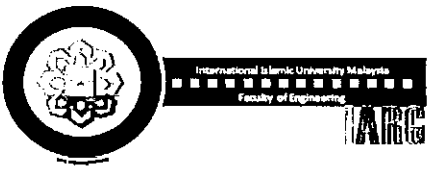
Topics in Coding, Cryptography and Information Security

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

Chapter 20

Video Streaming and Encrypting Algorithms

Mohammed Abumuala, 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 codec, 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 low1]. 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 × 16 pixel array. Macroblocks belonging to I pictures are spatially encoded. Those belonging