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
   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
    Hashum 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 183
   Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot

20. Video Streaming and Encrypting Algorithms 190
    Mohammed Abumual, 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 Asshaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah

Index
Chapter 20

Video Streaming and Encrypting Algorithms

Mohammed Abumualal, Othman O. Khalifa, and Aisha-Hassan A. Hashim

20.1. Introduction

The growth of popular web sites serving multimedia contents has led to the increase of video streaming applications. The challenges of multimedia data encryption come from two facts. First, the multimedia data is large (for example, the size of a two-hour MPEG-1 video is about 1 GB). Secondly, multimedia data needs to be processed in real time (for example, the data rates of MPEG-2 can go up to 40 Mbps or more). Processing vast amount of data in very short time puts great burden on video codecs, storage space requirements and network communications. Heavy-weight encryption and decryption algorithms (during or after encoding phase) will aggravate the problem and increase the latency. For commercial applications such as pay-per-view video, very expensive attacks of the scrambled multimedia data are not interesting to the attackers because most videos are not as valuable as military secrets or financial information [1]. In such cases, the information rate is very high, but the information value is very low [1]. The cost to break such encryption code is much higher than the cost to buy the programs. Security is a trade-off between the cost of the data being protected and the cost attackers pay to get that data. The costs of a multimedia security system include the amount of investment by data provider and the payment required for customer service.

20.2. Image and Video Coding

Image and video encryption are of course closely related by the fact that raw video data consists of a sequence of still images. However, compressed video like the MPEG format is composed of different types of data which can be treated in specific ways by special encryption schemes. In MPEG-1 video coding model [2], a video is composed of a sequence of group of pictures (GOPs). Each GOP is a series of I, P and B pictures. I pictures are intraframe coded without any reference to other pictures. P pictures are predicatively coded using a previous I or P picture. B pictures are bidirectionally interpolated from both the previous and following I and/or P pictures. The relative frequency of occurrence of I, P and B pictures can be controlled by the applications.

Each picture is divided into macroblocks. A macroblock is a $16 \times 16$ pixel array. Macroblocks belonging to I pictures are spatially encoded. Those belonging