Selective Video Encryption System using AES (Rijndael) Algorithm Using FPGA

I.Kamal.Ismail
Avionics R&D Center,
Egyptian Air Forces
Eng.ismailkamal@gmail.com

Ehab.A.Elsehely
Avionics R&D Center,
Egyptian Air Forces
Elsehely@yahoo.com

Ahmed.E.Abdalla
Assoc. Prof, M.T.C,
ahmedabdalla60@yahoo.com

Abstract: - The demand for efficient, real time video cryptography systems has become more prominent in our life, especially for military and sensitive-civilian applications. The proposed system design was constrained in both area and speed in order to fulfill the requirements for real time video signals with limited hardware resources. Using Field Programmable Gate Array (FPGA) for the system implementation is suitable for both video and cryptography processes due to video data rate, flexibility to design modifications, and cryptography algorithm agility. The design strategy was based on making use of all available pre-designed, pre-verified cores for low cost Xilinx Spartan III XC3S1000-ft256 FPGA chip.
In this system, only active video data are encrypted with (Rijndael) Advanced Encryption Standard (AES) crypto algorithm and a self-synchronized cipher key mechanism based on the embedded video Timing Reference Signals (TRS) was designed to overcome the security leakage in Electronic Codebook (ECB) mode and to reduce the possibilities of cryptanalytic attacks which are used to recover the encryption key like brute force attacks. The design is tested first using an internally generated video pattern, then using external composite video camera source. The design implementation results were significant for speed and area, it reached 59.044 Mbytes/sec. data throughput that fulfills the minimum requirements of colorful, 30 FPS video data rate of 27 Mbytes/sec., and the design occupies 4,007 slices (52% of chip size).

Key-Words: - AES, FPGA, cryptography, low cost video encryption, real time video encryption

1 Introduction

Video cryptography is a sequence of processes that are performed on digital video signals to convert it into secured format that only authorized persons can process and view. Video cryptography is used to guarantee the end-to-end video security for sensitive, video systems such as Unmanned Air Vehicles (UAVs) video-surveillance, home security, video conferencing, and prepaid-entertainment channels. The (Rijndael) [1] symmetric block cipher algorithm is designed by Joan Daemen and Vincent Rijmen, it is capable of supporting data and key sizes of 128, 192, and 256 bits with different modes of operation. AES is very fast when implemented on hardware [2, 3]. In this work AES is implemented with 128 bits data and key sizes and operate in ECB mode.

Hardware implemented cryptographic algorithms are more physically secured than the software implemented algorithms, as they are very hard to be read or modified by an outside attacker. The traditional Application Specific Integrated Circuits (ASICs) implementation is not flexible to algorithm and parameter switch. FPGAs are hardware devices whose function is variable and which can be easily reprogrammed in-system. FPGA implementation advantages of video cryptography systems include:

- Algorithm agility; changeability of encryption algorithm during operation for more security or when it is obsolete or been broken.
- Modification of design architecture; adding of new design-blocks easily to support new functions, like supporting new data links.
- Modification of design parameters; design tuning for nonstandard parameters, like nonstandard pixel resolutions or non-standard frame rates.
- Data throughput; FPGA implementations faster than software implementations but still slower than ASIC implementations.
- Cost efficiency; development time and cost for FPGA implementation of a system is much lower than ASIC implementation of the same system. However for mass production, ASIC implementation is the most cost-efficient choice.

In this paper section 2 describes the implementation process of video cryptography system. Section 3 describes the system synthesize results. Section 4 describes system simulations

results and hardware verification. Section 5 is a comparison to others similar published work.

2 Video Cryptography System Design

The video cryptography system block diagram is shown in Figure 1. The design is divided into 6 modules as follows:

(1) Digital Clock Manager (DCM).
(2) Video color bars generator.
(3) Video decoder initialization module.
(4) Video transmitter interface module.
(5) Video receiver interface module.
(6) Video display module.

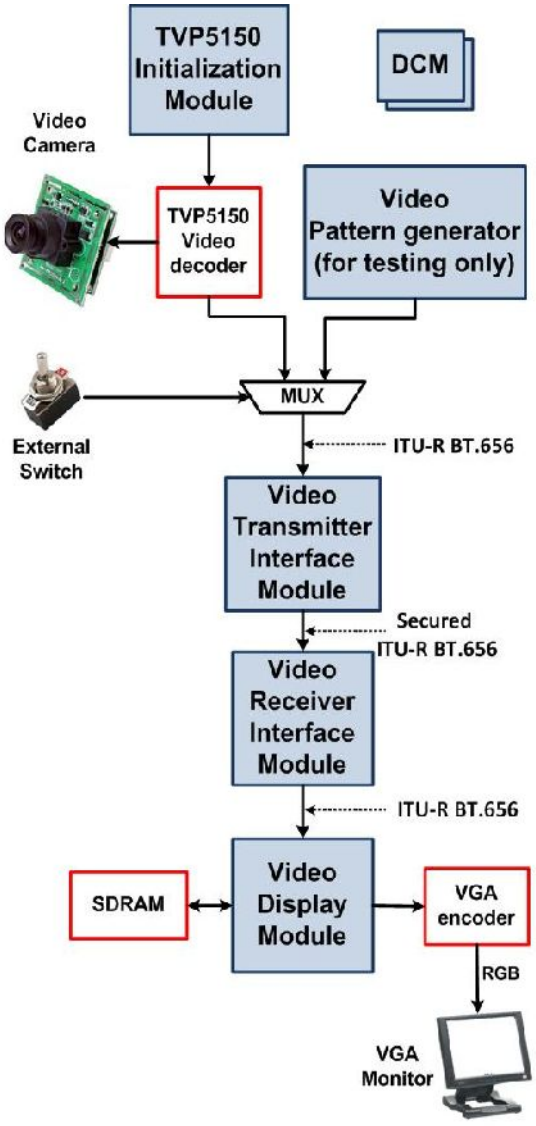

Figure 1: video cryptography system block diagram

2.1 Digital Clock Manager (DCM)

DCM is a Xilinx primitive IP core [4], used to provide advanced clocking capabilities to Spartan™-3 global clock distribution network for FPGA applications [5]. Spartan-3 DCMs solve a variety of common clocking issues, especially in high-performance, high frequency applications.

In this design two DCM blocks are used, the first DCM block is used to generate 50 MHz clock from the 100 MHz external oscillator clock that are needed in the Video Graphics Array (VGA) display module, and the second DCM block is used to generate 54 MHz clock from the 27 MHz video oscillator clock that are needed in the video transmitter interface module and the video receiver interface module.

2.2 Video Colorbar Generator Module

In this module a digital video 525 line YCbCr 4:2:2 color bar is implemented at 8-bit resolution. The generated pattern complies with SMPTE EG-1 standard [6] as in Figure 2.

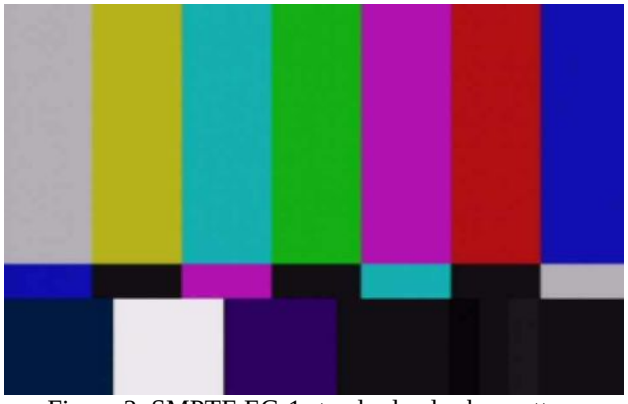

Figure 2: SMPTE EG-1 standard color bar pattern

This module is used for testing different system blocks that need ITU-R BT.656 digital video format [7] as an input and in system in-circuit testing stage.

2.3 TVP5150 Initialization Module

The video analog to digital converter (TVP5150 decoder chip) [8] is initialized and controlled by a set of internal registers which set all device operating parameters. Communication between the external controller and the TVP5150A decoder is through I^2C bus protocol. In this module, the internal-registers of TVP5150 are initialized, parameters like:

- Selection of video input source.
- Standard video output format.
- Brightness, saturation, hue, and sharpness.

2.4 Video Transmitter Interface Module

The video transmitter interface module is responsible for receiving the input plain-video from TVP5150 and deliver encrypted video data in the

same video format, block diagram for the video transmitter interface module is in Figure 3.

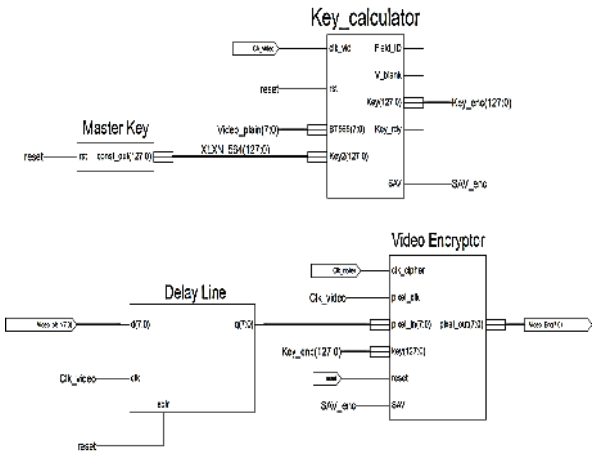

Figure 3: The video transmitter interface block diagram

The video transmitter interface module consists of four main sub-modules as follows.

2.4.1 Master Key

In the master key sub-module, a 128-bits master user-key is stored and used in the encryption process.

2.4.2 Delay Line

In this sub-module, the video signal is delayed to adjust the synchronization between the generated key and the plain video before the encryption process starts. This delay line has been designed using Xilinx® LogiCORE™ IP RAM-based shift register.

2.4.3 Key Calculator

In order to overcome the security leakage and achieve a reliable video encryption in ECB mode [9], a unique encryption key is calculated with each plain data block using the key calculator sub-module. The encryption keys are originated from the pixel sequence and a linear masking function (XOR) with the user master key.

This sub-module is self-synchronized as it extracts the key information from the video TRS signals that are sent unencrypted to the receiving part, so no extra framing data are needed.

Also, 47,160 different encryption keys are generated for every single video frame. This huge number of keys not only solves the lack of randomness that is the principle drawback of ECB mode but also it tremendously reduces the possibilities of cryptanalytic attacks such as the ciphertext only attack.

2.4.4 Video Encryptor

This sub-module is responsible for receiving the digital video signals from TVP5150 and coverts it into an encrypted ITU-R BT.656 format. The video encryption sub-module can be functionally divided into five main blocks.

(1) ITU-R BT.656 interface.
(2) Data-load-flag shaping circuit.
(3) AES cipher core.
(4) Parallel-128 to serial-8 converter.
(5) ITU-R BT.656 formatter.

2.5 Video Receiver Module

In this module the encrypted ITU-R BT.656 video signals are received and converted into plain ITU-R BT.656 video signals. The video receiver interface module consists of the following sub-modules:

(1) Master Key.
(2) Delay Line1.
(3) Delay Line2.
(4) Key calculator.
(5) Video decryptor.

2.5 Video Display Module

In this module plain video frames are received in YCbCr 4:2:2 format and pixels information are extracted and displayed on a VGA monitor.

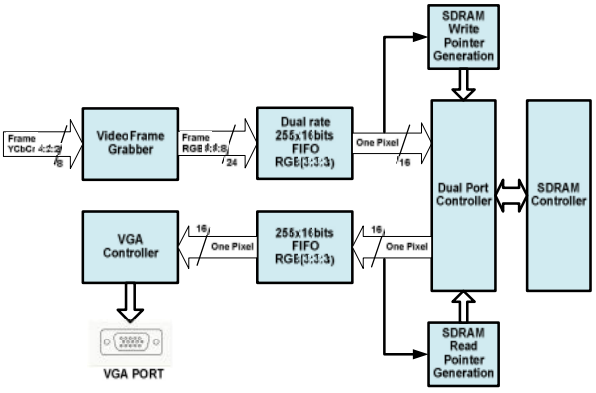

Figure 4: The video display block diagram

The video display module consists of six main sub-modules as follows.

2.5.1 Video Frame Grabber

In this sub-module, video pixels are grabbed and colors information is extracted from the video signals, then the pixel-color system is converted from YCbCr 4:2:2 to RGB 8:8:8. Finally a dual rate First-In First-Out (FIFO) with 255 locations is used to store the generated 16-bit pixels.

2.5.2 SDRAM Write Pointer Generator

In this sub-module, SDRAM write pointer value is evaluated according to the embedded video synchronization signals. The video pixels storing process is used to convert the video scanning technique from interlaced scan to progressive scan which is suitable for display over VGA screen.

2.5.3 Dual Port Controller

The dual port sub-module splits the SDRAM controller port signals between two identical host-side ports; the video frame grabber block and the VGA display module. Each port can perform memory read/write operations independently of any operations that occur on the other port.

2.5.4 SDRAM Controller

SDRAM controller sub-module accepts simple read and write requests on the host-side and generates the waveforms required to perform these operations on the SDRAM side.

2.5.5 SDRAM Read Pointer Generator

In this sub-module, SDRAM read address pointer value is evaluated and used by the VGA generator to get pixels from SDRAM. The read address pointer will be incremented when the read operation begun flag is received from the dual port controller. The read address pointer is set back to zero when receiving the end of video frame signal from the VGA generator.

2.5.6 VGA Controller

In this sub-module, a VGA controller is implemented and used to retrieve the video data from the SDRAM and format it into video pixels and lines and send it to the VGA monitor with the appropriate horizontal and vertical sync pulses.

3 System Synthesizes Results

Implementation of design has been done for Xilinx Spartan III. XC3S1000-ft256 with speed grade -5. Xilinx ISE v14.2 is used for design synthesize and implementation, Mentor Graphics Modelsim v.6.3f is used for functional and timing simulation, Xilinx Chipscope pro v14.2 is used for in-circuit testing. Implementation results are as follows in table 1.

Table 1: System implementation results

Implemented system	Speed (MHz)	Area (Slices)
Digital video display system	84.7	6%
AES ENC/DEC with 8-bits interface	88.2	38%
All Video cryptography system	59.044	52%

4 System Testing

Four tests are applied on the proposed system to accommodate the integrity nature and huge size of video signals. Testing types are shown in Figure 5.

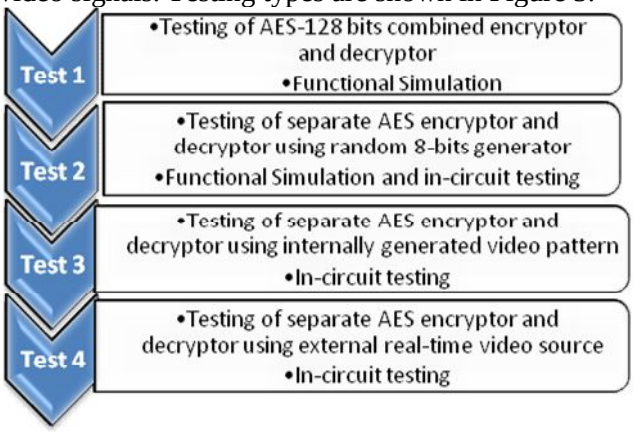

Figure 5: System testing structure

In test 1, a back to back AES 128-bits encryptor and decryptor is connected and functionally tested as in Figure 6.

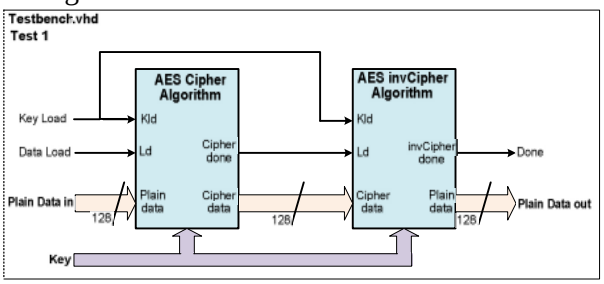

Figure 6: Test 1 structure

The simulation results in Figure 7 shows that the data value after decryption process is always the same as the input plain data when using the same key in encryption and decryption, as following:

Key = hex (000102030405060708090a0b0c0d0e0f).

Palin data input = hex (00112233445566778899aabbccddeeff).

Encrypted data out = hex (69c4e0d86a7b0430d8cdb78070b4c55a).

Decrypted data out = hex (00112233445566778899aabbccddeeff).

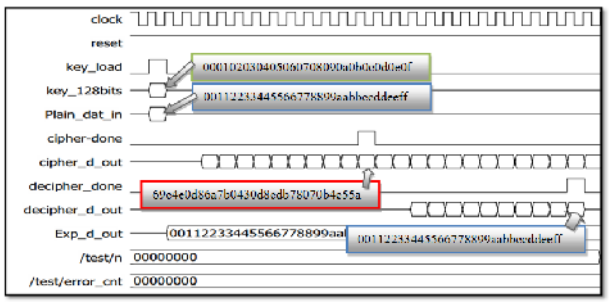

Figure 7: Test 1 simulation results

In test 2, AES separate encryptor and decryptor is tested using a pseudo random 8-bits generator as in Figure 8.

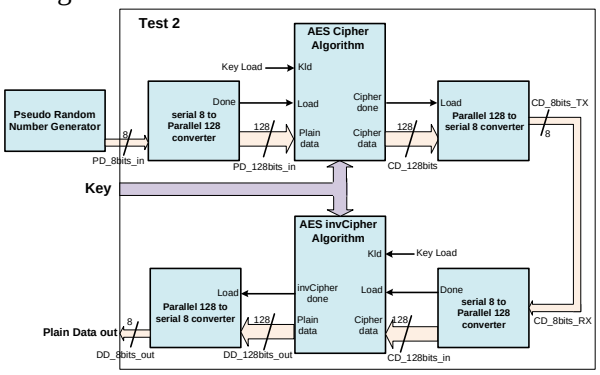

Figure 8: Test 2 structure

The simulation results for test 2 are illustrated in Figure 9. The simulation shows that the data value after decryption process is always the same as the input plain data.

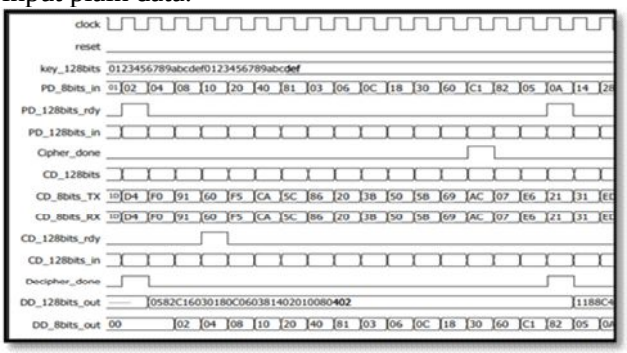

Figure 9: Test 2 simulation results

In test 3, the proposed design is tested by using an internally generated video pattern. The internally generated video colour bars signal is considered real-time, fixed pattern video scene that is connected to the proposed system input to test the internal modules as illustrated in Figure 10.

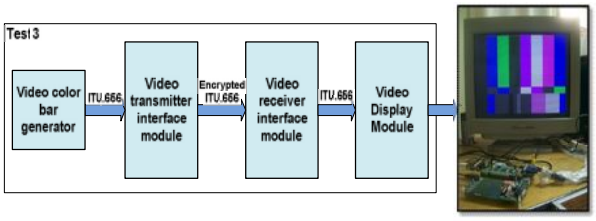

Figure 10: Test 3 structure

Finally in test 4, the proposed design is tested by using external video camera. The camera output is according to ITU-R BT.656 standard. The test structure is described in Figure 4.53. Test results are observed by Xilinx Chipscope pro v.9.2 while proposed system operation is running as illustrated in Figure 11.

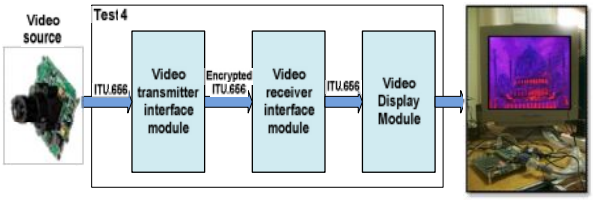

Figure 11: Test 4 structure

5 Comparison to Similar Published Work

The proposed design for comparison in Table 2 is the implementation of AES encryptor and decryptor with 8-bits interface accompanied with Key-Schedule algorithm that targeted Xilinx, Spartan3 chip. And the similar published work [10] is Implementation of AES encryption engine for real time video targeted Xilinx, Virtex 4 chip.

Table 2: Comparison to similar published work

Design	Targeted Platform	Speed (MHz)	Area
proposed design, Spartan3	XC3S1000-5ft256	88.8	38%
Published, AES, video,Virtex4	Xc4vsx35-10ff668	101.22	7%

6 Conclusion

An implementation of video cryptography system using AES is fulfilled. The design is optimized for small chip area and high data throughput to fulfil the video data encryption throughput speed on a low cost platform. The increased speed is achieved by portioning the design to different macros. Implementation results were significant and achieved a speed of 59.044 Mega Bytes/ second on Spartan-III™ XC3S1000. All

active video data are encrypted which increased the cryptanalysis complexity for intruders.

References:

[1] N. I. o. S. a. T. (NIST), "Advanced Encryption Standard (AES) (FIPS PUB 197)," in *Computer Security Standard, Cryptography*, ed. Federal Information Processing Standards Publication, 2001.

[2] Kris Gaj and P. Chodowiec, "Comparison of the hardware performance of the AES candidates using reconfigurable hardware," presented at the The Third Advanced Encryption Standard (AES3) Candidate Conference, New York, USA, April 2000.

[3] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*: Wiley India Pvt. Limited, 2007.

[4] X. I. T. Staff, "Digital Clock Manager (DCM) Module," ed: Xilinx Inc., 2009.

[5] X. I. T. Staff, "Spartan-3 FPGA Family Data Sheet," ed: Xilinx Inc., 2012

[6] S. o. M. P. a. T. Engineers, "Alignment Color Bar Test Signal for Television Picture Monitors," in *EG 1:1990*, ed, 1990.

[7] I. T. Union, "ITU-R BT.656-5. Interface for digital component video signals in 525-line and 625-line television systems operating at the 4:2:2 level of Recommendation ITU-R BT.601," ed, 2007.

[8] T. i. Staff, "TVP5150A ultralow power NTSC/PAL/SECAM video decoder with robust synch detector," ed: Texas instrument, 2004.

[9] N. DOUKAS, "Low Color-Depth Image Encryption Scheme for use in COTS Smartphones," *WSEAS TRANSACTIONS on SYSTEMS*, vol. 11, pp. 527-538, 2012.

[10] Jayashri E. Patil and A. D. Shaligram" FPGA Implementation for Real Time Encryption Engine for Real Time Video" , ICC'10 Proceedings of the 14th WSEAS international conference on Circuits.