Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

8th International Conference on Electrical Engineering

ICEENG 2012

A Low cost FPGA implementation of real time video cryptography system using AES (Rijndael) algorithm.

I.Kamal.Ismail[1], Ehab.A.Elsehely[2], A.E.Abdulla[3]

Abstract:

The demand for efficient, real time video cryptography systems has become more prominent in our life, especially for military and sensitive-civilian applications. FPGA implementation of video cryptography systems is suitable for both video and cryptography processes due to video data rate, flexibility to design modifications, and cryptography algorithm agility. In this paper, a bulk video cryptography system using AES (Advanced Encryption Standard) is designed and implemented on low cost FPGA Xilinx Spartan-III™. Bulk encryption is used to encrypt both video data and video synch to increase the cryptanalysis complexity for intruders. The design is implemented on different stages; camera interface, video frame grabber, VGA monitor interface, SDRAM controller, crypto processor, and communication channel interface. The design has been tested first using a generated video pattern, and using external composite PAL/NTSC video camera source. The design is implemented for XC3S1000 and the results were significant for speed

[1]Master Student, R&D Center, Egyptian Air Forces.

[2]PhD, R&D Center, Egyptian Air Forces.

[3]Assoc. Prof, Dean of M.T.C,M.T.C, Egyptian Air Forces

and area, it reached 77.6 Mbytes/sec. data throughput that fulfills the minimum requirements of colorful, 30 FPS video data rate of 27 Mbytes/sec., and the design occupies 3,738 slices (48 % 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, real time video systems such as UAV (Unmanned Air Vehicle) video-Surveillance, home security, video conferencing, and prepaid-entertainment channels. The AES (Rijndael) [1] symmetric block cipher algorithm has been 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] [4] [5]. In this work AES is implemented with 128 bits size key and Electronic CodeBook (ECB) mode [6].

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 (ASIC) hardware implementation is not flexible to algorithm and parameter switch. Field Programmable Gate Arrays (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 has been divided into 4 stages. Stage 1 is the design and implementation of camera / video decoder interface. Stage 2 is the implementation of AES-128 bits encryptor and decryptor. Stage 3 is the implementation of serial data stream of 8-bit width for the communication channel. Stage 4 is the implementation of digital video display system with frame grabbing, SD-RAM control, and VGA interface.

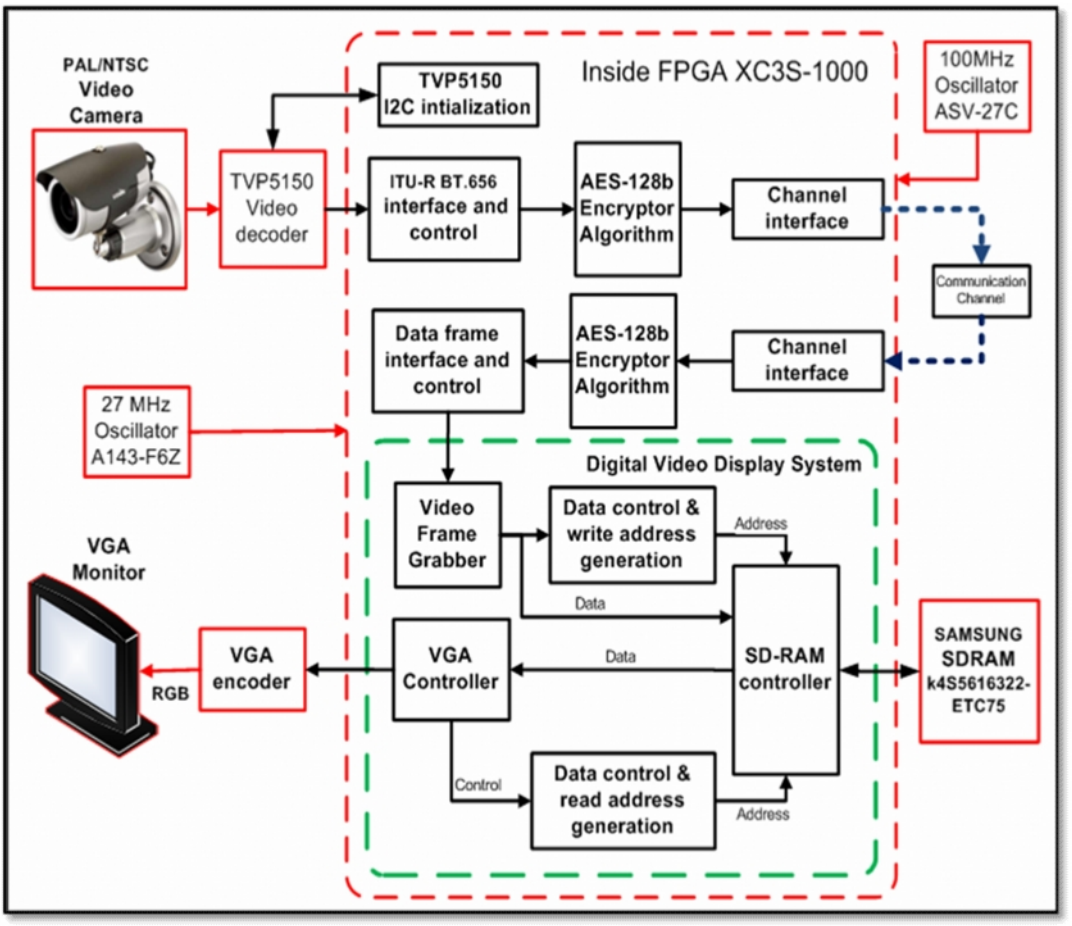


Figure (1) Structure of video encryption system

2.1 Implementation of Camera / Video Decoder Interface

In stage 1 video camera composite output [7] is converted to 8-bits width digital format in the video analog to digital converter TVP5150 [8]. The digital video output is according to ITU-R BT656 standard [9] and has data rate of 27 Mbytes/sec for interlaced scan, 4:2:2, PAL/NTSC ,30 FPS video system.

The digital video data rate equal to the video decoder clock times the number of bits per pixel= 27 MHz *8bpp = 216 Mbps.

Functions of video decoder interface design are:

- Initialize the TVP5150 decoder internal registers, via I2C bus and enables the digital video output.
- Convert data from 8-bits width, synched with 27 MHz pixel clock to 128-bits width, synched with 50MHz cipher clock.

- Generate the required controls for AES encryptor to work.

2.2 Implementation of AES-128 bits Encryptor and Decryptor

In stage 2, design is divided into two parts; AES encryptor and AES decryptor each with 128 bits width key and 128 bits width data in/out. These macros are design to process a block of data in 12 clock cycles (10 cycles for the 10 round, plus one cycle for initial key loading, and one cycle for the output stage) and operate at 50MHz clock speed to be suitable for video data rate.

AES has a round-oriented structure. For key length of 128 bits the number of required rounds is 10. Each round of encryption function consists of four transformations; SubBytes, ShiftRows, MixColumns & AddRoundKey and each round of decryption function consists of four transformations; InvByteSub, InvShiftRow, InvMixColumns & AddRoundKey[10].

A companied key schedule algorithm is used for Round keys calculation. It expands the main key into round keys; in the decryption process round keys are applied in reverse order.

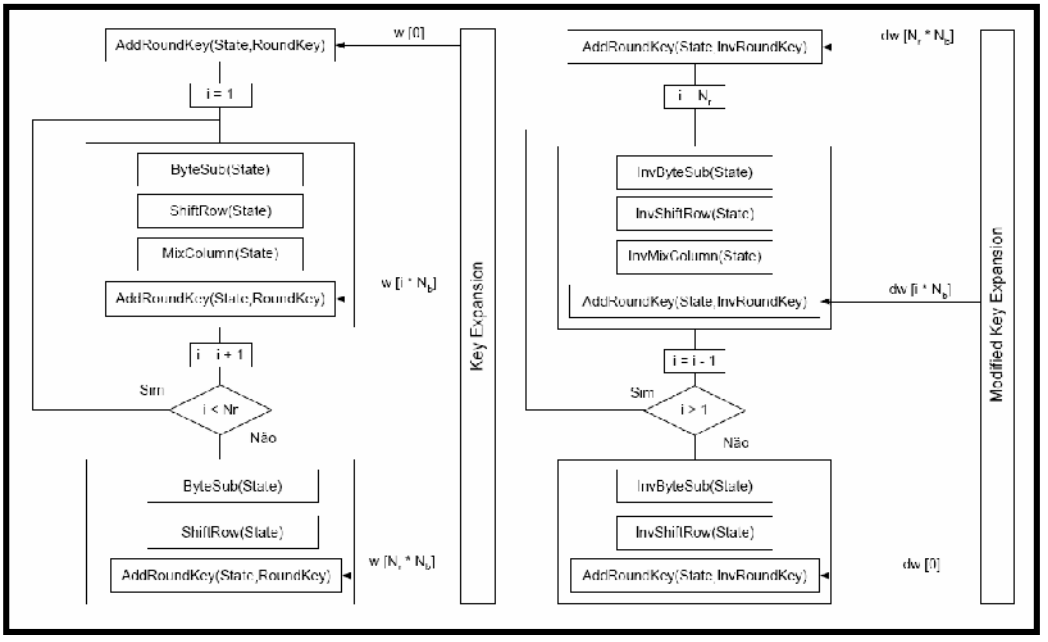


Figure (2) AES round structure for encryptor and decryptor.

2.3 Implementation of Serial 8-bits Data Stream for Channel Interface

In stage 3, design is divided into two parts:

1) *At the transmitter part of the channel*, the design converts the data from 128 bits width from the encryptor (synched with cipher clock) to serial 8 bits width (synched with channel clock) using dual rate FIFO.
2) *At the receiver part of the channel*, the design converts the data from serial 8 bits width (synched with channel clock) 128 bits width from the encryptor (synched with decipher clock) and generate all needed control signals needed for decryption process.

Figure (3) shows the design interface for 8-bits channel.

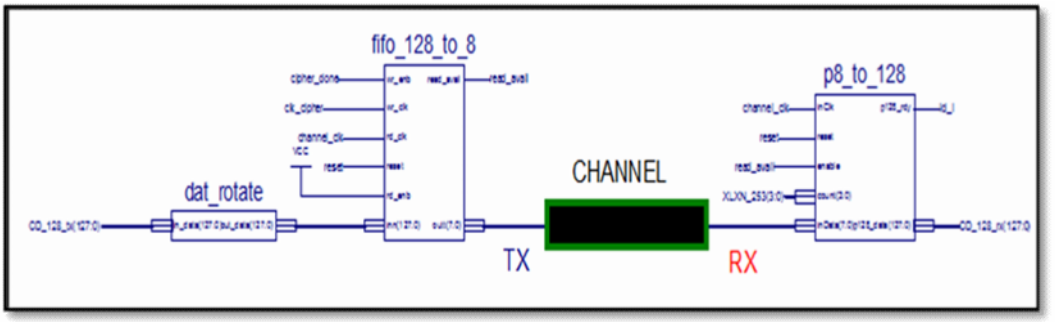


Figure (3) Communication channel interface.

2.4 Implementation of Digital Video Display System

In stage 4, design is divided into 3 parts:

*1) Frame grabbing***:**

- Grab frames of video in ITU-R.656 4:2:2 formats.
- Convert YcbCr to RGB format and create pixels.
- Store pixels in a dual rate FIFO.
- Generate the SDRAM writing address, as the video lines in each field are interleaved through the SDRAM.

2) SDRAM control:

- Generate commands to the SDRAM to perform certain operations using SDRAM-controller.
- Multiplex the SDRAM port signals using Dual Port Controller:

- Frame-grabber writing pixel operation.
- VGA-controller read pixel operation.

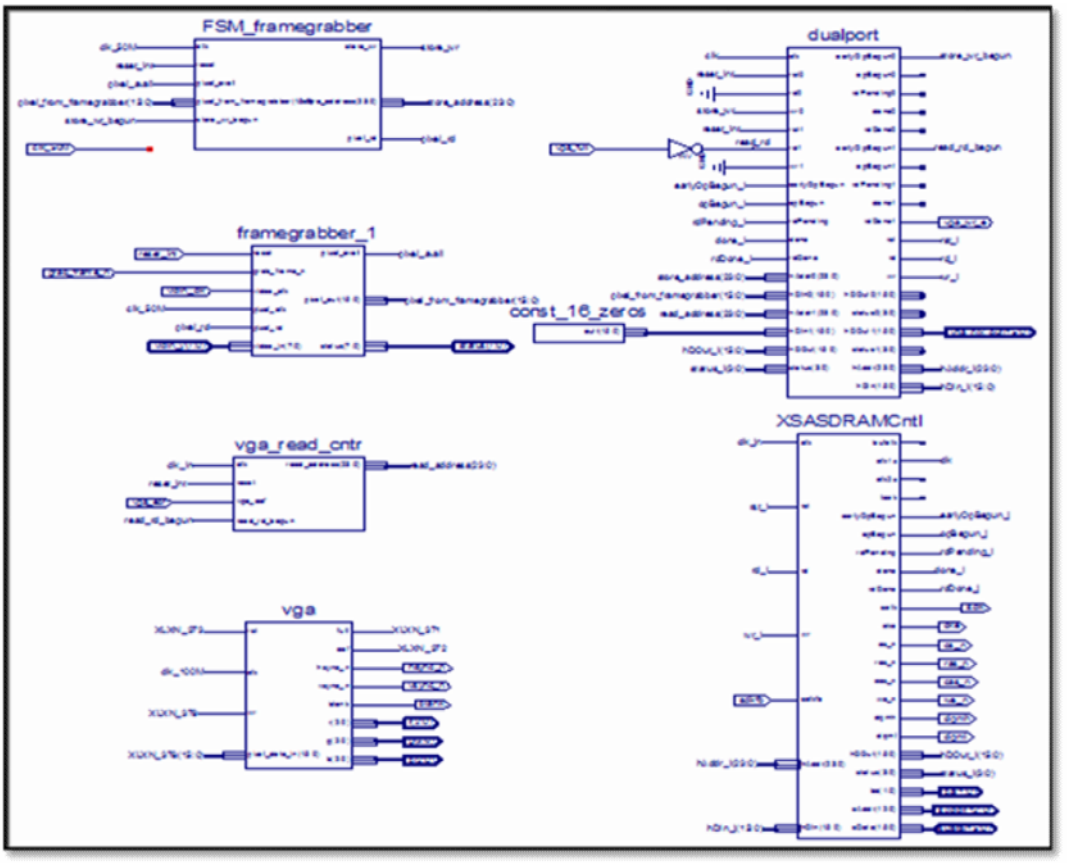


Figure (4) Structure of digital video display system.

3) VGA controller:

- Read pixels from SDRAM in progressive scan technique.
- Generate 3-bits per color for the resistors matrix (video encoder).
- Generate VGA monitor timing signals for 31 KHz horizontal synch, 60 Hz refresh rate, with (800*600) resolution.

3. System Synthesizes Results

Implementation of design has been done for Xilinx Spartan III XC3S1000-ft256 with speed grade -5 [11]. Xilinx ISE v12.3 is used for design synthesize and implementation, Mentor Graphics Modelsim v.6.3f is used for functional and timing simulation, Xilinx Chipscope pro v.9.2 is used for in-circuit testing. Implementation results are as follows in table 1.

Table 1: implementation results of different system stages.

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	77.6	48%

4. System Testing and Hardware Results Verification

The design testing has been performed 4 times and on different design stages because of the video data integrity and huge size.

In test 1, a back to back AES 128-bits encryptor and decryptor is connected and functionally tested as in Figure (5).

Key <= hex (000102030405060708090a0b0c0d0e0f).

Palin data input <= hex (00112233445566778899aabbccddeeff).

Encrypted data out <= hex (69c4e0d86a7b0430d8cdb78070b4c55a).

Decrypted data out <= hex (00112233445566778899aabbccddeeff).

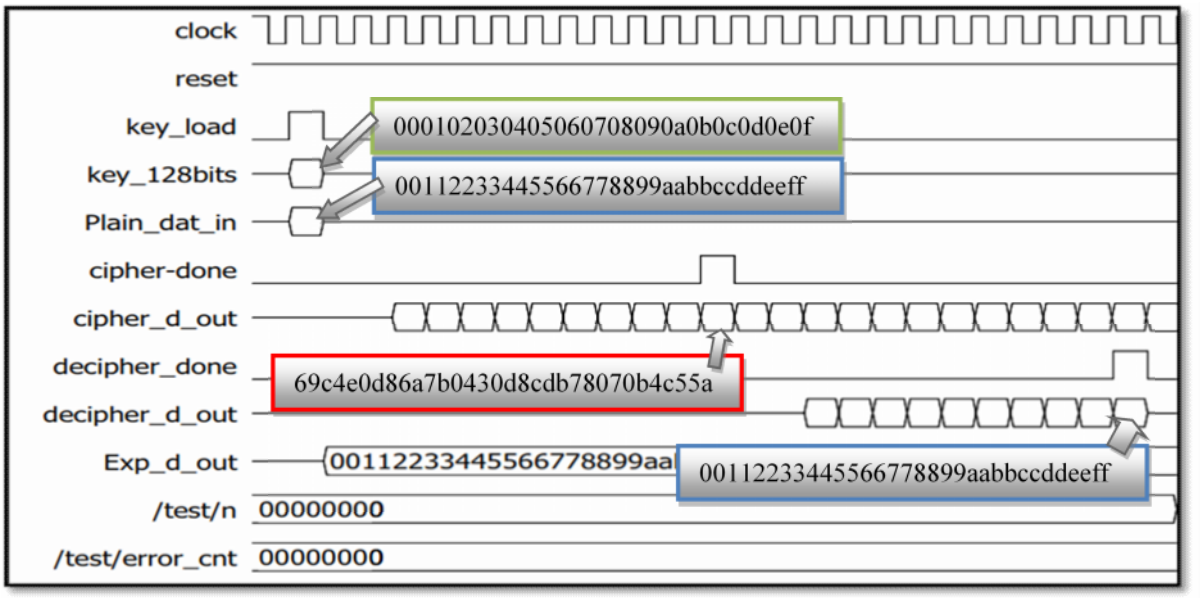


Figure (5) simulation of AES 128 bits Encryptor and Decryptor.

In test 2, AES separate encryptor and decryptor is tested using a pseudo random 8-bits generator as in figure (6).

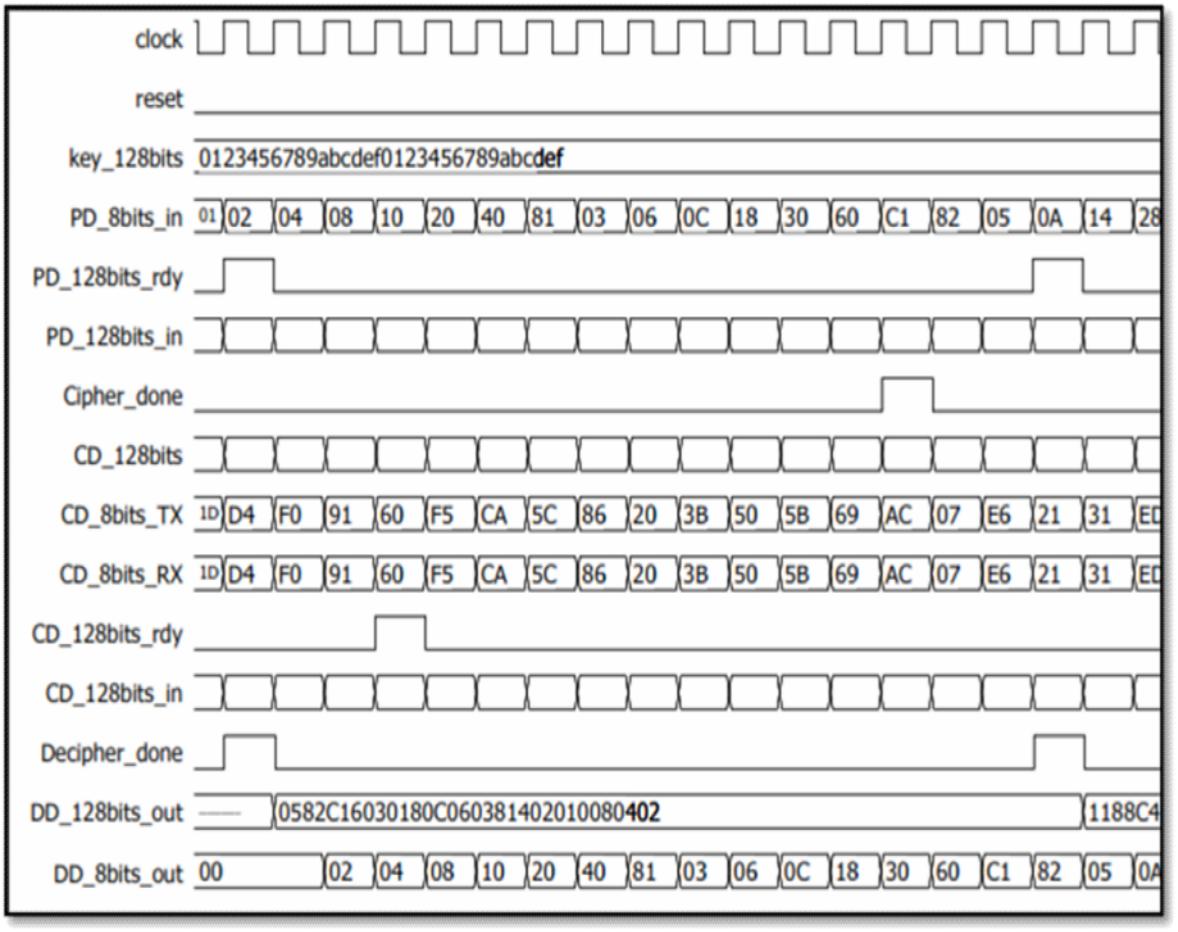
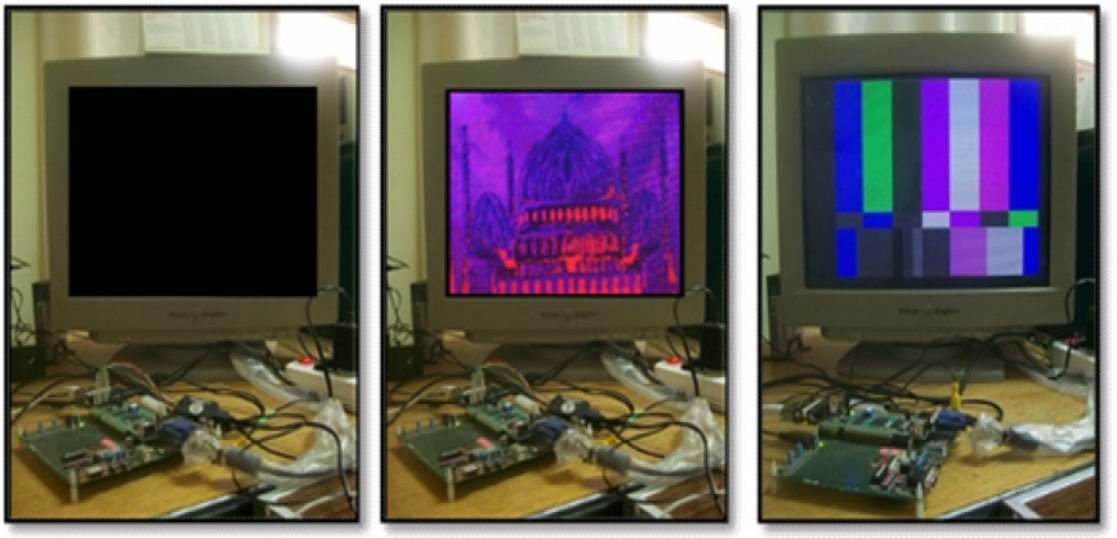


Figure (6) simulation of AES 8 bits Enc and Dec interface.

In test 3 and 4, design is tested in-circuit, first using internally generated video pattern, and later using external real-time video source connected to the system input. Figure (7) shows the VGA monitor display before and after decryption process for both internally generated video pattern and real video scene.



(a) **(b)** **(c)**

Figure (7) (a) generated video pattern or real video scene before decryption.

(b) real video scene after decryption.

(c) generated video pattern after decryption.

Figure (7) shows the VGA monitor blanked when displaying the encrypted video signals because both video data and video synch signals is encrypted.

Figure (8) shows the plain data, decrypted data and control signals waveforms

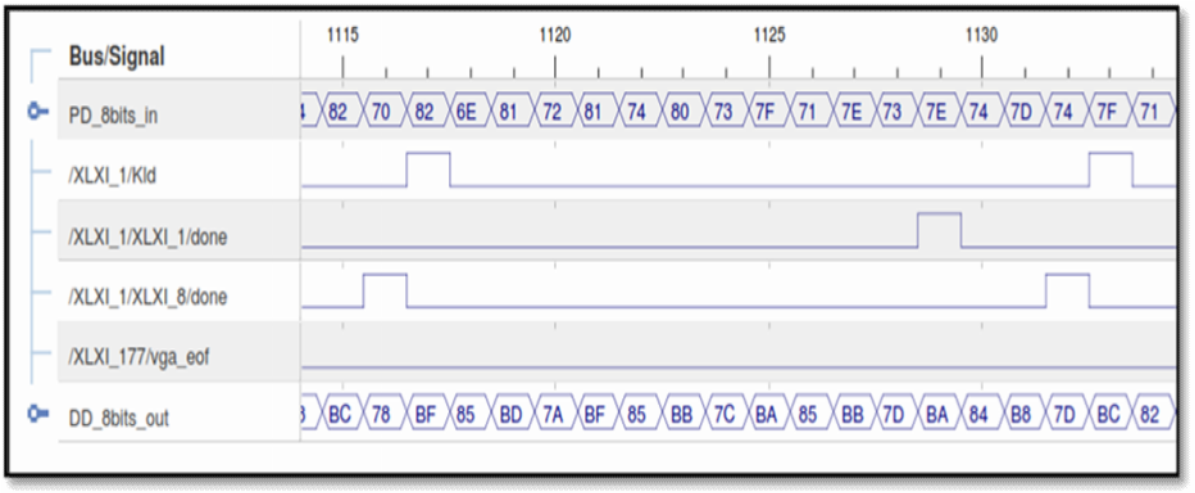


Figure 8: in-circuit testing using Xilinx Chipscope 9.2.

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 [12] is Implementation of AES encryption engine for real time video targeted Xilinx, Virtex 4 chip.

Table 2: comparison of proposed work and 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%

CONCLUSION

An implementation of video cryptography system using AES is presented. The design is optimized for small chip area and high data throughput to fulfill 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 77.6 Mega Bytes/ second on Spartan-III™

XC3S1000. The video signals are bulk-encrypted which increased the cryptanalysis complexity for intruders.

REFRENCES

[1] U.S Department of Commerce/National Institute of Standard and Technology. FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), November 2001.

[2] K. Gaj, P.Chodowiec, "Fast implementation and fair comparison of the final candidates for advanced encryption standard using field programmable gate arrays", in: CT-RSA 2001, pp.84-99.

[3] A. Hodjat, I. Verbauwhede, "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA". Proceedings of the 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'04).

[4] K.Janvinen, M. Tominisko, J. Skytta, "A fully pipelined memorlyess 17, 8 Gpbs AES-128 encryptor", in International symposium of Field programmable Gate arrays, 2003, pp.207-215.

[5] M. Mclone, J.V. McCanny, "Rijindael FPGA implementations utilizing look-up tables", J.VLSI signal process, syst. 34(3)(2003)261-275.

[6] Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition 2005.

[7] Video Signal Format http://www.kat5.tv/videoformats.html

[8] Texas Instrument:Datasheet "http/www.ti.com/lit/ds/symlink/tvp5150".

[9] Interface for digital component video signals of Recommendation ITU-R BT.601"http://www.itu.int/rec/R-REC-BT.656/en".

[10] Daemen J., and Rijmen V. "The Design of Rijndael: AES-the Advanced Encryption Standard". Springer-Verlag., 2002

[11] Xilinx: "Spartan-3 FPGA Family data sheet".

[12] 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.