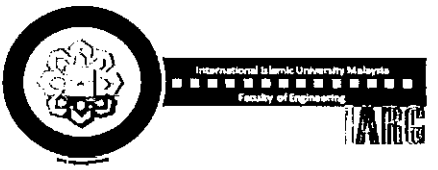
Topics in Coding, Cryptography and Information Security

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 21

Wireless IP Camera Based on Motion Detection Surveillance System

Zeeshan Shahid and Khaizuran Abdullah

21.1. Introduction

Camera surveillance has been a popular security tool nowadays. The new breakthroughs in technology, security cameras are more effective than ever before. Banks, retailed stores, and countless other end-users depend on the protection provided by video surveillance. While analog closed circuit television (CCTV) systems were once the norm, they can be expensive, requiring complicated installations and constant upkeep. Fortunately, advances in digital technology have made video surveillance systems far more cost-effective, flexible, and simple to operate. Security systems using IP (Internet Protocol) cameras are easy to install and maintain, and can be customized and scaled to perfectly match your specific needs.

Video surveillance has a number of benefits that are indispensable for today's society: it helps to prevent theft and vandalism of public and private places, prevent violence and crime, protect children and even improve customer image and trust on a particular vendor [1]. The aspects of video surveillance are pattern recognition, motion detection and tracking system [2].

Performance of the IP surveillance cameras is generally evaluated at encoding speed, video resolution, video frame bit rates and distortion, and power dissipation. Among these characteristics, the video resolution, the compression ratio and the frame rate are the most important to the users of the video surveillance systems because these features are highly related to the image quality and the network bandwidth. Moving Picture Experts Group (MJPEG) and MPEG4 Visual (Part 2 of the MPEG-4 group of standards) are the common standards used for image compression. However, both the MJPEG and the MPEG4 visual encoders are not efficient enough in terms of the compression ratio and image quality [3].

The availability and cost of high resolution surveillance camera, along with the growing need for remote controlled security, has been a major driving force in this field. A growing amount of information increases the demand on processing and tagging this information for subsequent rapid retrieval. To satisfy this demand, many researchers are working to find improvements and better solutions in video analytics, which is the semantic analysis of video data, to reduce running time and total cost of surveillance systems [4].

The advent of high resolution digital IP surveillance cameras, connected via the internet to a remote security monitoring station, enables a new approach that