



AIN SHAMS UNIVERSITY

FACULTY OF ENGINEERING

Electronics and Communications Engineering Department

A Thesis

Submitted in partial fulfillment of the requirements of the degree of
Master of Science in Electrical Engineering

Design of Video Signals Encryption/ Decryption Using FPGA

Submitted by

Ismail Kamal Ismail El-Sayed

B.Sc. of Electrical Engineering

(Electronics and Communications Engineering)

Military Technical College, 2003

Supervised By

Prof.Dr. Adel EL-Hennawy

Dr. Ehab El-Sehely

Cairo 2013



AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING

Name: **Ismail Kamal Ismail El-Sayed**
Thesis: Design of Video Signals Encryption/ Decryption Using FPGA
Degree: Master of Science in Electrical Engineering

Supervisors Committee

Prof.Dr. Adel Ezzat El-Hennawy
Electronics and Communications Engineering Dept., Faculty
of Engineering, Ain Shams University.

Dr. Ehab El-Sehely
Avionics Research Center

Examiners' Committee

Name: Ismail Kamal Ismail El-Sayed
Thesis: Design of Video Signals Encryption/ Decryption Using FPGA
Degree: Master of Science in Electrical Engineering

Title, Name and Affiliation	Signature
-----------------------------	-----------

Prof.Dr. Ismail Mohamed Hafez Chairman, Electronics and Communications Engineering Dept., Faculty of Engineering, Ain Shams University.	
---	-------

Prof.Dr. Hassan Ahmed Al-Ghitani Dean, Faculty of Engineering, MIU University.	
--	-------

Prof.Dr. Adel Ezzat El-Hennawy Electronics and Communications Engineering Dept., Faculty of Engineering, Ain Shams University.	
--	-------

Date: 10/10/2013.

STATEMENT

This dissertation is submitted to Ain Shams University for the degree of Master of Science in Electrical Engineering (Electronics and Communications Engineering).

The work included in this thesis was carried out by the author at the Electronics and Communications Engineering Department, Faculty of Engineering, Ain Shams University, Cairo, Egypt.

No part of this thesis was submitted for a degree or a qualification at any other university or institution.

Name: Ismail Kamal Ismail El-Sayed

Signature:

Date:

Curriculum Vitae

Name of Researcher:	Ismail Kamal Ismail El-Sayed
Date of Birth:	1/3/1981
Place of Birth:	Cairo, Egypt
First University Degree:	B.Sc. in Electrical Engineering
Name of University:	Military Technical College
Date of Degree:	June 2003

ACKNOWLEDGEMENT

All praise is due to Allah, Most Merciful, Lord of the Worlds, Who taught man what he knew not. I would like to thank God Almighty for bestowing upon me the chance, strength and ability to complete this work.

I would first like to thank my supervision committee for their great help and dedication through the duration of this work. I learned so many valuable things from them, but above all, they taught me how to be devoted to research and how to help others. I am in great debt to Dr. Ehab El-Sehely for being under his mentorship since early in my undergraduate years through my graduation project and my professional career as well as this thesis.

I would also like to thank Assoc. Prof. Gen. Maj. (R) Ahmed Elsaid Abdalla for his continuous support and enthusing help and very helpful comments during work and thesis writing. And Eng. Mohamed Fawaz, Eng. Haytham Abdalla, Eng. Hosam Yosry, Eng. Ahmed Fathy, Eng. Abd-elrahman Elakhdar from Egyptian Armed Force for their support and encouragement.

Last but not least, I would like to thank my wife and my parents. Their patience, care, and love are what guided me through whole life.

ABSTRACT

The demand for efficient, real time video cryptography systems has grown over the last decades from a problem that concern only military authority, to the primary concern of both civilian and military authorities. Civilian applications like health services (telemedicine, medical records etc.), commercial subscription television channel are demanding for video security for the legal personal data protection requirements or for commercial concerns.

In this dissertation the design and implementation of a modified Electronic Code Book (ECB) mode for the Rijndael Advanced Encryption Standard (AES) real time video encryption algorithm is developed. Field Programmable Gate Array (FPGA) is selected as an implementation platform for its advantages in both encryption process and video data process. In proposed system, selective video encryption scheme is applied where all active video data are encrypted and other inactive video data and embedded video timing reference data are left unencrypted to achieve the format compliance with highest level of security.

A self-synchronized cipher key mechanism based on the embedded video timing reference signals is designed and implemented to overcome the security leakage in case of using block cipher algorithms (like Rijndael) in ECB mode of operation and to reduce the possibilities of cryptanalytic attacks which are used to recover the encryption key from the cipher texts (like brute force attacks).

Besides, different video cryptography system evaluation criteria are discussed like throughput, cryptographic security, visual degradation, etc. that are used to evaluate the proposed system.

In order to accommodate the integrity nature and huge size of video signals during high level testing of the proposed system, four different tests are applied. Tests include the use of internally generated video pattern for system stimulation before using external NTSC video-camera source.

Key words: FPGA, video encryption, selective encryption, AES (Rijndael).

CONTENTS

Chapter 1	1
Video Cryptography Systems	1
1.1 Introduction.....	1
1.2 Problem Statement	3
1.3 Desirable Features in the Required Cryptosystem.....	4
1.4 Work Contribution	5
1.5 Thesis Organization	5
Chapter 2	7
Digital Video Signals	7
2.1 Introduction.....	7
2.2 Analog Video Signal.....	8
2.3 Analog Video Encoding Systems	10
2.4 Digitizing Analog Video Signals.....	12
2.4.1 Video Sampling.....	12
2.4.2 Video Data Format	14
2.4.3 Digital Video Data Rate	18
2.5 Color Spaces	18
2.6 Conclusion	23
Chapter 3	25
Video Cryptography.....	25
3.1 Introduction.....	25

3.2	Basic Cryptography Concepts	26
3.3	The Rijndael Advanced Encryption Standard (AES)	30
3.3.1	Encryption Process.....	33
3.3.1.1	SubBytes Transformation.....	35
3.3.1.2	ShiftRows Transformation	36
3.3.1.3	MixColumns Transformation	37
3.3.1.4	Add Round Key	38
3.3.2	Decryption Process	39
3.3.2.1	Inverse ShiftRows Transformation	42
3.3.2.2	Inverse SubBytes Transformation	42
3.3.2.3	Add Round Key	43
3.3.2.4	Inverse MixColumns	44
3.3.3	Key Expansion Algorithm	45
3.3.4	Modes of Operation	45
3.3.5	Implementation Architectures.....	52
3.3.6	Architecture Optimization.....	57
3.4	Video Encryption Schemes.....	57
3.4.1	Full Video Encryption.....	57
3.4.2	Partial Video Encryption.....	58
3.5	Cryptanalysis.....	59
3.6	Implementation Platforms.....	60
3.7	Conclusion	62
Chapter 4		63

Design and Implementation of Real Time Video Cryptography System	63
4.1 Introduction.....	63
4.2 System Design Strategy and Goals.....	64
4.2.1 Implementation Platform Selection	65
4.2.2 The System Constraints	66
4.2.3 The Clock Management Scheme	67
4.2.4 Target FPGA Device Selection.....	70
4.2.5 Video Encryption Scheme	73
4.2.6 Encryption Algorithm	73
4.2.6.1 Mode of Operation	73
4.2.6.2 Implementation Architecture.....	74
4.2.7 Key Scheduling Process.....	75
4.2.8 Used Software	75
4.3 Proposed System Architecture.....	75
4.3.1 Digital Clock Manager (DCM)	80
4.3.2 Video Color Bar Generator	81
4.3.3 TVP5150 Initialization Module	85
4.3.4 Video Transmitter Interface Module.....	85
4.3.4.1 Key Calculator.....	89
4.3.4.1.a Synch Detector.....	94
4.3.4.1.b Pixels and Lines Grouping Matrix	94
4.3.4.1.c 16-bit to 128-bit Converter	95
4.3.4.1.d Frame ID Inserter.....	95

4.3.4.1.e User Key Masking	96
4.3.4.1.f SAV Signal Generator.....	96
4.3.4.2 Video Encryptor	96
4.3.4.2.a ITU-R BT.656 Interface	100
4.3.4.2.b Data Load Shaping Logic	101
4.3.4.2.c AES Cipher Block	102
4.3.4.2.d Parallel-128 to Serial-8 Converter.....	105
4.3.4.2.e ITU-R BT.656 Formatter.....	106
4.3.5 Video Receiver Interface Module	107
4.3.5.1 Key Calculator.....	112
4.3.5.2 Video Decryptor	112
4.3.6 Video Display Module	119
4.3.6.1 Video Frame Grabber.....	121
4.3.6.2 SDRAM Write Pointer Generator	124
4.3.6.3 Dual Port Controller	125
4.3.6.4 SDRAM Controller	127
4.3.6.5 SDRAM Read Pointer Generator	128
4.3.6.6 VGA Controller	128
4.4 System Testing	130
4.5 System Evaluation.....	139
4.5.1 Latency	139
4.5.2 Throughput	140
4.5.3 Design Area.....	141

4.5.4 Visual Degradation (VD)	142
4.5.5 Encryption ratio (ER)	142
4.5.6 Compression Friendliness (CF).....	143
4.5.7 Format Compliance (FC)	143
4.5.8 Cryptographic Security (CS).....	143
4.6 Conclusion.....	143
Chapter 5	145
Conclusion and Future work	145
References	148

List of Figures

Figure 1.1: Command and Control System.....	2
Figure 1.2: UAV Role in Situation Awareness Systems	3
Figure 2.1: Temporal and Spatial Sampling	8
Figure 2.2: Interlaced Vs Progressive Scanning.....	10
Figure 2.3: Composite Video Signal.....	11
Figure 2.4: Video Sampling Formats.....	13
Figure 2.5: ITU-R BT656 4:2:2 Digital Video Standard.....	17
Figure 2.6: RGB Color Cubes.....	19
Figure 2.7: $Y C_b C_r$ Components of an Image	21
Figure 2.8: Implementation of Color Space RGB to $Y C_b C_r$ Conversion	23
Figure 3.1: Two Parties Communication Using Secret Key Encryption.....	28
Figure 3.2 : Two Parties Communication Using Public Key Encryption.....	29
Figure 3.3: AES (Rijndael) Encryption Process Overview	31
Figure 3.4: AES (Rijndael) Decryption Process Overview	32
Figure 3.5 : AES Encryption Process	34
Figure 3.6: Row Transformation Implementation	37
Figure 3.7 : AES-MixColumns Operation Overview	38
Figure 3.8: Add Round Key Process.....	39
Figure 3.9: AES Decryption Process	41
Figure 3.11: Add Round Key Implementation	44
Figure 3.12: Mix Columns Implementation.....	45
Figure 3.13 ECB Mode of Operation.....	47

Figure 3.14: CBC Mode of Operation.	48
Figure 3.15: CFB Mode of Operation.....	49
Figure 3.16: OFB Mode of Operation.....	50
Figure 3.17: CTR mode of operation.....	51
Figure 3.18: AES Basic Implementation Architecture	52
Figure 3.19: Loop Unrolling Architecture	53
Figure 3.20: Sub-Pipelining Architecture	54
Figure 3.21: Outer Pipelining Architecture	55
Figure 3. 22: Partial Pipelining with Sub-Pipelining Architecture.....	56
Figure 3.23: Naïve Encryption Scheme	58
Figure 3.24: Selective Encryption Scheme	59
Figure 4.1: Systems Operating In Single and Multiple Clock Domains	67
Figure 4.2: Data Input Setup and Hold Times	68
Figure 4.3: Metastability in Multi-Clock Designs	69
Figure 4.4: Xilinx Spartan III Family Structure.....	71
Figure 4.5: XESS XSA3S-1000 Board + XST	72
Figure 4.6: Encryption Leakage in ECB Mode	74
Figure 4.7: Secured Video Link System Architecture	77
Figure 4.8: Proposed System Architecture	78
Figure 4.9: System Design Hierarchy	79
Figure 4.10: DCM Blocks	81
Figure 4.11: SMPTE EG 1-1990 Color Bars	82
Figure 4.12: Behavioral Simulation of Video Color Bar Generator Module	84
Figure 4.13: Block Diagram of Video Transmitter Interface Module.....	86
Figure 4.14: Behavioral Simulation of Video Transmitter Interface Module	88
Figure 4.15: NTSC Video Frame Data Blocks	90
Figure 4.16: Block Diagram of Key Calculator Sub-Module.....	91

Figure 4.17: Behavioral Simulation of Key Calculator Sub-Module	93
Figure 4.18: Pixels and Lines Grouping Logic Circuit.....	94
Figure 4.19: InData Signal Structure	95
Figure 4.20: Serial 16-Bits To Parallel 128-Bits Converter	95
Figure 4.21: Video Encryptor Operation	97
Figure 4.22: Behavioral Simulation of Video Encryptor Sub-Module.....	99
Figure 4.23: ITU-R BT.656 Interface Block	100
Figure 4.24: ITU-R BT.656 Interface Block	101
Figure 4.25: Plain Data Load Shaping Logic.....	101
Figure 4.26: Data Load Shaping Logic.....	102
Figure 4.27: AES Cipher Core Architecture.....	103
Figure 4.28: AES Cipher Block Timing Diagram	104
Figure 4.29: Parallel-128 to Serial-8 Converter Block Interface.....	105
Figure 4.30: Communication Channel Interface Module	106
Figure 4.31: ITU-R BT.656 Formatter Interface	107
Figure 4.32: ITU-R BT.656 Formatter Block Diagram.....	107
Figure 4.33: Block Diagram of Video Receiver Module.....	109
Figure 4.34: Behavioral Simulation of Video Receiver Module	111
Figure 4.35: Operation Description of Video Decryptor Sub-Module.....	113
Figure 4.36: Behavioral Simulation of Video Decryptor Sub-Module	115
Figure 4.37: AES Inverse Cipher Block Architecture	117
Figure 4.38: AES Inverse Cipher Block Time Diagram.....	118
Figure 4.39: Video Display Module Block Diagram.....	120
Figure 4.40: Video Frame Grabber Flowchart.....	122
Figure 4.41: Video Pixel Structure	123
Figure 4.42: Implementation of YCbCr to RGB Converter	124
Figure 4.43: Dual Port Module	126
Figure 4.44: SDRAM Controller Connection.....	127