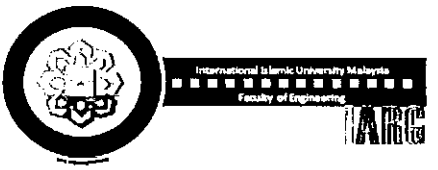
Topics in Coding, Cryptography and Information Security

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

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

PART II: CHANNEL CODING

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

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

5. Viterbi Decoder: A Review and Implementation 42
   Noorainani Ainina Bt. Md Noor Albakri and Othman O. Khalifa

6. Zigzag Codes: High Rate Low Complexity Iterative Codes 53
Sigit P.W. Jarot

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

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

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

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

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

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

PART III: CRYPTOGRAPHY AND INFORMATION SECURITY

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

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

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

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

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

18. Simulation of Artificial Noise based Physical Layer Security 174
Muhammad Izzat bin Zurkiple and Sigit Puspito Wigati Jarot

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
Fauzun Abdullah Asuhaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah

Index

Chapter 1

Performance Analysis of Image Data Compression using Zero-Tree Wavelet Transform

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

1.1. Introduction

With the growth of technology and the entrance into the digital age, the world has found itself amid a vast amount of information. Dealing with such enormous amount of information can often present difficulties. Digital information must be stored and retrieved in an efficient manner, in order to be practical. Wavelet compression is one way to deal with this problem. The row data (graphics, audio and video) requires considerable storage capacity and transmission bandwidth. Despite rapid progress in mass-storage density, processor speeds, and digital communication system performance, demand for data storage capacity and data-transmission bandwidth continues to outstrip the capabilities of available technologies. The recent growth of data intensive multimedia-based web applications have not only sustained the need for more efficient ways to encode signals and images but have made compression of such signals central to storage and communication technology [1, 2, 3, 4].

1.2. Compression Fundamentals

Compressions rely on two main strategies: getting rid of redundant information (redundancy reduction) and getting rid of irrelevant information (irrelevancy reduction).Redundancy reduction is often used when the image is being encoded (or re-encoded). It looks for patterns and repetitions that can be expressed more efficiently. If, for example, there are 25 black pixels in a row, it is clearly better to record the information for one pixel and state that the next 24 are all the same, than to record each pixel separately. This particular example is known as run-length encoding (RLE).Irrelevancy reduction aims to remove or alter information that makes little or no difference to the perception of the image. This usually happens prior to the encoding and involves a transformation of the image. Some of an image's color information, for example, can be safely simplified without being perceptible to the human eye. However, when carried to an extreme this sort of compression becomes visibly obvious and compromises the quality of the image.