

10007
1007628
911850

UNIVERSITI TEKNOLOGI MARA

**EFFICIENT SELECTIVE
ENCRYPTION SCHEMES TO
SECURE VIDEO DATA AND
MOVING OBJECTS INFORMATION
FOR HEVC/H.265 USING
ADVANCED ENCRYPTION
STANDARD**

MOHAMMED AHMED MOHAMMED SALEH

Thesis submitted in fulfillment
of the requirements for the degree of
Doctor of Philosophy

Faculty of Electrical Engineering

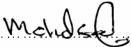
June 2016

AUTHOR'S DECLARATION

I declare that the work in this thesis was carried out in accordance with the regulations of Universiti Teknologi MARA. It is original and is the results of my own work unless otherwise indicated or acknowledged as referenced work. This thesis has not been submitted to any other academic institution or non-academic institution for any degree or qualification.

I, hereby, acknowledge that I have been supplied with the Academic Rules and Regulations for Post Graduate, Universiti Teknologi MARA, regulating the conduct of my study and research.

Name of Student : Mohammed Ahmed Mohammed Saleh
Student I.D. No. : 2010539481
Programme : Doctor of Philosophy – EE990
Faculty : Electrical Engineering
Thesis Title : Efficient Selective Encryption Schemes to Secure Video
Data and Moving Objects Information for HEVC/H.265
Using Advanced Encryption Standard

Signature of Student : .....
Date : June 2016

ABSTRACT

Due to the huge growth in communication and digital technologies in support of multimedia sharing, video security has recently attracted the attention of researchers. Since video data representation takes up a large amount of data, it has to be minimized before being transmitted through the channels. To do so, that data has to be subjected to a compression process. This process is performed according to the video coding standard (video compression). There have been different types of video coding standards, but High Efficiency Video Coding (HEVC) is the latest video coding standard being introduced. Whereas, in the field of video security, there are several types of encryption algorithms utilized by researchers, such as Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES) and Advanced Encryption Standard (AES). All of those encryption algorithms are classified as asymmetric and symmetric algorithms. Since the video data is still huge even after the compression process, most researchers apply their encryption approaches on a selective part of the video data whereas the compression process is performed by a different type of coding standard. Most of the existing video encryption methods are not adequate to secure the video contents against the modern security attacks and eavesdropping. Furthermore, those methods have become impractical especially for the video sharing through the internet using the new coding standard HEVC because of the limited resources on the devices. Wherein those approaches have fallen into some limitations, such as low-security level, high computational overhead, not maintaining the bitstream compliance and result in the increase of video bitrate. In this thesis, three lightweight selective encryption approaches have been developed to provide a visual video and moving objects protection of HEVC bitstream that can be utilized for real-time video streaming, while maintaining the computational cost and video bit rate. Those approaches named as, Encryption for Absolute Coefficient Level, Encryption of Intra Prediction Mode, and Encryption of Motion Vector Difference (MVD). In the first and second methods, the visual video information is secured by encrypting limited transformed coefficients using AES algorithm. Whereas the third method is dedicated to secure the moving object information in the video by exploiting the syntax element of motion vector difference, and this method is encrypted by AES as well. The experimental results for the first and the second of the proposed approaches has shown that a reliable security level of visual video perception was provided, in addition to having no observed effects on compression efficiency. Furthermore, from the test results of the third method, the moving objects information was encrypted and at the same time, the compression efficiency was maintained. The proposed schemes provide a trade-off between encryption reliability, flexibility, and computational complexity, where the encryption time in the first scheme increased by 13% and zero in the second and the third schemes, and the increase in bitrate is 1% in the first and the third schemes and zero in the second scheme. Thus, these methods can be considered as feasible techniques to secure the HEVC/H.265 bitstream, and can be applied in real-time applications.

TABLE OF CONTENTS

	Page
CONFIRMATION BY PANEL OF EXAMINERS	ii
AUTHOR'S DECLARATION	iii
ABSTRACT	ix
ACKNOWLEDGMENT	v
TABLE OF CONTENTS	vi
LIST OF TABLES	xi
LIST OF FIGURES	xiii
LIST OF SYMBOLS	xvi
LIST OF ABBREVIATIONS	xvii
CHAPTER ONE: INTRODUCTION	1
1.1 Motivation	2
1.2 Problem Statement	3
1.3 Objectives	4
1.4 Contributions	4
1.5 Thesis Outline	5
CHAPTER TWO: LITERATURE REVIEW	8
2.1 Introduction	8
2.2 Video Compression (Coding) Standards	8
2.2.1 Video Coding	9
2.2.2 Modern Video Coding Architecture	9
2.2.3 MPEG-4	11
2.2.4 H.264/AVC and MPEG-4 Part 10	12
2.2.5 HEVC	12
2.2.5.1 Coding Tree Units and Coding Tree Block Structure	13
2.2.5.2 Intra-Frame Prediction	15
2.2.5.3 Inter-Frame Prediction	16
2.2.5.4 Entropy Coding	16

CHAPTER ONE

INTRODUCTION

In tandem to the rapid spread in the use of internet and telecommunication technologies, information sharing is gaining importance. Recently, end users are conscious about their sensitive information that can be shared through the enormous internet network, especially after observing the increasing trends of security attacks [1][2][3]. Whereas according to the Shodan reports [4], there are over 28800 publicly accessible and potentially vulnerable cameras (surveillance cameras, wireless color video IP cameras) have been registered until 2013 [5]. On the other hand, the number of video sharing applications is rapidly growing, caused by the smart devices and the internet revolution. According to Cisco, mobile video sharing will occupy more than 69 percent of smart mobile data traffic by 2019, where the total global percentage of the smart mobile traffic will be 97 percent by 2019 [6].

To maintain the bandwidth requirements, the researchers have been trying to find a technique to minimize the data size that represents the video information. This technique is called video coding or video compression, wherein, it has been developed and continuously improved since 1960 by different engineering organizations such as International Telecommunication Union (ITU), and Motion Picture Expert Group (MPEG). That technique started as the analog videophone system in 1960, it evolved to become the High Efficiency Video Coding (HEVC) in 2013.

Data security has attracted the attention of people since 4000 BC to secure the sensitive information in data communication. Various cryptography systems have been used to protect information against cipher attacks and snooping. Through the centuries, cryptography systems have been adapted and improved to provide the required security at different stages of technology developments, where the use of the modern cryptography systems started from World War I.

Since the video is made up of a large data size, securing that data while transmitting it over internet network, can be regarded as a big challenge in terms of video streaming requirements, data communications, data retrieval, video contents compression and resource of hardware requirements. Thus, securing of video data have been performed by different encryption techniques during different developmental stages of video compression and data encryption techniques.