Topics in Coding, Cryptography and Information Security

Editors:
Mohammad Umar Siddiqi
Sgit 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
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

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

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

9. Channel Coding in CDMA 2000
   Othman O. Khalifa

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

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

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

PART III: CRYPTOGRAPHY AND INFORMATION SECURITY

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

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

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

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

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

18. Simulation of Artificial Noise based Physical Layer Security
    Muhammad Izzat bin Zurkiple and Sigit Puspito Wigati Jarot
19. Secure IPv6 Address Generation
   Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot
   183

20. Video Streaming and Encrypting Algorithms
   Mohammed Abumuala, Othman O. Khalifa, and Aisha-Hassan A. Hashim
   190

21. Wireless IP Camera based on Motion Detection Surveillance System
    Zeeshan Shahid and Khaizuran Abdullah
   217

22. Design of Mobile Phone Jammer
    Fauzun Abdullah Asuaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah
   223

Index
Chapter 22

Design of Mobile Phone Jammer

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

22.1. Introduction

Mobile Phone Jammer is a device used to prevent cellular phones from receiving
signals from base stations. When used, the jammer effectively disables cellular
phones. These devices can be used in practically any location, but are found pri-
marily in places where a phone call would be particularly disruptive because si-
lence is expected. In order to jam the phone, it is important to know the frequency
of service provider in Malaysia as instructed by Malaysian Communication Mul-
timedia Corridor (MCMC). Only jammer that transmits the same frequency as
mobile phone will be able to jam the signal.

Apart from frequency, the transmit power of RBS also plays important role in
the signal strength. By knowing this power we will know what is the suitable
power transmits by the jammer to block the entire mobile phone signal. The jam-
mer need to have same or more power than the phone to jam the signal.

If the jammer has wide frequency ranges, it might block the signal of other ap-
lication like radar. Since this jammer is only concern to jam mobile phone only,
the design of selective frequency jammer can be put into consideration. This selec-
tive jammer will choose the frequency to jam the mobile phone since the frequen-
cies are different depending on the service provider. Thus we would suggest de-
veloping this current jammer to selective frequency jammer that will increase the
efficiency of the jammer.