Perspective
    Hashim Mohamed Rafiq and Mohammad Umar Siddiqi
    120

14. Implementation of RSA Algorithm
    Hafizul Azizi Rasid, Mohd Azmi Jabar and Othman O. Khalifa
    141

15. GSM Security: Problems and Solutions
    Rashid A. Saeed and Othman O. Khalifa
    152

16. Recent Approaches to Wireless Physical Layer Security
    M. Tahir, Sigit P.W. Jarot and M.U. Siddiqi
    161

17. Securing OFDM-based Systems from the Physical Layer
    Sigit P.W. Jarot
    169

18. Simulation of Artificial Noise based Physical Layer Security
    Muhammad Izzat bin Zurkiple and Sigit Puspito Wigati Jarot
    174
19. Secure IPv6 Address Generation
   Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot

20. Video Streaming and Encrypting Algorithms
   Mohammed Abumuala, Othman O. Khalifa, and Aisha-Hassan A. Hashim

21. Wireless IP Camera based on Motion Detection Surveillance System
   Zeeshan Shahid and Khaizuran Abdullah

22. Design of Mobile Phone Jammer
   Fauzun Abdullah Astuhaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah

Index
Chapter 10
Channel Coding in Mobile WiMAX

Rashid A. Saeed and Othman O. Khalifa

10.1. Introduction

In general, WiMAX (Worldwide Interoperability for Microwave Access) is a metropolitan access technique, which not only provides wireless access, but also expands the coverage of wired networks. This facilitates network access for remote or suburban areas. In 2004, the IEEE 802.16d standard was published for Fixed Wireless Access (FWA) applications. In December 2005 the IEEE ratified the 802.16e amendment, which aimed to support Mobile Wireless Access (MWA) with seamless network coverage [1]. Consequently, as 802.16e is commercialized, WiMAX will become a promising scheme to evolve FWA to MWA. At present there is particular interest in mobile WiMAX, since this offers data transfer rates that exceed those of current 3G [2]. In this chapter we discussed mobile WiMAX channel code; concatenated Reed-Solomon-convolutional code (RS-CC), Block turbo coding (BTC) and Convolutional turbo codes (CTC). Each has four channel coding steps: randomization, forward error correction (FEC) interleaving, and modulation. A pseudorandom noise (PN) sequence generator is used to randomize each FEC data block.

10.2. Overview of (Mobile) WiMAX

In general, WiMAX (Worldwide Interoperability for Microwave Access) is a metropolitan access technique, which not only provides wireless access, but also expands the coverage of wired networks. This facilitates network access for remote or suburban areas. In 2004, the IEEE 802.16d standard was published for Fixed Wireless Access (FWA) applications. In December 2005 the IEEE ratified the 802.16e amendment, which aimed to support Mobile Wireless Access (MWA) with seamless network coverage [1]. Consequently, as 802.16e is commercialized, WiMAX will become a promising scheme to evolve FWA to MWA. At present there is particular interest in mobile WiMAX, since this offers data transfer rates that exceed those of current 3G [2].

The mobile WiMAX air interface adopts Scalable Orthogonal Frequency Division Multiple Access (SOFDMA) for improved multi-path performance in non-line-of-sight (NLOS) environments. Radio resource allocation and sharing (also known as channel loading) plays an important roll in optimizing the performance of WiMAX-based OFDMA systems [3]. Radio resources allocation is a major challenge for relay systems. Resource allocation such as power control has long