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

List of Figures