Secure Video Transmission System for UAV Applications

Dimitrios Psilias
dpsilias@uniwa.gr, Department of Informatics and Computer Engineering University of West Attica
Athens, Greece

Athanasios Milidonis
milidon@uniwa.gr, Department of Informatics and Computer Engineering University of West Attica
Athens, Greece

Ioannis Voyiatzis
voyageri@uniwa.gr, Department of Informatics and Computer Engineering University of West Attica
Athens, Greece

ABSTRACT

UAV applications are starting to increase nowadays. Their data demanding applications are implemented mostly using software platforms. These applications have critical requirements on high performance, power consumption and there should be security at their transmissions, especially for video data. In this paper, an architecture is proposed for secure video transmission for UAV applications. The system consists of a digital camera a transmission board to transmit the video and a FPGA for implementing the security encryption tasks. The camera sends the video data to the FPGA and the inside circuit encrypts the video data. The transmission module transmits the encrypted data to the Ground Station (GS). Measurements taken concerning the execution time and power consumption, reveal the benefits of the proposed architecture in comparison with well-known software platforms.

KEYWORDS

UAV, AES, FPGA, Video, Security, ESP

ACM Reference Format:
Dimitrios Psilias, Athanasios Milidonis, and Ioannis Voyiatzis. 2021. Secure Video Transmission System for UAV Applications. In *25th Pan-Hellenic Conference on Informatics (PCI 2021), November 26–28, 2021, Volos, Greece.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3503823.3503882

1 INTRODUCTION

The significance of securing data on applications based on Unmanned Aerial Vehicles (UAVs) is necessary in our days. Some of the applications are surveillance, construction, military, delivery of goods, and search and rescue. In these cases, video data are exchanged between UAVs and their GS. These video data are sensitive information, and no one should be able to have access to them except from the authorized personnel. Since there is a wide use of digital images and videos in UAV applications, there is a critical requirement to secure the data and from unauthorized persons. Until now most of the transmissions are analogue with no security. Therefore, secure transmission of the previous mentioned data is a high-priority requirement. By encrypting these data, the privacy issue is avoided. Latest cryptography standards consist of complex mathematical algorithms and require many iterations resulting in increased execution time and power consumption. Moreover, video data are characterized by great volumes and real-time transmissions. For the efficient execution of encryption tasks there is a need for special hardware that will accelerate execution, keeping the power consumption low. Since the cryptography algorithm may vary according to the security needs, the use of a Field Programming Gated Array (FPGA) is beneficial since it is reconfigurable. Moreover, it can process large amounts of data concurrently and it has a small implementation cost comparing to an ASIC.

In this paper we propose an architecture for secure video transmission system for UAS applications, consisting of a platform based on a camera module, an FPGA and a transmission module. The security algorithm is implemented in the FPGA and the transmission is made by an ESP. Data is sent from the camera module to the FPGA for encryption. Then, the encrypted data generated at the FPGA, are transmitted with the ESP.

The remaining of the paper is organized as follows. Section 2 presents the related work. Section 3 describes the proposed architecture. In section 4, the architecture implementation and the results in terms of execution time and power consumption are analyzed. Finally, section 5 concludes this paper.

2 RELATED WORK

The new encryption standard recommended by the National Institute of Standards and Technology (NIST) to replace the Data Encryption Standard (DES) algorithm, is Advanced Encryption Standard (AES). AES is a symmetric block cipher that can encrypt and decrypt information and is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. Both hardware and software implementations perform very efficiently and is used not only for security but also for great speed. It can be implemented on various platforms and also in small devices. It is extremely difficult to hackers to get the real data when encrypting by AES as it has the ability to deal with three different keys [1],[2],[3].

Multimedia applications have become very popular. The information of an image or a video is valuable and needs to be protected. Real time streaming of the above information also needs the suitable bandwidth for transmission. This is why a high performance platform implementation is needed [4].

Software and hardware implementations which attempts to detect and keep away the unauthorized persons of stealing sensitive information that is transmitted. Software implementations are reliable and trustful but not so efficient . For time critical applications, a hardware implementation is always the best solution [5[,[6].

Hardware implementations in FPGA are often appears in Unmanned Aerial Vehicles (UAVs), and specifically for Flight Controller

PCI 2021, November 26–28, 2021, Volos, Greece
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-9555-7/21/11…$15.00
https://doi.org/10.1145/3503823.3503882

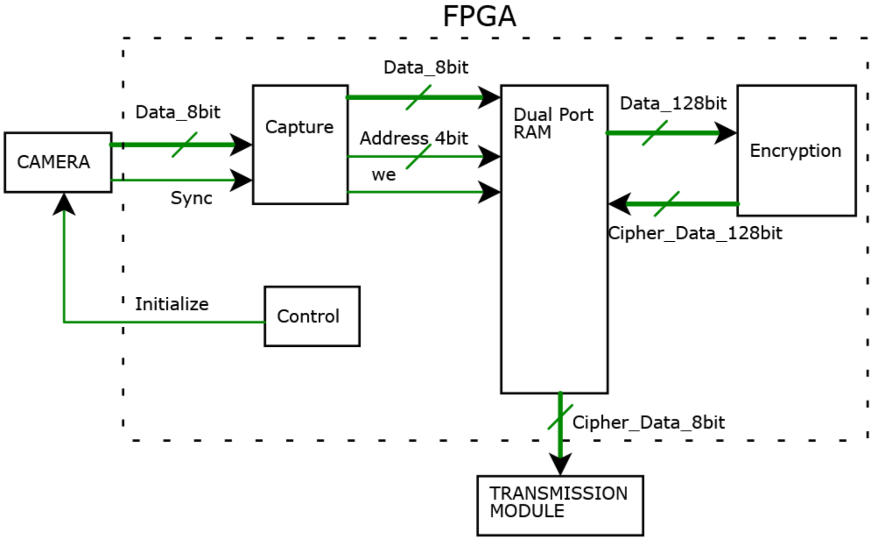

Figure 1: Proposed Architecture

(FC) implementation. That is because the demands for greater mission complexity and the need to increase the flight performance creates the need for onboard processing. With the use of FPGA as a FC, better stability is succeeded, faster PID control adjustment and in some cases more flight time [7],[8], [9].

AES implementations on FPGA have been made for general applications but not for UAVs. These implementations take advantage of the parallelism of the FPGA inside operations and the low power consumption [10], [11], [12], [13].

3 PROPOSED ARCHITECTURE

Figure 1 shows the proposed architecture for transmitting secure video in UAVs. A digital camera with 8bits data output, is attached to the FPGA to generate the video source signal in real time. The implemented circuit at the FPGA [8] consists of a control module which is used for the initial configuration of the camera, and capture the video data. To configure it properly, the device control register is set properly. Beside the configuration, timing signals (PCLK, HREF, VSYNC), are controlled for the proper output data. After configuring the camera, the next step is to capture the image data. The capture module is responsible for controlling the camera. Moreover, there is a dual port RAM which is also controlled by the capture module. Video data are written to a RAM's address when the capture module sets write enable (we) signal high and configures the address bus. Next, there is an encryption component which reads the video data from RAM and outputs the encrypted data for transmission.

The encryption algorithm used is the AES . According to AES, 128 bits of data are required as input and the result is 128 bits of encrypted data. Because the camera output sends 8 bits data, we need to buffer that data until they are 128 bits. For this reason, there is a need to implement inside the FPGA a dual port RAM. One port of this RAM is used for buffering the 1 byte information and the other port is used for sending 16 bytes for encryption in one clock cycle. When all 16 bytes are written to RAM, the encryption procedure begins. The output of the previous process is a 16-byte word that is written in one clock cycle from Encryption component to RAM. Then, RAM data are read by the Transmission module and transmitted

Table 1: Operation Mode Algorithm

Operation Mode Algorithm

```
Step1:
Initialize Camera
if Camera not initialized
send initialize error and start over
end if
Step1.1:
for each and every block of a frame do
capture video
Step1.2:
for i=0 to 16
send 8bit video data to RAM
end for
read 128bit data for encryption from RAM
send 128bit encrypted data to RAM
Step2:
for i=0 to 16
Send encrypted data for transmission
end for
end for
```

Table 1 shows the operation flow of the proposed architecture. It is a detailed description of the path followed by data generated from the camera until they are transmitted encrypted by the transmission module. Initially, the control module initializes the camera. If an error occurs, it tries again until the camera is initialized. Then, concerning the encryption process, camera sends 8bits video data

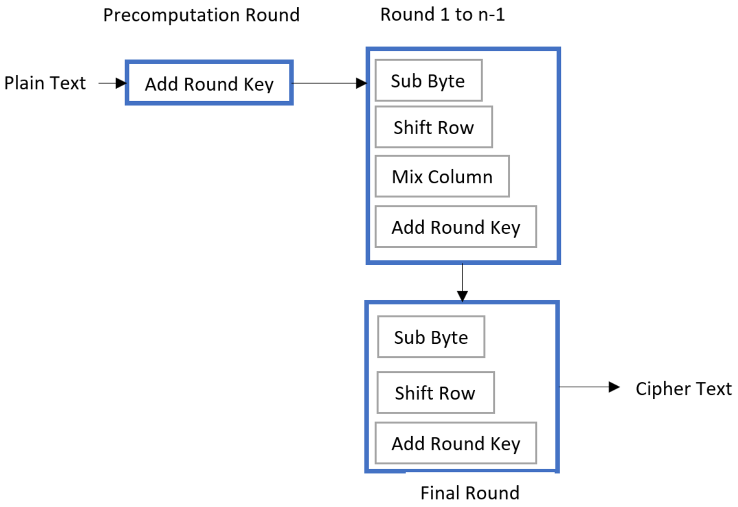

Figure 2: AES Encryption Structure

to the FPGA. Data are written to the FPGA's internal RAM at sequential addresses using an 8bit data bus. This is repeated until 16 bytes of data are written. Then the encryptor reads the 16 bytes and starts the encryption procedure. When the 16 bytes cipher data are ready, they are written to RAM in one clock cycle using the 128 bit data bus. Finally, the encrypted video data are sent to the transmission module.

Figure 2 shows the AES encryption procedure that is implemented inside the FPGA. Here is a typical round of AES encryption. Each round has four sub-processes.

Byte Substitution (SubByte)

The 16 input bytes are substituted by looking up a fixed table. The result is in a matrix of four rows and four columns.

Shiftrows (Shiftrow)

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows:

First row is not shifted.

Second row is shifted one (byte) position to the left.

Third row is shifted two positions to the left.

Fourth row is shifted three positions to the left.

The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns (MixColumn)

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and another similar round begins.

Figure 3 shows the parallel computing concept of the AES. Instead of processing one word at a time, it performs the operations in parallel. Figure 4 explains the concept of parallel operation. That is, all 16 bytes operations are simultaneously processed. Initially, word 1, word 2, word 3, and word 4 are used as inputs. These inputs are then processed in parallel, to give the cipher text output of same length. The next set of inputs is processed, after the cipher text is obtained.

4 EXPERIMENTAL RESULTS

4.1 Experimental method

For the implementation of the proposed architecture, OV7670 module is used as a digital camera. It takes power from the Basys 3 [14], [15] board and all the signals and the output are also connected to Basys 3. This board is used for the hardware implementation of the AES. It contains an FPGA of Atrix-7 family [16], [17]. The FPGA's performance is estimated using Vivado's [18] timing reports for extracting the operation frequency and the post implementation simulation process for extracting the number of the executed clk cycles. Also using Vivado, the proposed architecture's circuit is implemented and the corresponding bitstream is extracted for configuring the FPGA at the Basys 3 board. Moreover, the FPGA's power consumption is extracted using the same framework. Finally, the ESP module [19], [20] is used as a transmitting module and it is attached to the Basys 3 board.

The proposed architecture is compared with two software platforms. The first one consists of a digital camera for video source data and an ESP module for software encryption and transmission through Wi-Fi. The second platform uses a camera and a Raspberry Pi 4 (Rpi 4) [21] executing a software implementation of AES encryption and by using its Wi-Fi module, the encrypted data are transmitted.

The execution time for encryption at the ESP and the Rpi 4 has been calculated through the software implementation of AES. The

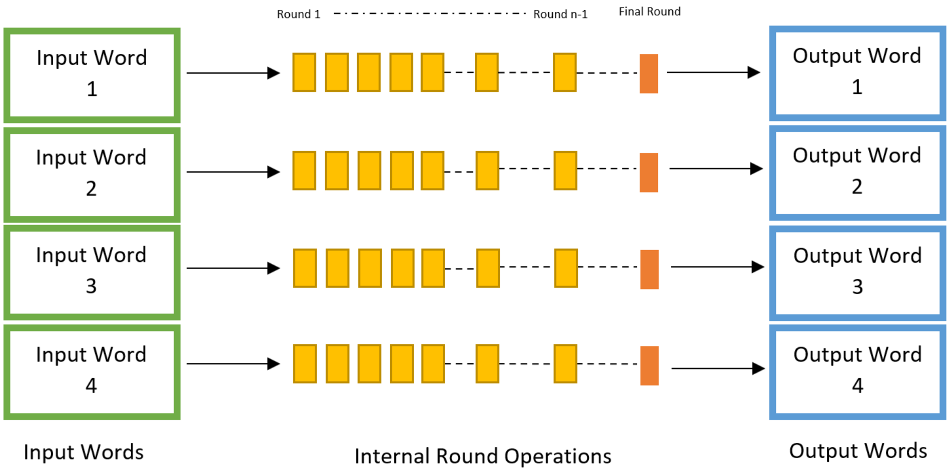

Figure 3: FPGA Parallel operations

Table 2: Performance - Consumption Measures

	Frequency (MHz)	Encryption Time(μs)	Power (mW)
FPGA	100	0.11	0,086
ESP	80	30.576	0,132
Rpi 4	1.500	198,2	2,86

power consumption of these two software platforms has measured using a USB power meter.

4.2 Experimental results

Table 1 shows the comparison of the three platforms in terms of execution frequency, performance and power consumption. The proposed architecture's approach (FPGA) performs better in execution time of AES keeping the power consumption low. It only needs 0.11μs to encrypt data and it consumes only 0.086. Rpi 4 consumes a lot of power and it takes 198.2μs to execute an AES encryption task, despite the quad core 64bit ARM processor at 1.5GHz. The ESP module performs better than RPi 4 but far slower than the FPGA due to the 30.576μs needed for AES encryption.

With a typical frame size of 640×480 and a 16-bit/pixel at 25 fps, the required bitrate for transmitting video is 125Mbps. The FPGA architecture needs 11cycles to encrypt 128 bits block of data. The following formula is used to calculate the throughput:

$$\text{Throughput} = \frac{128}{11*clock\_cycle} \quad (1)$$

Using an operating frequency at 100MHz the secure data are produced at a rate of 1.16 Gbps.

The experimental results reveal the benefits of the proposed architecture which are mostly due to better exploitation of parallelism. Moreover, the hardware used in the FPGA is lighter than in the other platforms, which have redundant circuits that are unnecessary for this application. This is resulting in significant decrement of power consumption in the proposed architecture.

5 CONCLUSION AND FUTURE WORK

In this paper an architecture for secure transmission of video data is presented for UAV applications. The presented architecture consists of a camera, an FPGA and a transmission module. The camera is generating the video stream data which is encrypted in the FPGA. The transmission module sends the encrypted data to the GS. The FPGA's hardware accelerates the execution due to efficient exploitation of parallelism of the execution tasks, while it consumes low power.

REFERENCES

[1] Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001

[2] Dr. Prerna Mahajan, Abhishek Sachdeva. A Study of Encryption Algorithms AES, DES and RSA for Security. Global Journal of Computer Science and Technology Network, Web & Security. 2013

[3] Ako Muhamad Abdullah. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. Article June 2017

[4P.P.] Dang, P.M. Chau. Image encryption for secure Internet multimedia applications. 2000 Digest of Technical Papers. International Conference on Consumer Electronics. Nineteenth in the Series (Cat. No.00CH37102). June 2000

[5] https://en.wikipedia.org/wiki/Secure_transmission

[6Dag] Arne Osvik, Joppe W. Bos, Deian Stefan, David Canright. Fast Software AES Encryption. Laboratory for Cryptologic Algorithms, EPFL, CH-1015 Lausanne, Switzerland2 Dept. of Electrical Engineering, The Cooper Union, NY 10003, New York, USA3 Applied Math., Naval Postgraduate School, Monterey CA 93943, USA. 2010

[7Justin] Young, Andrew Ross Price. FPGA Based UAV Flight Controller. AIAC-11 Eleventh Australian International Aerospace Congress. 2005

[8Cameron] D. Patterson, Paul E. Plassmann, Lynn A. Abbott. Implementation of a Trusted I/O Processor on a Nascent SoC-FPGA Based Flight Controller for Unmanned Aerial Systems. Thesis submitted to the Faculty of the Virginia Polytechnic Institute and State University. 2018

[9] Noé Monterrosa, Jason Montoya, Fredy Jarquín, Carlos Bran. Design, Development and Implementation of a UAV flight controller based on a State Machine approach using a FPGA embedded system. 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)

[10] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar. FPGA Implementation of AES Encryption and Decryption. 2009 International Conference on Control, Automation, Communication and Energy Conservation

[11] Paweł</number> Chodowiec, Kris Gaj. Very Compact FPGA Implementation of the AES Algorithm. Cryptographic Hardware and Embedded Systems - CHES 2003 pp 319-333

[12] Tim Good, Mohammed Benaissa. AES on FPGA from the Fastest to the Smallest. Cryptographic Hardware and Embedded Systems – CHES 2005 pp 427-440

[13] Atul M. Borkar, R. V. Kshirsagar, M. V. Vyawahare. FPGA implementation of AES algorithm. 2011 3rd International Conference on Electronics Computer Technology

[14] https://store.digilentinc.com/basys-3-artix-7-fpga-trainer-board-recommended-for-introductory-users

[15] https://www.xilinx.com/products/boards-and-kits/1-54wqge.html

[16] https://www.xilinx.com/products/silicon-devices/fpga/artix-7.html

[17] https://digilent.com/shop/boards-and-components/system-boards/fpga-boards/?FPGAFamily=Artix-7&

[18] https://www.xilinx.com/products/design-tools/vivado.html

[19] https://www.espressif.com/en/products/socs/esp8266

[20] https://diyi0t.com/esp8266-nodemcu-tutorial

[21] https://www.raspberrypi.com/products/raspberry-pi-4-model-b/specifications