


A Combined Video and Telemetry Encryption Architecture for UAVs with FPGA


Dimitrios Psilias

(Department of Informatics and Computer Engineering University of West Attica Athens,
Greece,

 <https://orcid.org/0000-0002-2042-9037>, dpsilias@uniwa.gr)


Athanasios Milidonis

(Department of Informatics and Computer Engineering University of West Attica Athens,
Greece,

 <https://orcid.org/0000-0001-9408-2104>, milidon@uniwa.gr)

Ioannis Voyiatzis

(Department of Informatics and Computer Engineering University of West Attica Athens,
Greece,

 <https://orcid.org/0000-0002-3173-8054>, voyageri@uniwa.gr)

Abstract: This work presents a novel Field Programmable Gate Array (FPGA)-based architecture for encrypting telemetry together with high-definition video data in unmanned aerial vehicles (UAVs). The design uses the Advanced Encryption Standard (AES-128) to secure data and video streams, ensuring protection against cyberattacks. The proposed system integrates a pipeline data path for video and telemetry data, coupled with FIFO buffers, enabling efficient handling of different bandwidth requirements while maintaining high throughput. Our platform encrypts/decrypts both down-stream and up-stream telemetry data and encrypts down-stream of video data. To the best of our knowledge, no such architecture has been proposed in the literature, as existing research focus on encrypting only a part of the aforementioned types of data. Experimental results demonstrate that the proposed architecture performs efficiently without adding serious execution delays comparing to existing FPGA platforms, while keeping energy consumption low.

Keywords: UAV, FPGA, encryption, drones, AES, decryption, FC, MAVLink

Categories: B.2.2, B.3.3, B.4.4, D4.8, E.3, E.4

DOI: 10.3897/jucs.154482

1 Introduction

UAVs are constantly improving our daily lives. There is a significant growth of unmanned aerial vehicle (UAV) applications in several domains e.g. military missions, shipment and delivery, information gathering, surveillance, and geographical mapping. UAVs are quite beneficial as they provide flight services with low cost [Shakhathreh, 19]. However, the applications use, manage and control sensitive information related to telemetry and video. Telemetry consists of general flight information, e.g. altitude, speed and position. Additionally, data generated by sensors from internal subsystems are included, like engines and communications. This information is transmitted from a UAV to its Ground Station (GS). Moreover, commands sent from a GS to a UAV are

also included in telemetry data. Video data are generated through the UAVs' cameras and transmitted to the respected GSs. Current applications require high definition (HD) video quality, resulting in high processing and transmission rates demands [Lee, 10], [Nosheen, 20]. Communication mechanisms for transmitting UAV data have been proposed in Yu et al. [Yu, 21] where a design of a multi-UAV full-duplex system is proposed for joint high-specification video, i.e., 4K video, transmission and stable flight control.

Both telemetry and video are information streams that must be protected from malicious interceptors, as they could take control of the vehicle or compromise other systems e.g. its GS. Using encryption/decryption algorithms, transmitted data are secured eliminating the chances of interception. Advanced Encryption Standard (AES) algorithm is preferred for encryption/decryption of video and sensitive data [Tsai, 18], [Dayane, 22], [Altigani, 21], [Rajasekar, 16], [Dey, 18]. AES can be implemented using software or hardware platforms. Common UAV implementations are based on software platforms, which focus on encrypting/decrypting the transmitted telemetry data. This is not very efficient as they consume much power and their performance is limited. In modern UAV applications, telemetry data are processed in parallel with the large amounts of video data. Therefore, there is a need for secure UAV platforms that operate with low latency and consume low power.

Existing hardware platforms like Shoufan et al. [Shoufan 15] and Kim et al. [Kim 21], are based on Field Programming Gated Arrays (FPGAs) that focus on encrypting/decrypting of only the telemetry data which is the key information for controlling a UAV. Kotel et al. [Kotel 14] implement FPGA-based AES video encryption only, with no support for telemetry data at all. They are very efficient in performance and power consumption. However, securing video and telemetry data is not an option at these platforms.

In this work, an FPGA-based platform is proposed for encrypting/decrypting all data (video and telemetry related) exchanged between a UAV and its GS. A mechanism is introduced for frequent selection of video data for encryption and a less frequent selection of telemetry data for encryption/decryption. Experiments show that the processing of the combined telemetry/video data is done with insignificant delays, comparing to existing hardware platforms which process only telemetry data. The novel aspects of this architecture include a dual-pipeline design, optimized for different bandwidth requirements, and the use of FIFO buffers to eliminate data loss and metastability issues. Compared to prior work, this architecture achieves high throughput and energy efficiency, making it well-suited for power-constrained UAV systems.

The remaining of the paper is organized as follows. In section 2 the related work is given. In section 3 the proposed architecture is presented. In section 4, the experimental methods and results, in terms of execution time and throughput, are analysed. Finally, section 5 concludes this work.

2 Related Work

In recent years there is an increased use of UAVs in applications related to delivery of goods, engineering, agriculture, communication etc. Cornelius et al. [Cornelius, 15] explore the necessity, viability, and dangers of using UAVs to transport medical

supplies during emergencies. Giordan et al. [Giordan, 20] provide solutions by using UAVs in a number of engineering and geology applications. Tkáč et al. [Tkáč, 19] present an extensive review of UAV usage in civil engineering. Liuzza et al. [Liuzza, 18] is a study on methods for using UAVs with multispectral, thermal, and vision cameras for precision agriculture monitoring. The primary restrictions for each application are indicated, along with the factors to be considered before flight execution.

UAV communication aspects have been explored in the literature. Critical technologies have been adapted e.g. machine learning, energy efficiency, security, telemetry etc. Abhishek et al. [Abhishek, 20] presents the most recent advancements in UAV communication technology. Furthermore, it investigates path planning, while machine learning technologies are exploited for improving current UAV communication systems. Techniques for power management and encryption are considered, in order to provide safe and long-lasting connections. The development of a communication system for UAVs, is presented in Jahwar et al. [Jawhar, 17]. Suryanegara et al. [Suryanegara, 15] explore the communication technologies that support Unmanned Aircraft System (UAS) operation.

In the context of UAVs, telemetry refers to the system that collects data related to flight and transmits them to a GS [Hristov, 16]. These data are crucial for monitoring the vehicle's location, altitude, speed, battery life, and other critical parameters. Moreover, they are important for controlling flight paths, payloads and overall mission, ensuring safe operation within limits.

Telecommand, on the other hand, is the system that allows the remote control and guidance of the UAV from a ground station. Telecommand enables the operator to send commands and instructions to the UAV through telemetry, allowing for real-time adjustments to the vehicle's flight plan, payload, and other operational parameters as needed. The combination of telemetry and telecommand is essential for the safe and effective operation of UAVs, providing the operator with the necessary information and control to ensure the successful completion of the UAV's mission [Mozaffari, 19].

Imaging and sensing systems provide important features to UAVs in various applications. These systems consist of several methods for capturing images or measuring ranges e.g. RGB, thermal, optical HD, infrared (IR), multispectral, Light Detection and Ranging (Li-DAR) etc. The transmission of the produced data is done using analog or digital Video Transmitters (VTx). An analog VTx uses an analog modulation technique, often providing longer range but potential interference and lower image quality compared to digital VTx. Digital VTx utilize digital modulation, offering improved image quality and reduced interference, although they may have a shorter transmission range. An overview of current developments in UAV communications is provided in Zeng et al. [Zeng, 19], with a focus on integrating UAVs into cellular networks of the fifth generation (5G) and beyond. Moreover, Guirado et al. [Guirado, 21] offer a workable way to use 4G telecommunications to directly connect UAVs to the internet and take advantage of data collected by UAVs, such as telemetry and pictures, with a particular emphasis on video transmission. However, both analog and digital VTx can be vulnerable to security issues, as the video feed could be intercepted by unauthorized parties, posing privacy and data security risks.

Malicious attempts may be performed for seizing control of a UAV, for stealing important data or for taking its control in order to violate other elements. An example of such an attempt is by spoofing Global Positioning System (GPS) data, for altering

coordinates and making the UAV to deviate from its programmed course. Wagner et al. [Wagner, 23], discuss the detection of GPS spoofing attacks against cyber-physical systems using a confidence attribution scheme based on machine learning. Telemetry data, videos, images and mission data are UAV critical information and must be held secured. Li et al. [Li, 17] presents a high throughput architecture with FPGAs for AES encryption and decryption. Moreover, Kim et al. [Kim, 21] propose a module for encrypting only UAV telemetry data.

The most common implementations for UAV encryption/decryption are using software platforms. They are easy to maintain, and offer code portability [Li, 22], [Zhang, 20], [Cheng, 19], [Deebak, 20], [Botta, 13], [Prapulla, 16]. However, their throughput is limited and they consume a lot of power. A platform using ESP32 can be used for implementing security protocols, offering satisfactory execution time and power consumption [Barybin, 19], [Podder, 21], [Setiawan, 21], [Iqbal, 18]. Raspberry Pi Pico is also used for encryption/decryption tasks [Nooruddin, 23], [Desbiens, 23]. STM32 processor is used for secure video data on IoT systems [Tian, 18], but its performance is limited when used for real-time HD video encryption [Schwabe, 17].

On the other hand, hardware platforms have several advantages. They consume low power and execute tasks with low latency while processing high volumes of real-time data. These platforms can be implemented using FPGAs [Jahanirad, 23], [Molina, 22], [Dipankar, 03]. An FPGA AES implementation is proposed on [Visconti, 20], where data are encrypted/decrypted in a pipelined approach. It is used for general purpose applications, and it is not beneficial for the special needs of UAV data. Therefore, even though the achieved throughput is 28,16 Gbps, it is not designed to process both telemetry and video data which are arriving to the architecture's input with different rates. Standaert et al. [Standaert, 03] propose an AES implementation, optimized in terms of area. Despite the system's low latency, it is a general-purpose architecture which cannot process telemetry and video data in parallel. Another notable FPGA AES implementation is Kotel et al. [Kotel, 14], which is used for encrypting/decrypting video data with achieved throughput 4,28 Gbps.

Our work is beneficial for encrypting/decrypting UAV data, which consists of processing both telemetry and video data while exploiting the advantages of FPGA architectures.

3 Proposed Architecture

A real-time video and telemetry data encryption for UAVs is described in this section. Since UAV missions are time sensitive, encryption/decryption tasks must be executed with low latency. However, as existing UAV batteries have limited capacities, our encryption/decryption architecture needs to consume low power. Therefore, implementing software encryption on UAVs could cause flight instabilities and reduced flight duration. By using in the proposed approach an FPGA architecture all of the previously mentioned requirements are met.

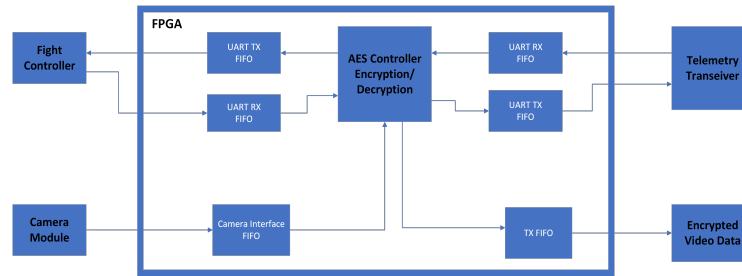


Figure 1: Proposed Architecture

Figure 1 shows the proposed FPGA architecture. For encryption/decryption a pipelined AES 128 architecture Visconti et al. [Visconti, 20] is used. The video data are sent from the UAV's camera. Then they are processed by the proposed architecture and sent to the GS using a video transmitter. Respectively, telemetry data are initially sent from the Flight Controller (FC) to the AES Controller Encryption/Decryption module and the encrypted data are sent to the telemetry transceiver which transmits them to the GS. Respectively, when the GS sends data to the UAV, a decryption procedure is performed until the decrypted data are passed to the FC.

In the proposed architecture different clock domains are used. Data are sent to the FC-Telemetry path, using a frequency described by the FC's specifications. However, data are processed in the AES Controller Encryption/Decryption module using a higher frequency for maximizing performance. Therefore, for avoiding metastability issues First In, First Out (FIFO) buffers are introduced and analysed in the next section. Also, in the Camera data Encryption path, similar FIFOs are introduced and analysed at the following sections since there are differences in the frequencies used for data sent by the Camera and the ones used for processing data, described by the camera's specifications. The proposed architecture uses one AES Controller Encryption/Decryption module for both, video and telemetry data. The different types of data are multiplexed before their encryption.

3.1 Telemetry TX Encryption

At figure 1 the architecture for receiving data from the FC and delivering them to the GS through the encryption module can be seen. Data are received in serial mode in packets of 8bits and are stored in the Universal asynchronous receiver-transmitter (UART) Receive (RX) FIFO component until their size becomes 128 bits, 16 packets. This is the amount of data needed for initializing the encryption process. After the completion of encryption, the produced cyphertext is temporarily stored at the UART Transmit (TX) FIFO, in order to be sent to the GS using serial transmission. It must be noticed that the clock frequency used in the UART FIFO buffers, is much lower comparing to the one used for encryption. The existence of these buffers assures that there will be no metastability issues. Also, there will be no data losses in the RX side, since newly received data will arrive much later than the completion of decryption/encryption.

3.2 Telemetry RX Decryption

At figure 1 the architecture for receiving data from the GS and delivering them to FC through decryption module can be seen. Data are received in serial mode in packets of 8 bits and are stored in the UART RX FIFO component until their size becomes 128 bits, 16 packets. This is the amount of data needed for initializing the decryption process. After the completion of decryption, the produced plaintext is temporarily stored at the UART TX FIFO, in order to be sent to the FC using serial transmissions. As in the process of encryption, the decryption buffers are used to eliminate the metastability issues and data losses.

3.3 Video Encryption

At figure 1 the architecture for receiving video data from a digital parallel output camera and delivering them to Transmitter through encryption module can be seen. Data are received in parallel mode and are stored in the Camera Interface FIFO component in packets of 8 bits until their size becomes 128 bits (16 packets). This is the amount of data needed for initializing the encryption process. After the completion of encryption, the produced cyphertext is temporarily stored at the TX FIFO, in order Encrypted Video Data to be sent to the Transmitter. Also, at this architecture, buffers are used to eliminate the metastability issues and data losses.

3.4 AES Controller Encryption/Decryption

This module is used for encryption/decryption. For this process, the pipelined AES 128 architecture [Visconti, 20] is used without any changes.

The encryption process is used for data sent from the UAV to the GS. Initially, there is a selection between data generated by the Flight Controller (FC) and the ones by the camera. The two different types of data are multiplexed assuring there is no data loss. For achieving this, video data are processed with high priority. Telemetry data is received using Micro Air Vehicle link (MAVLink) protocol within a heartbeat message using a frequency of 1 Hz [Atoev, 17], [Kwon, 18], [Koubâa, 19]. This message is transmitted serially to this module. When telemetry data are encrypted, the incoming video data are temporarily stored in FIFO buffers.

The decryption process is used for data sent from the GS to the UAV. These data are processed by this module and finally are sent to the FC.

3.5 Architecture Evaluation

The target of this research is not to present a new AES architecture as it uses an already efficient one proposed in the literature. This work proposes a complete solution for securing all types of UAV data exchanged with the GS (video and telemetry data) while in literature there are architectures that secure only one type of data.

Table 1 compares the proposed architecture to other FPGA-based AES implementations. Unlike previous work, this architecture supports simultaneous encryption/decryption of telemetry and video data, offering a unique advantage for real-time UAV operations. In Shoufan et al. [Shoufan, 15] the encryption is performed on video data while data sent from remote controller, used for navigation, are decrypted. In this platform there is no secure transmission for the telemetry data sent from the

UAV to the GS. In Kotel et al. [Kotel, 14] the encryption is performed only on video data.

Platform	Telemetry Encryption is Supported	Telemetry Decryption is Supported	Video Encryption is Supported
Proposed	Yes	Yes	Yes
[Shoufan, 15]	No	Yes	Yes
[Kotel, 14]	No	No	Yes

Table 1: Comparison with Prior FPGA Work

Moreover, the most common solutions for the implementation of these architectures are based on software platforms. This approach uses an FPGA platform which performs more efficiently while it consumes less power. Experimental results shown in the next section, indicate the achieved data throughput is much higher than the one needed for transmitting HD video. Additionally, it combines data paths with different throughputs (video and telemetry) assuring efficient data synchronization due to different rates. Besides, comparing to existing FPGA architectures for UAV security, this approach has similar results in terms of performance and power consumption as no serious delays are added to the data path nor extra consuming components.

4 Experimental Methods and Results

For the implementation of the proposed architecture, the Artix-7 XC7A35T-1CPG236C development board is used [Xilinx, 22]. All architecture's sub-blocks between the FC, the Transmitter and the Receiver are implemented in the FPGA using VHDL description language. The FPGA is configured using a bitstream generated from Vivado synthesizer [Townsend, 17].

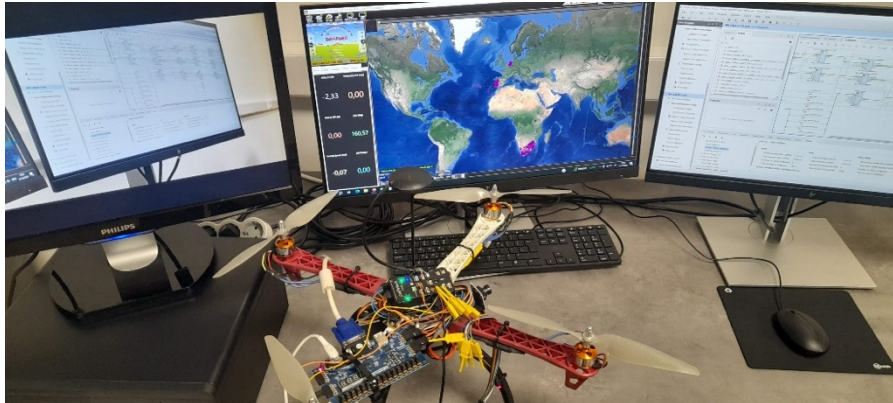


Figure 2: Experimental Set Up on Bench of UAV Platform

Figure 2 shows the experimental setup of our platform. A custom made F450 frame UAV with a Pixhawk 2.4.8 FC is used for the telemetry data that are sent to the FPGA board attached on it, for further processing. An OV2710 HD complementary metal-oxide semiconductor (CMOS) camera is used, which features an 8-bit data output. It supports a maximum video resolution of 1920×1080 pixels in RGB RAW format, with an output data rate of 30 frames per second (fps). All camera interface signals are connected to the FPGA development board, where video data is processed and encrypted before being transmitted. Mission Planner is used as GS for exchanging all UAV information. A USB protocol analyzer to captures the MAVLink signal.

The FPGA’s performance is estimated using Vivado’s timing reports, for extracting the system’s clock frequency. The number of clock cycles needed for execution are extracted using Vivado’s post implementation simulation process. Moreover, the FPGA’s power consumption is extracted using Vivado’s power reports.

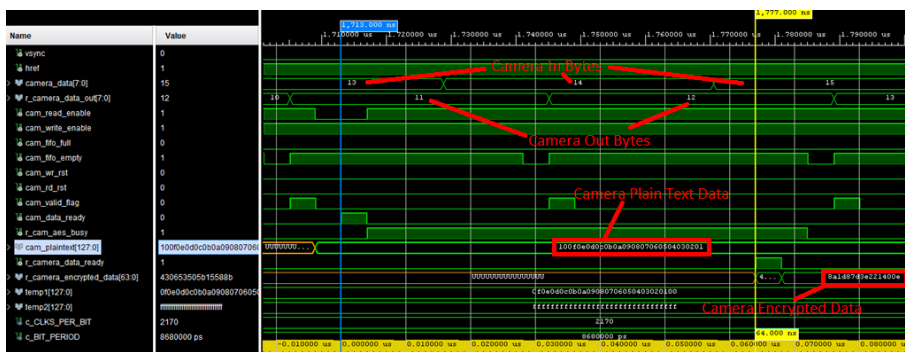


Figure 3: Camera Data Encryption

Figure 3 shows the Camera data encryption procedure at Vivado’s simulation. The cam_data_ready signal indicates whether the cam_plaintext vector contains data ready for encryption. When cam_data_ready is set to 1, data are available for processing. During encryption, the r_cam_aes_busy signal remains 1, signifying active encryption. The entire encryption and data transfer process takes 68 ns.

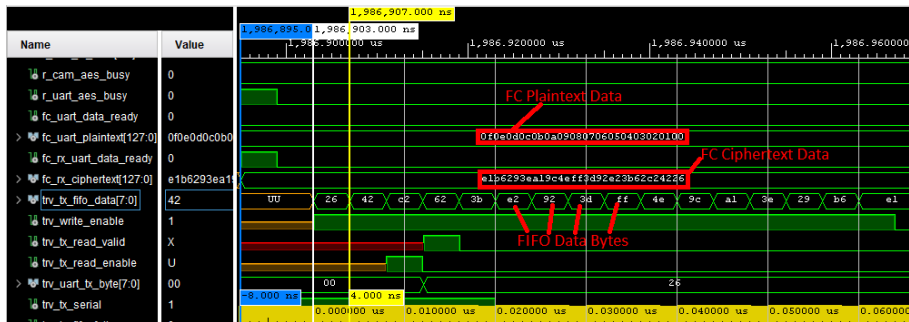


Figure 4: FIFO Module

Figure 4 shows the FIFO module simulation in Vivado for Telemetry data before they are sent to AES module. The FIFO module temporarily stores data before they are given to the AES encryption/decryption module, preventing metastability issues and data losses.

When the `fc_rx_uart_data_ready` signal is set to 1, the UART Transmitter Buffer stores the `fc_rx_ciphertext` vector. Subsequently, the `trv_write_enable` signal is set to 1, enabling the storage of 8-bit data blocks from the `trv_tx_fifo_data` vector into the FIFO buffer.

Once this process is complete, the `trv_write_enable` signal is reset to 0. The total time required for this operation is 72 ns. Considering that data are sent using MAVLink every 1 sec, the remaining time is used for processing video data, minimizing idle time. Therefore, the total throughput is defined by the rates for arriving and processing video data.

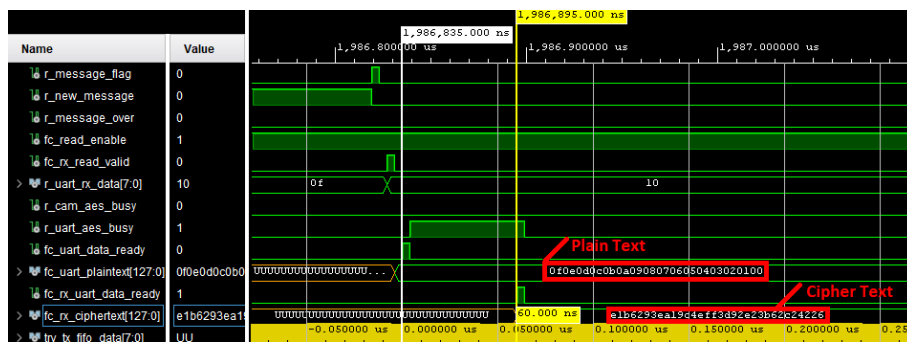


Figure 5: Telemetry Data Encryption

Figure 5 shows the simulation for the telemetry encryption process. When the `fc_uart_data_ready` signal is set to 1, the data contained in the `fc_uart_plaintext` vector is stored in the AES Encoder/Decoder component. While the encryption process is ongoing, the `r_uart_aes_busy` signal remains 1, indicating that the module is busy. The encryption process takes 10 clock cycles (60 ns) from the moment the data enters the AES Encoder/Decoder component until the encrypted data is produced. Once encryption is complete, the encrypted data is stored in the `fc_rx_ciphertext` vector, and the `fc_rx_uart_data_ready` signal is set to 1.

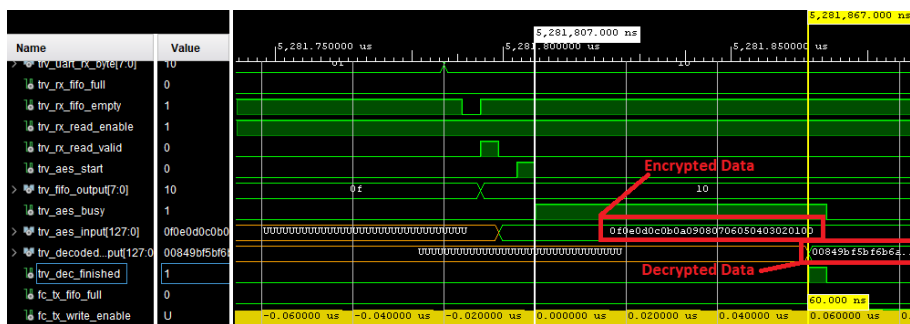


Figure 6: Telemetry Data Decryption

Figure 6 shows the simulation for the decryption process. The AES encryption/decryption module is responsible for decrypting the telemetry data received by GS. When the `trv_aes_start` signal is set to 1, the data contained in the `trv_aes_input` vector is stored in the AES Encoder/Decoder component. While the decryption process is ongoing, the `trv_aes_busy` signal remains 1, indicating that the module is actively decrypting. Once decryption is completed, the decrypted data is stored in the `trv_decoded_output` vector, and the `trv_dec_finished` signal is set to 1. The decryption process requires 10 clock cycles (60 ns) to complete.

The AES implementation used is pipelined for optimized throughput. Table 2 shows the proposed architecture's measurements extracted after implementation. The clock frequency is 200MHz which means that each clock period is 5ns. As the architecture is pipelined, the encryption of first cypher text (128 bits) requires 10 clock cycles and 1 clock cycle for every other cyphertext (in the case of 100% utilization). The system's maximum throughput is 25,6 Gbps according to equation (1), where AES bits are 128, Encryption Cycle is 1 (AES pipelined implementation) and Clock Period is 5ns.

$$\text{Throughput} = \text{AES bits} / (\text{Process Cycles} \times \text{Clock Period}) \quad (1)$$

Proposed Architecture	Values
Clock frequency	200 MHz
Clock period	5 ns
Cycles for first AES encryption	10
Cycles for pipelined AES encryption	1
Architecture Throughput	25,6 Gbps

Table 2: Proposed Architecture's post implementation measurements

Table 3 presents the specifications of the camera used in the proposed architecture. The frame size is calculated using Equation (2), where Quality represents the total number of pixels, obtained as the product of 1920 pixels (horizontal resolution) and 1080 pixels (vertical resolution). Each pixel is 18 bits in size, as it is encoded in RGB RAW format.

Camera	Values
Clock frequency	80 MHz
Clock period	12.5 ns
Frame Size	37,324,800 bits
Throughput	640 Mbps

Table 3: Camera's specifications

$$\text{Frame size} = \text{Resolution} \times \text{Size of each pixel} \quad (2)$$

The current experimental setup, the OV2710 camera is configured to transmit data to our system, in a maximum bit rate of 640 Mbps. This throughput is lower than the proposed architecture’s throughput. Therefore, there are no data losses by the proposed architecture, concerning the video data. For the same reason, there are no losses concerning the telemetry data, as they are sent from the FC with rate 115200 bps.

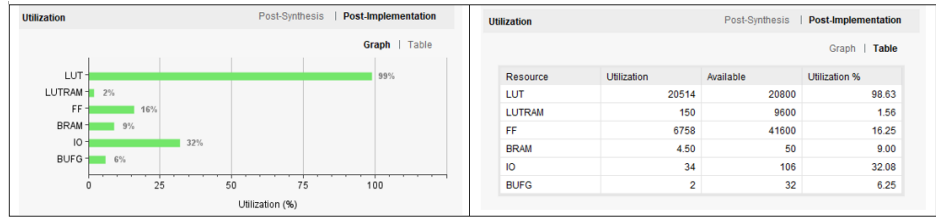


Figure 7: Post-Implementation Utilization

Figure 7 illustrates the utilization of FPGA system resources for the proposed architecture. These metrics, obtained from Vivado, provide insights into how the FPGA's resources, such as logic elements, memory blocks, and input/output pins, are allocated and utilized. This information is critical for evaluating the efficiency of the proposed design and ensuring that the resource usage is within the FPGA's capacity, enabling seamless operation without exceeding hardware limitations.

	FROM	TO	TIME		
	Data Selection	AES Out	Total Delay	Logic Delay	Net Delay
1	AES_Cont_Enc_Dec/AES/register_round5/current_state_reg[112]/C	AES_Cont_Enc_Dec/AES/register_round6/current_state_reg(11)/D	4.884	1.247	3.637
2	AES_Cont_Enc_Dec/AES/register_round5/current_state_reg(21)/C	AES_Cont_Enc_Dec/AES/register_round6/current_state_reg(52)/D	4.769	1.282	3.487
3	AES_Cont_Enc_Dec/AES/register_round5/current_state_reg(107)/C	AES_Cont_Enc_Dec/AES/register_round6/current_state_reg(33)/D	4.766	1.247	3.519
4	AES_Cont_Enc_Dec/AES/in_reg_reg/C	AES_Cont_Enc_Dec/AES/round1_in_reg[51]/CE	4.282	0.419	3.863
5	AES_Cont_Enc_Dec/AES/in_reg_reg/C	AES_Cont_Enc_Dec/AES/round1_in_reg[40]/CE	4.269	0.419	3.850

6	AES_Cont_Enc_Dec /AES/in_reg_reg/C	AES_Cont_Enc_Dec /AES/round1_in_reg[41]/ CE	4.269	0.419	3.850
7	AES_Cont_Enc_Dec /AES/in_reg_reg/C	AES_Cont_Enc_Dec /AES/round1_in_reg[44]/ CE	4.269	0.419	3.850
8	AES_Cont_Enc_Dec /AES/in_reg_reg/C	AES_Cont_Enc_Dec /AES/round1_in_reg[24]/ CE	4.264	0.419	3.845
9	AES_Cont_Enc_Dec /AES/in_reg_reg/C	AES_Cont_Enc_Dec /AES/round1_in_reg[27]/ CE	4.264	0.419	3.845
10	AES_Cont_Enc_Dec /AES/in_reg_reg/C	AES_Cont_Enc_Dec /AES/round1_in_reg[35]/ CE	4.264	0.419	3.845

Table 4: Critical Paths

Table 4 shows the most critical paths of the proposed architecture, which are included in the component for data processing of AES encryption/decryption.

Vivado’s report indicates that the critical path of our proposed architecture is approximately 4.89 ns, which corresponds to a maximum achievable frequency of about 204.49 MHz. This timing margin confirms stable operation at the claimed frequency of 200 MHz.

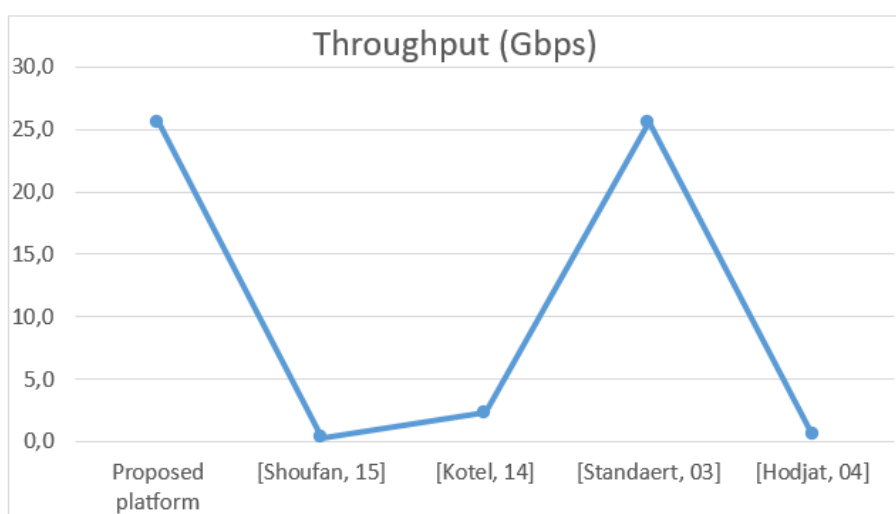


Figure 8: Performance Comparison

Table 5: Power Consumption of Critical Components

5 Conclusions and Discussion

This work presents a novel FPGA-based encryption architecture that integrates both real-time telemetry and video encryption/decryption, providing a secure UAV communication without affecting the system's performance. The proposed architecture uses hardware acceleration to maintain high-speed encryption and decryption while ensuring continuous video transmission and stable UAV operations, without any significant burden on the flight time.

Compared to existing FPGA-based AES implementations, our platform achieves efficient performance in terms of throughput, 25,6Gbps and latency, only 1 clock cycle in pipeline mode, while introducing a crucial advantage, video encryption together with telemetry encryption. Many prior implementations focus on telemetry or video encryption only, whereas our approach integrates both functions using a single pipeline AES module, reducing hardware complexity and resource overhead. This design consumes low power, making it particularly suitable for UAVs.

Finally, this work demonstrates that secure telemetry and real-time video encryption can coexist within a single FPGA-based architecture, without sacrificing throughput, energy efficiency or flight stability because it only burdens 0.081% on overall power consumption.

The reported 0.198 W refers only to the power consumption of our FPGA encryption/decryption module, as estimated by Vivado's power-analysis tool using real switching activity (SAIF) data. Our FPGA architecture does not necessarily consume less power than other hardware architectures. Our architecture exploits the UAV characteristics (video and telemetry encryption/decryption) with no serious decrements in performance and increments in power consumption comparing to existing general purpose architectures.

In our simulation we assumed a fully utilized data path. Meaning that there is zero idle time between sequential encryptions/decryptions. The system's throughput (25,6 Gbps) is by far higher than the minimum demand for 4K video (~3 Gbps). Therefore, no extra power consumption should be considered in the case of video surveillance, as no extra effort is needed for satisfying these demands. For this reason, the ratio Total UAV Power/FPGA Power is not expected to increase.

References

- [Abeywickrama, 18] H. V. Abeywickrama, B. A. Jayawickrama, Y. He and E. Dutkiewicz, "Empirical Power Consumption Model for UAVs," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 2018, pp. 1-5, doi: 10.1109/VTCFall.2018.8690666.
- [Abhishek, 20] Abhishek Sharma, Pankhuri Vanjani, Nikhil Paliwal, Chathuranga M. Wijerathna Basnayaka, Dushantha Nalin K. Jayakody, Hwang-Cheng Wang, P. Muthuchidambaranathan, Communication and networking technologies for UAVs: A survey, *Journal of Network and Computer Applications*, Volume 168,2020,102739, ISSN 1084-8045, <https://doi.org/10.1016/j.jnca.2020.102739>.

- [Altigani, 21] A. Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig and H. T. Elshoush, "A Polymorphic Advanced Encryption Standard – A Novel Approach," in *IEEE Access*, vol. 9, pp. 20191-20207, 2021, doi: 10.1109/ACCESS.2021.3051556.
- [Atoev, 17] S. Atoev, K. -R. Kwon, S. -H. Lee and K. -S. Moon, "Data analysis of the MAVLink communication protocol," *2017 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, Uzbekistan, 2017, pp. 1-3, doi: 10.1109/ICISCT.2017.8188563.
- [Barybin, 19] O. Barybin, E. Zaitseva and V. Brazhnyi, "Testing the Security ESP32 Internet of Things Devices," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 143-146, doi: 10.1109/PICST47496.2019.9061269.
- [Botta, 13] M. Botta, M. Simek and N. Mitton, "Comparison of hardware and software based encryption for secure communication in wireless sensor networks," *2013 36th International Conference on Telecommunications and Signal Processing (TSP)*, Rome, Italy, 2013, pp. 6-10, doi: 10.1109/TSP.2013.6613880.
- [Cheng, 19] X. Cheng, Y. Liu, and C. Chang, "An Ultra-Low Power Encryption Scheme for Secure UAV Communications," *Proceedings of the 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, Beijing, China, pp. 1-6, October 2019.
- [Cornelius, 15] Cornelius A. Thiels, Johnathon M. Aho, Scott P. Zietlow, Donald H. Jenkins, "Use of Unmanned Aerial Vehicles for Medical Product Transport," *Air Medical Journal*, Volume 34, Issue 2, 2015, Pages 104-108, ISSN 1067-991X, <https://doi.org/10.1016/j.amj.2014.10.011>.
- [Dayane, 22] Dayane Reis, Haoran Geng, Michael Niemier, and Xiaobo Sharon Hu. 2022. IM-CRYPTO: An In-Memory Computing Fabric for AES Encryption and Decryption. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2022).
- [Deebak, 20] B.D. Deebak, Fadi Al-Turjman, "A smart lightweight privacy preservation scheme for IoT-based UAV communication systems," *Computer Communications*, Volume 162, 2020, Pages 102-117, ISSN 0140-3664, <https://doi.org/10.1016/j.comcom.2020.08.016>.
- [Desbiens, 23] Desbiens, F. (2023). *The Hardware*. In: *Building Enterprise IoT Solutions with Eclipse IoT Technologies*. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-8882-5_8.
- [Dey, 18] Dey, A.; Nandi, S.; Sarkar, M. Security Measures in IOT based 5G Networks. In *Proceedings of the 2018 3rd International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, 15–16 November 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 561–566.
- [Dipankar, 03] Dipankar Pramanik, Henry H. Kamberian, Christopher J. Proglar, Michael Sanie, David Pinto, "Cost-effective strategies for ASIC masks," *Proc. SPIE 5043, Cost and Performance in Integrated Circuit Creation*, (2 July 2003); doi: 10.1117/12.485280
- [Ghufran, 19] Ghufran Baig, Jian He, Mubashir Adnan Qureshi, Lili Qiu, Guohai Chen, Peng Chen, and Yinliang Hu. 2019. Jigsaw: Robust Live 4K Video Streaming. In *The 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19)*. Association for Computing Machinery, New York, NY, USA, Article 14, 1–16. <https://doi.org/10.1145/3300061.3300127>

- [Giordan, 20] Giordan, D., Adams, M.S., Aicardi, I. et al. The use of unmanned aerial vehicles (UAVs) for engineering geology applications. *Bull Eng Geol Environ* 79, 3437–3481 (2020). <https://doi.org/10.1007/s10064-020-01766-2>
- [Guirado, 21] Guirado, R., Padró, J., Zoroa, A., Olivert, J., Bukva, A., & Cavestany, P. (2021, January 28). StratoTrans: Unmanned Aerial System (UAS) 4G Communication Framework Applied on the Monitoring of Road Traffic and Linear Infrastructure. *Multidisciplinary Digital Publishing Institute*, 5(1), 10-10. <https://doi.org/10.3390/drones5010010>
- [Hodjat, 04] A. Hodjat and I. Verbauwheide, "A 21.54 Gbits/s fully pipelined AES processor on FPGA," 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, Napa, CA, USA, 2004, pp. 308-309, doi: 10.1109/FCCM.2004.1.
- [Hristov, 16] Hristov, G., Zahariev, P., & Beloev, I. (2016, June 1). A Review of the Characteristics of Modern Unmanned Aerial Vehicles. *De Gruyter Open*, 19(2), 33-38. <https://doi.org/10.1515/ata-2016-0008>
- [Iqbal, 18] A. Iqbal and T. Iqbal, "Low-cost and Secure Communication System for Remote Micro-grids using AES Cryptography on ESP32 with LoRa Module," 2018 IEEE Electrical Power and Energy Conference (EPEC), Toronto, ON, Canada, 2018, pp. 1-5, doi: 10.1109/EPEC.2018.8598380.
- [Jahanirad, 23] Jahanirad, Hadi. (2023). Dynamic power-gating for leakage power reduction in FPGAs. *Frontiers of Information Technology & Electronic Engineering*. 24. 582-598. doi:10.1631/FITEE.2200084.
- [Jawhar, 17] Jawhar, I., Mohamed, N., Al-Jaroodi, J., Agrawal, D P., & Zhang, S. (2017, February 27). Communication and networking of UAV-based systems: Classification and associated architectures. Elsevier BV, 84, 93-108. <https://doi.org/10.1016/j.jnca.2017.02.008>
- [Kim, 21] Kim, K., & Kang, Y. (2020, October 21). Drone security module for UAV data encryption. <https://doi.org/10.1109/ictc49870.2020.9289387>
- [Kotel, 14] Kotel, Sonia & Zeghid, Medien & Baganne, Adel & Saidani, Taoufik & Daradkeh PhD., P.Eng, Dr.Yousef & Tourki, Rached. (2014). FPGA-Based Real-Time Implementation of AES Algorithm for Video Encryption. *Recent Advances In Telecommunications, Informatics And Educational Technologies*.
- [Koubâa , 19] A. Koubâa, A. Allouch, M. Alajlan, Y. Javed, A. Belghith and M. Khalgui, "Micro Air Vehicle Link (MAVlink) in a Nutshell: A Survey," in *IEEE Access*, vol. 7, pp. 87658-87680, 2019, doi: 10.1109/ACCESS.2019.2924410.
- [Kwon , 18] Y. -M. Kwon, J. Yu, B. -M. Cho, Y. Eun and K. -J. Park, "Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles," in *IEEE Access*, vol. 6, pp. 43203-43212, 2018, doi: 10.1109/ACCESS.2018.2863237.
- [Lee, 10] W. Lee, K. Noh, S. Kim and J. Heo, "Efficient cooperative transmission for wireless 3D HD video transmission in 60GHz channel," in *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, pp. 2481-2488, November 2010, doi: 10.1109/TCE.2010.5681131.
- [Li, 17] Li, L.; Li, S. High throughput AES encryption/decryption with efficient reordering and merging techniques. In *Proceedings of the 2017 27th International Conference on Field Programmable Logic and Applications (FPL)*, Gent, Belgium, 4–6 September 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–4.
- [Li, 22] T. Li et al., "Energy-Efficient and Secure Communication Toward UAV Networks," in *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 10061-10076, 15 June 2022, doi: 10.1109/JIOT.2021.3118079.

- [Liuzza, 18] Liuzza, Davide & Silano, Giuseppe & Picariello, Francesco & Iannelli, Luigi & Glielmo, Luigi & De Vito, Luca & Daponte, P. (2018). A review on the use of drones for precision agriculture. *IOP Conference Series: Earth and Environmental Science*. 275. 10.1088/1755-1315/275/1/012022.
- [Molina, 22] R. S. Molina, V. Gil-Costa, M. L. Crespo and G. Ramponi, "High-Level Synthesis Hardware Design for FPGA-Based Accelerators: Models, Methodologies, and Frameworks," in *IEEE Access*, vol. 10, pp. 90429-90455, 2022, doi: 10.1109/ACCESS.2022.3201107.
- [Mozaffari, 19] M. Mozaffari, W. Saad, M. Bennis, Y. -H. Nam and M. Debbah, "A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2334-2360, thirdquarter 2019, doi: 10.1109/COMST.2019.2902862.
- [Nooruddin, 23] M. Nooruddin and D. Valles, "An Advanced IoT Framework for Long Range Connectivity and Secure Data Transmission Leveraging LoRa and ASCON Encryption," 2023 *IEEE World AI IoT Congress (AIoT)*, Seattle, WA, USA, 2023, pp. 0583-0589, doi: 10.1109/AIIoT58121.2023.10174401.
- [Nosheen, 20] S. Nosheen and J. Y. Khan, "High Throughput and QoE Fairness Algorithms for HD Video Transmission over IEEE802.11ac Networks," 2020 *International Conference on Computing, Networking and Communications (ICNC)*, Big Island, HI, USA, 2020, pp. 84-89, doi: 10.1109/ICNC47757.2020.9049818.
- [Podder, 21] R. Podder and R. K. Barai, "Hybrid Encryption Algorithm for the Data Security of ESP32 based IoT-enabled Robots," 2021 *Innovations in Energy Management and Renewable Resources (52042)*, Kolkata, India, 2021, pp. 1-5, doi: 10.1109/IEMRE52042.2021.9386824.
- [Prapulla, 16] Prapulla, N., Veena, S., & Srinivasalu, G. (2016, May 1). Development of algorithms for MAV security. , 9, 799-802. <https://doi.org/10.1109/rteict.2016.7807936>
- [Rajasekar, 16] Rajasekar, P.; Haridas, M. Efficient FPGA implementation of AES 128 bit for IEEE 802.16e mobile WiMax standards. *Circuits Syst*. 2016, 7, 371–380.
- [Schwabe , 17] Schwabe, P., & Stoffelen, K. (2017, January 1). All the AES You Need on Cortex-M3 and M4. *Springer Science+Business Media*, 180-194. https://doi.org/10.1007/978-3-319-69453-5_10
- [Setiawan, 21] F. B. Setiawan and Magfirawaty, "Securing Data Communication Through MQTT Protocol with AES-256 Encryption Algorithm CBC Mode on ESP32-Based Smart Homes," 2021 *International Conference on Computer System, Information Technology, and Electrical Engineering (COSITE)*, Banda Aceh, Indonesia, 2021, pp. 166-170, doi: 10.1109/COSITE52651.2021.9649577.
- [Shakhatreh, 19] Shakhatreh, Hazim & Sawalmeh, Ahmad & Al-Fuqaha, Ala & Dou, Zuochao & Almaitta, Eyad & Khalil, Issa & Othman, Noor & Khreishah, Abdallah & Guizani, Mohsen. (2019). Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges. *IEEE Access*. 7.
- [Shoufan, 15] Shoufan, Abdulhadi & Alnoon, Hassan & Baek, Joonsang. (2015). Secure Communication in Civil Drones. 10.1007/978-3-319-27668-7_11.
- [Standaert, 03] Standaert, FX., Rouvroy, G., Quisquater, JJ., Legat, JD. (2003). Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs. In: Walter, C.D., Koç, Ç.K., Paar, C. (eds) *Cryptographic Hardware and Embedded Systems - CHES 2003*. CHES 2003. *Lecture Notes in Computer Science*, vol 2779. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-45238-6_27

- [Suryanegara, 15] Suryanegara, M., Asvial, M., & Raharya, N. (2015, September 1). System engineering approach to the communications technology at unmanned aircraft system (UAS). , 475-480. <https://doi.org/10.1109/syseng.2015.7302800>
- [Tian, 18] Tian, X., Fan, C., Liu, J., Ding, Q. (2018). Design and Implementation of Network Video Encryption System Based on STM32 and AES Algorithm. In: Pan, JS., Tsai, PW., Watada, J., Jain, L. (eds) *Advances in Intelligent Information Hiding and Multimedia Signal Processing. IHH-MSP 2017. Smart Innovation, Systems and Technologies*, vol 82. Springer, Cham. https://doi.org/10.1007/978-3-319-63859-1_7
- [Tkáč, 19] Tkáč, Matúš & Mésároš, Peter. (2019). Utilizing drone technology in the civil engineering. *Selected Scientific Papers - Journal of Civil Engineering*. 14. 27-37. 10.1515/sspjce-2019-0003.
- [Townsend, 17] T. Townsend and B. Nelson, "Vivado design interface: An export/import capability for Vivado FPGA designs," 2017 27th International Conference on Field Programmable Logic and Applications (FPL), Ghent, Belgium, 2017, pp. 1-7, doi: 10.23919/FPL.2017.8056809.
- [Tsai, 18] K. -L. Tsai, Y. -L. Huang, F. -Y. Leu, I. You, Y. -L. Huang and C. -H. Tsai, "AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments," in *IEEE Access*, vol. 6, pp. 45325-45334, 2018, doi: 10.1109/ACCESS.2018.2852563.
- [Visconti, 20] Visconti, P.; Capoccia, S.; Venere, E.; Velázquez, R.; Fazio, R.d. 10 Clock-Periods Pipelined Implementation of AES-128 Encryption-Decryption Algorithm up to 28 Gbit/s Real Throughput by Xilinx Zynq UltraScale+ MPSoC ZCU102 Platform. *Electronics* 2020, 9, 1665. doi:10.3390/electronics9101665
- [Wagner, 23] M. Wagner and A. A. Fröhlich, "Securing Cyber-Physical Systems Against GPS Spoofing Attacks Using Confidence Attribution," 2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2023, pp. 1-6, doi: 10.23919/SoftCOM58365.2023.10271629.
- [Xilinx, 22] Artix 7 Series Product Selection Guide. https://docs.xilinx.com/v/u/en-US/ds181_Artix_7_Data_Sheet
- [Yu, 21] T. Yu, S. Imada, K. Araki and K. Sakaguchi, "Multi-UAV Full-Duplex Communication Systems for Joint Video Transmission and Flight Control," 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), NV, USA, 2021, pp. 1423-1428, doi: 10.1109/CCWC51732.2021.9375952.
- [Zeng, 19] Zeng, Y., Wu, Q., & Zhang, R. (2019, December 1). *Accessing From the Sky: A Tutorial on UAV Communications for 5G and Beyond*. Institute of Electrical and Electronics Engineers, 107(12), 2327-2375. <https://doi.org/10.1109/jproc.2019.2952892>
- [Zhang, 20] Z. Zhang, S. Wang, Q. Gu, and L. Ma, Low-Power High-Speed Parallel Encryption Algorithm for UAV Remote Sensing Images, *Sensors*, vol. 20, no. 11, p. 3052, May 2020.