



شبكة المعلومات الجامعية

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Ain Shams University Information Network

جامعة عين شمس

شبكة المعلومات الجامعية
@ ASUNET



شبكة المعلومات الجامعية

جامعة عين شمس

التوثيق الالكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأفلام قد أعدت دون أية تغيرات



يجب أن

تحفظ هذه الأفلام بعيدا عن الغبار

في درجة حرارة من ١٥-٢٥ مئوية ورطوبة نسبية من ٢٠-٤٠%

To be Kept away from Dust in Dry Cool place of
15-25- c and relative humidity 20-40%



شبكة المعلومات الجامعية التوثيق الالكتروني والميكرو فيلم

بعض الوثائق الأصلية تالفة

بالرسالة صفحات لم ترد بالاصل

SECURED VIDEO STREAM ACROSS WIRELESS NETWORKS

BY

Eng. Mohamed Aly Elsharkawy

A dissertation submitted to the
Faculty of Computers and Information
Cairo University

In Partial Fulfillment of the requirements for the
DEGREE OF DOCTOR OF PHILOSOPHY
in
Information Technology

Under the supervision of

Prof. Dr. Imane Aly Saroit Ismail

A. Prof. Dr. Hesham N. Elmahdy

Dr. Abdelatif Ahmed ElKouny

**FACULTY OF COMPUTERS AND INFORMATION
CAIRO UNIVERSITY-EGYPT**

June 2007

Secured video stream across wireless networks

By

Eng. Mohamed A. ELsharkawey

**A dissertation submitted to the
Faculty of Computers and Information
Cairo University**

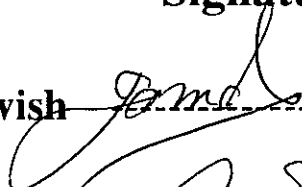
**In partial fulfillment of the
Requirements for the degree of Ph.D. in
Information Technology**

Approved by

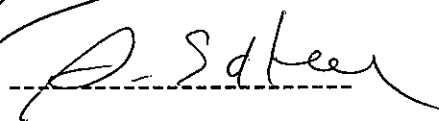
Examination Committee

Signature

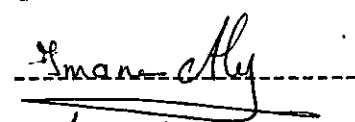
Prof. Dr. Mohamed Gamal-Eldin Darwish



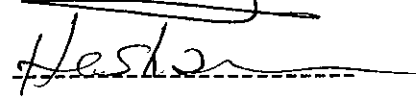
Prof. Dr. Abdel-badeeh Mohamed Salem



Prof. Dr. Imane Aly Saroit Ismail



Prof. Dr. Hesham N. Elmahdy Mohamed



FACULTY OF COMPUTER AND INFORMATION

CAIRO UNIVERSITY-EGYPT

July - 2007

I certify that this work has not been accepted in substance for any academic degree and is not being concurrently submitted in candidature for any other degree.

Any portions of this dissertation for which I am indebted to other sources are mentioned and explicit references are given.

Mohamed Aly Elsharkawy

ACKNOWLEDGEMENT

It is a pleasure to express my sincere gratitude to my supervisors:

Prof. Imane Aly Saroit Ismail, A. Prof. Hesham N. Elmahdy, Dr. Abdelatif A. ElKouny, for their encouragement and valuable expert guidance throughout this work. It has been a great honor and privilege to work with them.

I am deeply grateful my mother for her valuable help, kind support throughout the duration of this work.

My sincere appreciation to my wife and kids Ahmed, Omar and Hoda for their moral support.

Mohamed Aly Elsharkawy

ABSTRACT

Recent advances in digital media technologies have created a large number of secured multimedia applications. Those applications and services are often deployed in a wireless network environment. Generally, three main contexts play the main roles in streaming secured video stream across wireless network. These contexts include video compression techniques, adaptation of transmitted video stream according to the available bandwidth, and the applied security techniques.

There are several video coding techniques that compress video sequences to bit streams. These coding techniques exploit spatial and temporal redundancy to achieve high compression ratios. However, they are usually unaware about the channel conditions and client resources. Thus, transcoding of video contents was introduced as a key technology to make this possible. The role of the transcoder is to adapt the contents of a video stream to fit the client capabilities. Additionally, Transcoding is performed according to the change in the available resources. Transcoders are introduced to tailor the same media contents to different derived users. However, transmitting the multimedia contents across wireless network makes them vulnerable to malicious attacks. Thus, the security concerns, if not addressed appropriately, will potentially prevent or delay the wide dissemination of the multimedia applications.

Most of transcoders are focused on how to perform the adaptation more efficiently without considering the real time constraints and the involved security issues. Although, there are some recent works on multimedia security, there is a leak between the comprehensive treatment of the design, the implementation of security functions, and the transcoder functionalities.

This dissertation presents a new model for the three tier transcoding architecture known as Two-Way Secure Scalable Stream (TW-SSS). The objective of that model is to minimize the transcoding process while upholding the security aspect of the stream. In addition, a novel security technique is proposed. This technique is mainly designed to provide more security on higher levels of applications (for examples; pay TV and military applications). A novel and simple scrambling method was proposed too. Both of the proposed security technique and the scrambling method are based on the scalability. The scalability is introduced as the only solution used to prepare the pre-compressed stream of

each movie frame in the separate layers that are suited for adaptation. Several methods are established in order to achieve this scalability concept.

In the dissertation a new method to represent each frame in scalable layers is proposed. Moreover, this dissertation includes the comparison results between the TW-SSS and other used techniques. In addition, the results of implementing the developed security techniques according to the selective encryption equation of the off-line-scenario are deployed and analyzed.

TABLE OF CONTENTS

ACKNOWLEDGEMENT.....	I
ABSTRACT.....	II
LIST OF TABLES.....	VIII
LIST OF FIGURES.....	IX
LIST OF ABBREVIATIONS.....	XII
CHAPTER 1 INTRODUCTION.....	2
1.1 INTRODUCTION	2
1.2 MOTIVATIONS.....	3
1.3 DISSERTATION OBJECTIVES.....	5
1.4 DISSERTATION OUTLINES	6
1.4.1 Chapter 2: Image and Video Compression Systems	6
1.4.2 Chapter3: Image and Video Data Encryption.....	6
1.4.3 Chapter4: The proposed Video Transcoding Architecture	7
1.4.4 Chapter5: The Proposed Encryption Algorithms.....	7
1.4.5 Chapter 6: Conclusion and Future Work	7
CHAPTER 2 IMAGE AND VIDEO COMPRESSION SYSTEMS.....	9
2.1 INTRODUCTION	9
2.2 IMAGE AND VIDEO DATA	10
2.3 COLOR SPACES	11
2.4 FUNDAMENTALS OF IMAGE/VIDEO CODING	12
2.4.1 Transformation Process	13
2.4.1.1 Discrete Cosine Transform (DCT).....	13
2.4.1.2 Discrete Wavelet Transform (DWT).....	16
2.4.2 Quantization Process.....	19
2.4.2.1 Quantization Techniques	22
2.4.3 Zig-zag Reordering	24
2.4.4 Entropy Coding	25
2.5 DECODING PROCESS.....	26

2.6 MOTION ESTIMATION AND COMPENSATION.....	27
2.6.1 Frame Prediction	28
2.6.2 Motion-Vector	29
2.6.3 Block Matching Evaluation.....	30
2.7 SCALABILITY	32
2.7.1 Rate-Scalable Strategies	33
2.7.2 Types of Scalability	34
2.7.3 Proposed Method for Generating Scalable Layers	35
2.7.3.1 The proposed Masking Method	35
2.8 CODING SCHEMES	36
2.8.1 DCT Based System.....	37
2.8.1.1 Motion JPEG	37
2.8.1.2 MPEG Video Coding (Mpeg-1, 2, 4)	39
2.8.2 Wavelet-based Systems (MJPEG-2000)	40
2.8.3 MJPEG Versus MJPEG2000	42
CHAPTER 3 IMAGE AND VIDEO DATA ENCRYPTION.....	46
3.1 INTRODUCTION	46
3.2 SECURITY PLACES	47
3.3 A BRIEF INTRODUCTION TO MODERN CRYPTOGRAPHY	48
3.3.1 Classical Cryptosystems	48
3.3.1.1 Data Encryption Standard (DES).....	50
3.3.1.2 Rivet Shamir Adleman public key Cipher (RSA)	51
3.4 PROPERTIES OF IMAGE/VIDEO ENCRYPTION TECHNIQUES	52
3.5 FULL ENCRYPTION VERSUS SELECTIVE ENCRYPTION (SE).....	53
3.6 SELECTIVE ENCRYPTION TECHNIQUES OF IMAGE/VIDEO	54
3.6.1 Selective Encryption of uncompressed Image/Video.....	55
3.6.2 Selective Encryption of compressed Image/Video.....	58
3.6.2.1 Permutation Algorithm.....	58
3.6.2.2 Secure MPEG Algorithm	59
3.6.2.3 Video Encryption Algorithm by Qiao and Nahrstedt	60
3.6.2.4 Video Encryption Algorithms by Shi, Wang and Bhargava,	62
3.6.2.5 Video Encryption Methods by Alattar, Al-Regib and Al-Semari	66

3.6.2.6 Format-Compliant Configurable Encryption by Wen et al.....	67
3.6.2.7 Selective Scrambling Algorithm by Zeng and Lei.....	69
3.7 INTERPLAY BETWEEN COMPRESSION AND ENCRYPTION	71
3.7.1 Optimal Cost of Confidential Visual Data Transmission.....	72
CHAPTER 4 THE PROPOSED VIDEO TRANSCODING ARCHITECTURE 76	
4.1 INTRODUCTION	76
4.2 TRANSCODING PARAMETERS	77
4.3 TRANSCODING TECHNIQUES.....	78
4.3.1 Conventional Transcoding Techniques.....	78
4.3.1.1 Bit-Rate Reduction Technique.....	80
4.3.1.2 Spatial Resolution Reduction Transcoding	83
4.3.1.3 Temporal Resolution Reduction Transcoding	85
4.3.2 Scalable Stream Transcoding.....	87
4.3.3 Comparison Transcoding Techniques	89
4.4 TWO-WAY SCALABLE STREAM TRANSCODER (TW_SS) MODEL...90	
4.4.1 TW_SS Server:	92
4.4.1.1 Encoding Module	92
4.4.1.2 The Dynamic Shared List.....	96
4.4.1.3 Packetization Module	96
4.4.2 The TW_SS Transcoder Components:	98
4.5 IMPLEMENTATION OF TWO-WAY SCALABLE STREAM MODEL	
(TW_SS).....	100
4.5.1 Software Description	100
4.5.2 Hardware Description	101
4.5.3 Operations Scenario	101
4.5.4 Software Implementation of the TW_SS.....	102
4.5.4.1 CPU Time Measurements with different Frame-Scale	106
4.5.4.2 Throughput Measurements with different Frame-Scale.....	107
4.6 COMPARISONS OF TW-SS VERSUS SS TRANSCODERS	108
4.6.1 Q-scale Measurements.....	108
4.6.1.1 CPU usage of the TW-SS Versus SS Transcoder	108
4.6.1.2 Throughput of the TW-SS Versus SS Transcoder	111

4.6.2 Frame-Scale Measurements	113
4.6.2.1 CPU Usage of the TW-SS Versus SS Transcoder	113
4.6.2.2 Throughput of the TW-SS Versus SS Transcoder	115
CHAPTER 5 THE PROPOSED ENCRYPTION ALGORITHMS.....	118
5.1 INTRODUCTION	118
5.2 APPLICATION SCENARIOS FOR THE SELECTIVE ENCRYPTION OF VISUAL DATA	119
5.2.1 Off-Line Scenario.....	120
5.2.2 On-Line Scenario	121
5.3 SCALABLE LAYERS ENCRYPTION.....	122
5.4 THE PROPOSED SELECTIVE ENCRYPTION ALGORITHMS	126
5.4.1 The Basic Keys Generation.....	126
5.4.2 The Proposed A Symmetric Block Cipher Algorithm	129
5.4.2.1 A Symmetric Key Generation.....	130
5.4.2.2 A symmetric Block Cipher Operation.....	130
5.4.3 The Proposed Key-Based Scrambling Method	135
5.4.3.1 Scrambling Keys Generation	135
5.4.3.2 The Scrambling Operation	136
5.5 EXPERIMENTAL RESULTS	140
5.5.1 Q-Scale Measurements	141
5.5.1.1 The CPU-Time Comparison	141
5.5.1.2 Throughput Comparison	143
5.5.2 The Frame Scale Measurements	144
5.5.2.1 The CPU-Time Comparison	144
5.5.2.2 Throughput Comparison	146
5.5.3 Testing Single Frame.....	146
CHAPTER 6 CONCLUSION AND FUTURE WORK.....	151
6.1 CONCLUSIONS	151
6.2 FUTURE WORKS.....	155
REFERENCES.....	157
OUTPUT OF THIS DISSERTATION	165