



---

# **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 <i>Othman O. Khalifa, Emir Tabakovic, Zlatko Memisevic and Aisha-Hassan Abdullah</i>	2
2. Scalable and Robust Streaming Video System Challenges <i>Othman O. Khalifa, Sinzobakwira Issa and Mohammad Umar Siddiqi</i>	12

### PART II: CHANNEL CODING

3. Golay Codec: An Overview <i>Othman O. Khalifa</i>	23
4. Reed-Muller Codes: An Overview <i>Othman O. Khalifa</i>	35
5. Viterbi Decoder: A Review and Implementation <i>Noorainani Ainina Bt. Md Noor Albakri and Othman O. Khalifa</i>	42

6.	Zigzag Codes: High Rate Low Complexity Iterative Codes <i>Sigit P.W. Jarot</i>	53
7.	Convolutional Coded OFDM in Broadband Mobile Communication <i>Sigit P.W. Jarot</i>	66
8.	Channel Coding Techniques in Mobile Communication Systems <i>Othman O. Khalifa and Rashid A. Saeed</i>	77
9.	Channel Coding in CDMA 2000 <i>Othman O. Khalifa</i>	85
10.	Channel Coding in Mobile WiMAX <i>Rashid A. Saeed and Othman O. Khalifa</i>	91
11.	Turbo Codes: An Error Correction Technique for 4G <i>Mosharraf Hussain Masud and Mohammad Umar Siddiqi</i>	99
12.	Combined Source Channel Decoding for Image Transmission over Noisy Channels <i>Jalel Chebil</i>	108

### **PART III: CRYPTOGRAPHY AND INFORMATION SECURITY**

13.	Cryptographic Boolean Functions: Transform Domain Perspective <i>Hashum Mohamed Rafiq and Mohammad Umar Siddiqi</i>	120
14.	Implementation of RSA Algorithm <i>Hafizul Azizi Rasid, Mohd Azmi Jabar and Othman O. Khalifa</i>	141
15.	GSM Security: Problems and Solutions <i>Rashid A. Saeed and Othman O. Khalifa</i>	152
16.	Recent Approaches to Wireless Physical Layer Security <i>M. Tahir, Sigit P.W. Jarot and M.U. Siddiqi</i>	161
17.	Securing OFDM-based Systems from the Physical Layer <i>Sigit P.W. Jarot</i>	169
18.	Simulation of Artificial Noise based Physical Layer Security <i>Muhammad Izzat bin Zurkiple and Sigit Puspito Wigati Jarot</i>	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 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  
*Fauzum Abdullah Asuhaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah*

## **Index**

# Chapter 5

## Viterbi Decoder: A Review and Implementation

Noorainani Ainina Bt. Md Noor Albakri and Othman O. Khalifa

### 5.1. Introduction

Viterbi decoding was developed by Andrew J. Viterbi, a founder of Qualcomm Corporation. His seminar paper on the technique is "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm," published in *IEEE Transactions on Information Theory*, Volume IT-13, pages 260-269, in April, 1967. There are 3 types of decoding algorithms which are Viterbi decoding, Sequential decoding and Threshold decoding. However, Viterbi decoding is the most often used for decoding convolutional codes. Therefore, it is important to understand the encoding part first, which is convolutional encoding before proceed to decoding algorithm. However, the Viterbi decoding is still the main focus in this chapter. Convolutional encoding with Viterbi decoding is a Forward Error Correction (FEC) technique that is particularly matched to a channel in which the transmitted signal is corrupted mainly by Additive White Gaussian Noise (AWGN). For years, convolutional encoding with Viterbi decoding has been predominant for FEC technique used in space communication.

### 5.2. Convolutional Coding

Convolutional codes are widely used to encode digital data before transmission through noisy or error-prone channels. During encoding,  $k$  input bits are mapped to  $n$  output bits to give a rate  $k/n$  coded bit stream. The encoder consists of a shift register of  $kL$  stages, where  $L$  is described as the constraint length of the code.

In order to describe the convolutional encoding process, it is much easier to go through an example [3]. Figure.5.1 shows a simple convolutional coder suitable for incorporating forward error correction into a transmitted message.

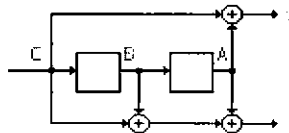


Fig. 5.1. Typical Convolutional coder