International Islamic University Malaysia
Faculty of Engineering
IARG

Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa

IIUM PRESS
2011

International Islamic University Malaysia
Faculty of Engineering

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

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

PART I: SOURCE CODING

PART II: CHANNEL CODING

PART III: CRYPTOGRAPHY AND INFORMATION SECURITY

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.

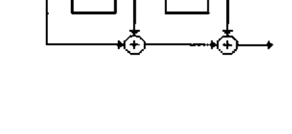

Fig. 5.1. Typical Convolutional coder