



SoC FPGA-Based Rapid Prototyping of Compressed, Secured and Wireless Image Transmission for Wildlife Surveillance System

Muhammad Muzakkir Mohd Nadzri^{1*}, Afandi Ahmad¹

¹Reconfigurable Computing for Analytics Acceleration (ReCAA) Research Laboratory, Microelectronic and Nanotechnology-Shamsuddin Research Centre (MiNT-SRC), Universiti Tun Hussein Onn Malaysia (UTHM), 86400 Batu Pahat, Johor, MALAYSIA.

*Corresponding Author

DOI: <https://doi.org/10.30880/ijie.2022.14.04.021>

Received 31 May 2021; Accepted 11 October 2021; Available online 20 June 2022

Abstract: Wildlife plays an important role in balancing the earth's ecosystem. Today, many species of wildlife are threatened with extinction. Images are important input data for wildlife surveillance technology, which allows real situations in the field to be observed and analysed. This project proposed a wireless transmission system of compressed and secured images using the SoC FPGA platform for improving the existing system in terms of image data collection. Image compression ensured that the proposed system was efficient in terms of data processing, transmission and storage. Image data encryption aimed at ensuring that the security of the transmitted image data would not be hijacked by poachers or non-authorities and ultimately this system would transmit compressed and secured images wirelessly to provide real-time data. The prototype used LabVIEW 2017 software and NI myRIO (as image transmitter) and a computer (as image receiver) hardware. This platform has been utilised for the development of the architectural design of a compression system using the discrete cosine transform (DCT) method, the development of an encryption system using the advanced encryption standards (AES) method and wireless transmission using Wi-Fi. The implementation of DCT on the field-programmable gate array (FPGA) platform allowed the images to be compressed by an average of 44% to shorten the time used in the transmission process. The AES method guaranteed data security with images that can only be viewed when using the correct password. Combining both the DCT and AES methods, the rapid prototyping of the wireless transmission of compressed and secured images for a wildlife surveillance system equipped with a motion sensor and a camera was developed to detect motion, capture images and transmit three (3) different image resolutions at distances of up to 60 m.

Keywords: Wildlife surveillance system, discrete cosine transform (DCT), advanced encryption standards (AES), system-on-a-chip (SoC), field-programmable gate array (FPGA), wireless image transmission, LabVIEW

1. Introduction

Wildlife crime is the illegal taking, trading, exploiting, possessing or killing of animals or plants in contravention of national or international laws [1]. Many wildlife habitats have been lost due to human exploitation for establishing buildings, farms, roads and industrial development. As earth's important living entity, wildlife plays a major role in sustaining the biodiversity of earth's ecosystem, but greedy and irresponsible humans have caused wildlife destruction through wildlife crime and habitat loss. Serious efforts must be put into wildlife issues to avoid wildlife extinction. The Living Planet Report 2018 by World Wildlife Fund (WWF) reported that the global Living Planet Index (LPI) indicated a 60% overall decrease in the global populations of birds, fish, mammals, amphibians and reptiles between 1970 and 2014 [2]. To highlight the significance and criticality of this issue, the International Union for Conservation of Nature

*Corresponding author: muzakkirnadzri@gmail.com

(IUCN) has categorised at-risk wildlife species into seven (7) categories: least concern, near threatened, vulnerable, endangered, critically endangered, extinct in the wild and extinct [3].

To solve these problems, the wildlife surveillance system (WSS) plays an important role in monitoring, tracking, securing and gathering field data to perform systematic and integrated planning towards wildlife conservation. There is a huge gap in improving the existing WSS, shown in Fig. 1, especially in terms of image data collection. The stored image data in the memory card is manually collected, which demands the worker to go into the field. This task is very unsafe, unpredictable, human-based, skill-subjective and time-consuming. The present system is also incapable of delivering real-time alerts, where no instant plan can be carried out immediately, for example, if there is the presence of poachers [4–6]. Images are the most important data collected in the WSS that ensure a complete and effective overview of the field being monitored [5, 7–11].



Fig. 1 - The current system uses a trap camera [12]

The development goal of this rapid prototyping is to compress, secure and wirelessly transmit images to overcome some problems of the existing system. NI myRIO is a prototyping hardware/software platform that has the ability to design real systems more quickly than ever before. Complete with the latest Zynq system-on-a-chip (SoC) technology from Xilinx, NI myRIO is integrated with a dual-core ARM® Cortex™-A9 processor and an FPGA with 28,000 programmable logic cells, 10 analogue inputs, 6 analogue outputs, audio I/O channels and up to 40 lines of digital input/output (DIO).

The higher computational complexities of an image compression system using the discrete cosine transform (DCT) method was implemented on the field-programmable gate array (FPGA) platform to improve system efficiency by minimising image size and transmission time. Reconfigurable hardware (RH) in the form of FPGA is an ideal candidate to implement this technology. The advantages of FPGA, such as vast parallelism capabilities, multimillion gate counts and special low-power packages, will reduce the use of memory, computational complexity and power consumption [13] to meet the requirements of this application. The images were secured by the utilisation of the advanced encryption standards (AES) method to encrypt the data and ensure security during image data transmission. The AES encryption and the wireless image transmission were processed using the ARM® processor. Lastly, the compressed and secured images were transmitted wirelessly using Wi-Fi for real-time implementation.

The rest of the paper is structured as follows. The proposed system architecture is presented in Section 2. Details of the experiment's results and analysis are discussed in Section 3. Finally, the conclusion and recommendations for future works are provided in Section 4.

2. Proposed System Architecture

The prototype is divided into two (2) main parts: the transmitter and the receiver. Each part comprises of the input, processing unit and output. Fig. 2 shows an illustration of the prototype, as well as the input, processing unit and output of the hardware and software used in each part. There are three (3) main types of hardware used in the transmitter part, which are the HCSR-05 motion sensor, the Logitech C170 web camera and NI myRIO-1900. The HCSR-05 motion sensor and the Logitech C170 web camera were hardware that provided input data to the system, while NI myRIO-1900 equipped with the Zynq SoC platform acted as the processor to process the input data.

The hardware used in the receiver part is the HP Elite Book 820 computer as the processor for receiving and storing images. The overall design and implementation of the system in both parts are programmed using the NI LabVIEW 2017 software. NI LabVIEW 2017 uses a graphical (G) programming language that is different from the usual text-based programming language, in that it is easy to understand and to locate and solve the programming error. The graphical user interfaces (GUIs) on both parts were also designed simultaneously with G programming as the platform to control and monitor the system. The implementation process of the system can be monitored easily with the presence of the GUIs.

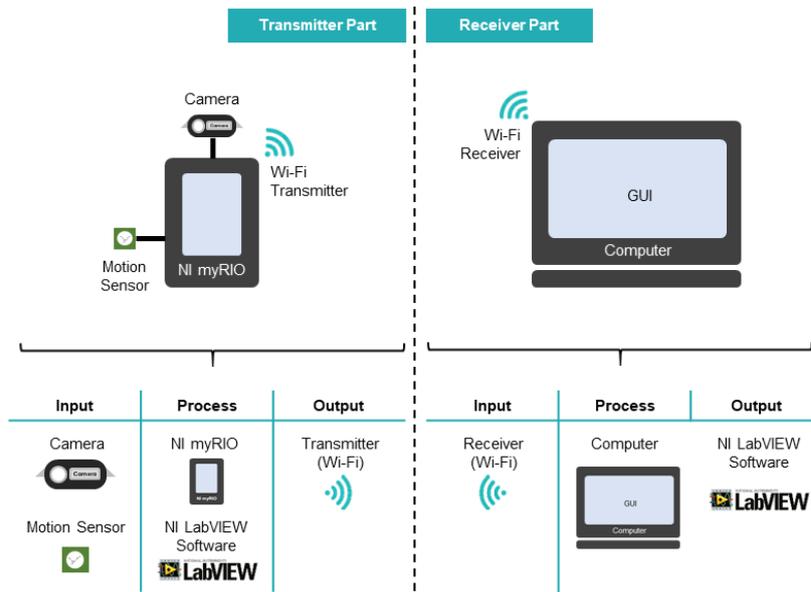


Fig. 2 - Input, process and output for each part

The block diagram in Fig. 3 describes the overall architectural design of the prototype to compress, secure and transmit images wirelessly. For the transmitter part, the motion sensor input is used as a trigger system to activate the camera. When the motion sensor detects any movement, the camera will be activated to capture the image. The captured image will then be processed by the NI myRIO platform. NI myRIO with the SoC hybrid system, incorporating the LabVIEW RT processor and LabVIEW FPGA, will implement DCT-based image compression and image data encryption using the AES method before transmitting the image wirelessly using Wi-Fi.

For the receiver part, the image transmitted is received by the built-in Wi-Fi on the computer. The computer as the processor will execute the AES decryption and image decompression using an inverse DCT algorithm to produce the actual image sent by the transmitter. The image will be later saved and displayed on the monitor screen.

Due to the limitation of FPGA resources, the DCT algorithm as the most complex computation is chosen to utilise the FPGA's parallelism capabilities to accelerate the process. DCT-based image compression is programmed using VHDL programming and targeted to the Xilinx Zync-7010 board in NI myRIO, while the AES and other processes is using the processor dual-core ARM® Cortex™-A9 processor.

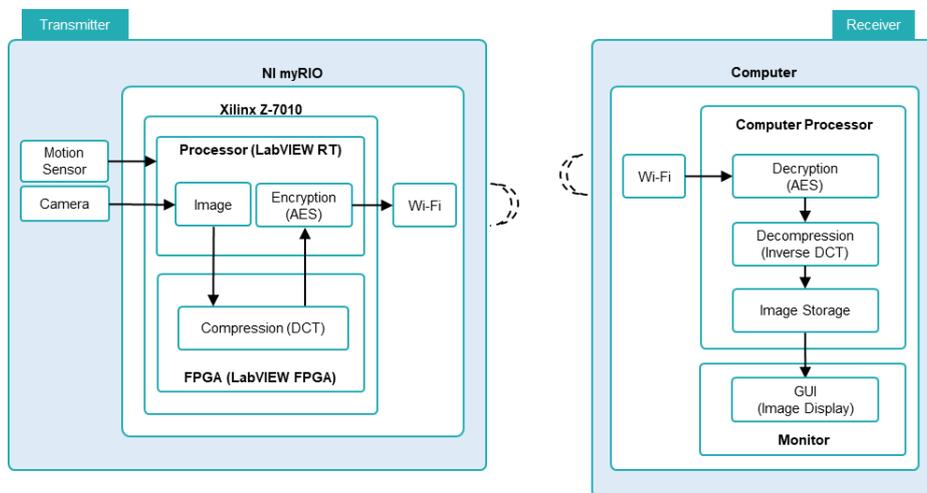


Fig. 3 - Prototype system's block diagram

2.1 Image Compression Using DCT

The design and implementation of image compression were performed using the discrete cosine transform (DCT) method on the FPGA platform. A two-dimension (2D) DCT algorithm with lossy type of compression provides the maximum compression. Image compression is needed to ensure that the transmission of images for the proposed WSS is

effective for data processing, storage and transmission. The compression process was programmed as the earliest task in the system to reduce image size, hence giving an advantage to the next task by having smaller image data to process.

In this study, 2D DCT-based image compression was selected as one of the key factors that could improve the efficiency of the system. DCT is a rapid transform method that is broadly used for image compression [14]. In addition, DCT is a discrete transform with a lossy compression method that is specially designed to remove image data information that cannot be seen by human vision [15]. In the wildlife surveillance system, it is sufficient that the image received by the user reveals the presence of animals or humans in the monitored field. This is different than, for example, images for the medical field, which require full information of the image data. By using the lossy compression method, image size can be reduced more than by using the lossless compression method. DCT's performance is also good in terms of time saving and energy consumption [16].

The DCT implementation in this study used LabVIEW FPGA, as in [17], as the LabVIEW software offers a hybrid method (graphical programming and VHDL) compared with traditional methods, which use fully VHDL programming. Direct memory access (DMA) uses the first-in first-out (FIFO) method with high-speed data transfer is fully utilised to stream the data. The feature of component-level IP node (CLIP) offered by LabVIEW FPGA is inserted with the executed VHDL program. The VHDL program must be first compiled using Xilinx ISE 14.7 included in the LabVIEW 2017 software. Fig. 4 shows the G programming of the DCT implementation using LabVIEW FPGA.

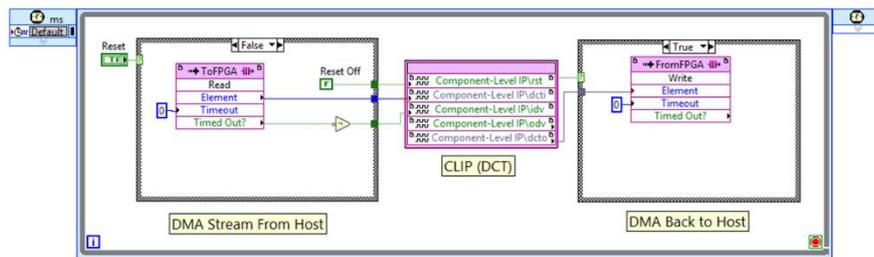


Fig. 4 - G programming of LabVIEW FPGA

2.2 Image Encryption Using AES

To ensure image data were transmitted safely, image data encryption using the advanced encryption standards (AES) method was implemented in the system. AES algorithm ensures data integrity by converting image data into other sets of data that can only be viewed using the correct password. AES is a symmetrical type of cryptography that uses the same password or key for both the encryption and decryption processes. For the transmitter part, image data will be encrypted with the entered password, and for the receiver part, the same password must be used to decrypt and retrieve the original data image. As long as the secret key or password used by the user is not compromised, the symmetrical type of encryption is secured and protected. In addition, symmetric encryption is much faster than the asymmetric encryption technique, as it requires less computational process [18]. Fig. 5 shows the whole system of the rapid prototyping, which encompassed both the transmitter and receiver parts.

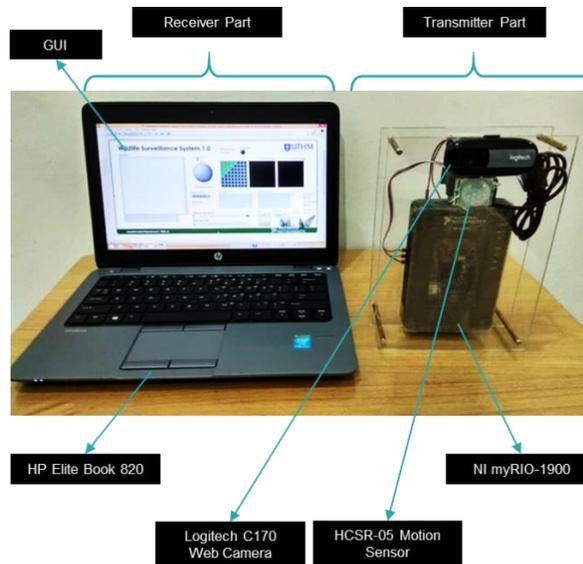


Fig. 5 - Overall rapid prototyping

3. Experiment's Results and Analysis

The results and analysis of the prototype in this section are divided into four (4) parts, which are software development, DCT image compression evaluation, AES evaluation and wireless image transmission evaluation.

3.1 Software Development

The software development of the proposed system used LabVIEW 2017 software for both the hardware platforms NI myRIO (transmitter) and the computer (receiver). NI LabVIEW 2017 is divided into three (3) main modules: LabVIEW FPGA, LabVIEW RT and LabVIEW Windows. LabVIEW FPGA and LabVIEW RT were the modules used in the NI myRIO platform, while LabVIEW Windows is the module used with the computer. In this system, the interaction between each module occurred because the images will be sent from LabVIEW RT to LabVIEW FPGA for the image compression process and then back to LabVIEW RT for the encryption process before transmitting to the computer through Wi-Fi. The images would be received by the computer and processed using LabVIEW Windows for decryption, decompression, storage and display. Fig. 6 shows the block diagram of the interaction between the three (3) NI LabVIEW 2017 modules.

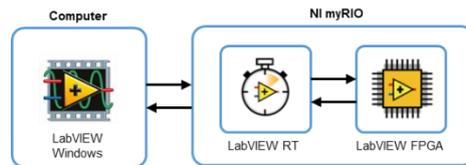


Fig. 6 - Interaction between three (3) NI LabVIEW 2017 modules

Fig. 7 shows the GUIs of the proposed system, which were built on the NI LabVIEW platform as the transmitter and on the computer as the receiver. Several sections on the GUIs were created, such as a section to display the original image captured, a notification part for the motion sensor, connectivity to the computer and buttons to stop the system. For encryption and decryption purposes, there are three (3) options of key lengths with passwords that can be set by the user. There is also a part that displays normal text and encrypted text to let the user know the status of the encrypted image. The execution time in milliseconds for each process is also displayed, including the compression, encryption and overall processes. On the computer, the file directory section can be set to store the images.



Fig. 7 - (a) GUI for the transmitter part; (b) GUI for the receiver part

Fig. 8(a) shows part of the G programming to save the images on the computer. The images will be saved according to the file directory set by the user and renamed using the format of day, date and time of receiving the images. This process is beneficial for further data arrangement, reference and analysis. The images, after renamed into day, date and time to be saved in the computer, are as shown in Fig. 8(b).

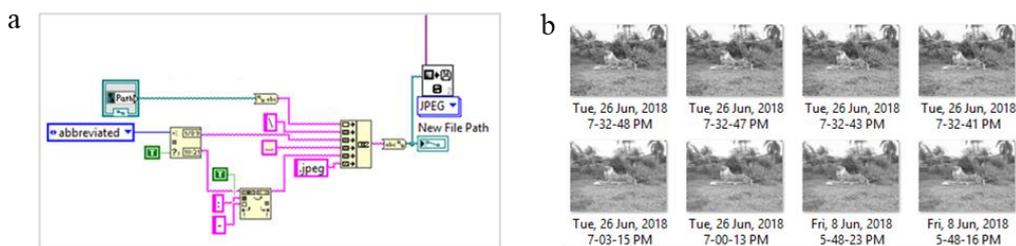


Fig. 8 - (a) Graphical code for storing images; (b) images renamed into day, date and time for storage

3.2 DCT Image Compression Evaluation

Image compression in the proposed system was implemented using the DCT method and executed on the FPGA platform. By using the DCT method, the image would look similar to the human vision before and after being compressed, even though some data information were removed from the real image. The comparison between original images and reconstructed images after being compressed using DCT is shown in Table 1.

Table 1 - Comparison between original and compressed images

Image Resolution	Original Image	Compressed Image
160 × 120	 7.70 KB	 4.47 KB
320 × 240	 38.6 KB	 20.8 KB
640 × 480	 127.0 KB	 69.2 KB

The reconstructed image quality was assessed using the PSNR formula as in Equation (1), with mean square error (MSE) representing the cumulative square error between the original and the reconstructed images. The R notation represents the maximum fluctuations in the input data image. In this system, the input data for grayscale images used 8-bit unsigned integer with the maximum R value of 255 [19]. A value between 30 dB to 50 dB is generally the common value of PSNR for image processing [20]. An increased PSNR value indicates higher quality of the reconstructed image. The PSNR and MSE values for three (3) types of image resolutions were recorded, as shown in Table 2.

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \tag{1}$$

Table 2 - PSNR value for each image resolution

Image Resolution	MSE	PSNR (dB)
160 × 120	6.734	27.967
320 × 240	1.661	40.159
640 × 480	2.748	35.679

The comparison of image sizes between compressed and uncompressed images is shown in Table 3. The system successfully compressed the images to almost half the original images’ size for three (3) types of image resolution. The space saving in terms of percentage is also tabulated in the table.

Table 3 - Image size and space saving of compressed and original images

Image Resolution	Image Size (kB)		Space Saving (%)
	Original	Compressed	
160 × 120	7.70	4.47	41.95
320 × 240	38.6	20.8	46.11
640 × 480	127.0	69.2	45.51

The performance of the FPGA was assessed in terms of area (slices) and maximum frequency (MHz). The proposed system’s implementation was compared with other existing implementations, as shown in Table 4. The result obtained shows that the area and frequency of the proposed DCT algorithm in this prototype were lower compared with the existing works of [21, 22].

Table 4 - Comparison of proposed FPGA-based DCT with existing works

Parameter	Proposed	[21]	[22]
FPGA device	Xilinx Zync-7010	Xilinx Virtex-4	Xilinx Spartan-3E
Area (slices)	4017	7260	4327
Maximum frequency (MHz)	40.000	308.182	89.469

The image compression system using the DCT algorithm was successfully developed in this prototype. The calculation process of the DCT algorithm using the FPGA platform compressed images by up to an average of 44%. This compression performance is significant towards a more effective system and give advantage for other processes, such as data transmission and data storage. The image quality result is adequate for the WSS applications that are based on lossy image compression with the posted PSNR value of between 27 dB to 42 dB.

3.3 AES Evaluation

The performance of the AES method was evaluated based on the parameters shown in Fig. 9.

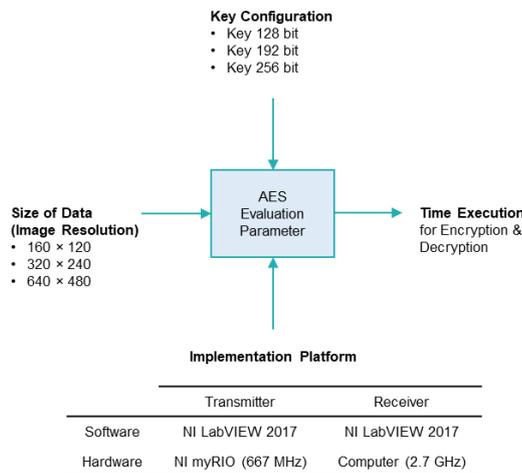


Fig. 9 - AES evaluation parameters

AES evaluation was carried out using three (3) input parameters and one (1) output parameter. The first input parameter is the size of the input data (image), where three (3) image resolutions were used in this prototype. Implementation platform is the second input parameter, where the software used was the NI LabVIEW 2017, while the hardware used were NI myRIO as the transmitter and the computer as the receiver. The third input parameter is the key configuration. There are three (3) types of key lengths for the AES system. The output of these three (3) inputs parameters is the execution time for the encryption and decryption processes. Fig. 10 shows the execution time based on the three (3) input parameters.

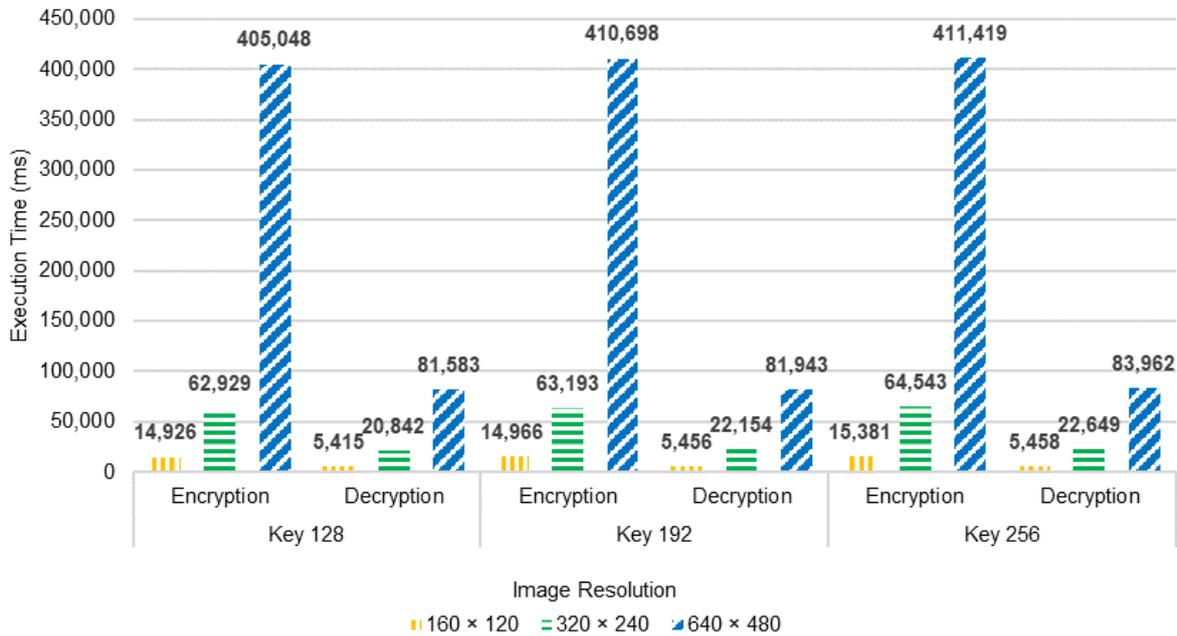


Fig. 10 - Execution time based on AES parameters

From the AES evaluation, there are three (3) considerations to implement AES as follows:

1. the higher the image resolution, the higher was the time taken for the encryption and decryption processes. This is due to the higher-resolution image having higher bits of data to be processed, which increased the time required for both the encryption and decryption processes of the AES method;
2. using a key with higher bits increased the time for encryption and decryption. This is because the increased length of the key would increase the number of cycles of both the encryption and decryption processes of the AES method. The number of cycles for keys 128, 192 and 256 were 10, 12 and 14 cycles, respectively; and
3. The implementation time of the AES method is influenced by the computational speed of the hardware involved. For example, as the computer hardware used a processor with a higher speed, the decryption execution time were shorter compared with encryption execution that using the NI myRIO platform.

3.4 Wireless Image Transmission Evaluation

The rapid prototyping of compressed, secure and wireless image transmission for the wildlife surveillance system was evaluated with three (3) different wireless transmission ranges of 0, 30 and 60 m between the transmitter and the receiver. The execution time for each distance was recorded. Table 5 shows the result of wireless image transmission at three (3) different ranges with different image resolutions and key lengths for the overall implementation.

The result as shown in Table 5 indicates that the motion was successfully detected and the images were successfully delivered from the transmitter to the receiver wirelessly at a distance of up to 60 m. The distance between NI myRIO (transmitter) and the computer (receiver) affected the system by increasing the execution time at longer distances. Other than that, the larger the image resolution and key length, the higher was the time required for the transmission process of the compressed image. Table 5 also recorded that the image size transmitted was not affected by different ranges and key lengths, as the compressed image size received was unchanged.

Table 5 - Prototype's execution time at three (3) different ranges

Image Resolution	Key	Transmission Time Execution (ms)		
		Range 0 m	Range 30 m	Range 60 m
160 × 120	Key 128	19,773	20,002	20,008
	Key 192	20,185	20,451	20,459
	Key 256	21,644	22,001	22,006
320 × 240	Key 128	78,749	80,432	80,379
	Key 192	79,663	81,892	82,002
	Key 256	80,944	83,062	83,064
640 × 480	Key 128	389,012	394,836	395,188
	Key 192	391,005	394,952	395,027
	Key 256	392,119	396,378	396,408

4. Conclusion and Future Works

In the wildlife surveillance system, image input data are important data required by the authorities to monitor the wildlife. A rapid prototyping system architecture using SoC FPGA that provides higher integration, lower power, smaller board size and higher bandwidth communication between the processor and the FPGA platform has been proposed in this study for efficient image transmission for the wildlife surveillance system.

The prototype with an image compression system using the DCT method on the FPGA platform was implemented and succeeded in improving system efficiency by minimising image size and transmission time. The implementation of the lossy compression system using the DCT method also maximised the size reduction of image data. With the size of the image successfully reduced, the transmission time was also shortened.

The implementation of image data encryption using the AES method was also developed in the proposed prototype. The use of the AES method ensured that the security of the image data being transmitted would only be readable and viewed if the password was correct.

The rapid prototyping of the compressed, secured and wireless image transmission for the wildlife surveillance system was developed equipped with a motion sensor and a camera for the input data. The developed prototype was capable of detecting movements, which acted as the trigger to capture images. The captured images were then processed using the NI myRIO platform for the compression and encryption processes before being sent wirelessly using Wi-Fi. The images sent wirelessly were received by the computer for the decryption and decompression processes.

Future improvements, such as image detection and classification, are suggested to improve the system on whether to transmit or store the images in the device when power consumption is high during the transmission process. Energy efficiency in terms of wireless image transmission and the implementation of a wireless sensor network topology should be further explored to transmit images at longer distances.

Acknowledgement

The authors would like to thank Universiti Tun Hussein Onn (UTHM) for funding this research work via the Postgraduate Research Grant Scheme (PRGS-U456) and National Instruments Virtual Instrument & System Innovation Sdn. Bhd (NI VISI) for hardware support.

References

- [1] Kurland, J., Pires, S. F., Mcfann, S. C., & Moreto, W. D. (2017). Wildlife crime: conceptual integration, literature review, and methodological critique. *Crime Science*, 6(4), 1–15. <https://doi.org/10.1186/s40163-017-0066-0>
- [2] WWF. (2018). Living Planet Report - 2018: Aiming higher. *Environmental Conservation* (Vol. 26). <https://doi.org/10.1080/09528820802312343>
- [3] IUCN Red List. (2008). The IUCN Red List of Threatened Species.
- [4] Sabine, J. B., Meyers, J. M., & Schweitzer, S. H. (2005). A Simple, Inexpensive Video Camera Setup for the Study of Avian Nest Activity. *Journal of Field Ornithology*, 76(3), 293–297.
- [5] Newbery, K. B., & Southwell, C. (2008). An automated camera system for remote monitoring in polar environments. *Cold Regions Science and Technology*, 55(2009), 47–51.
- [6] He, Z. (2009). Energy-efficient integrated camera and sensor system design for wildlife activity monitoring. *Proceedings - 2009 IEEE International Conference on Multimedia and Expo, ICME 2009*, 1580–1581.

- [7] He, Z., Eggert, J., Cheng, W., Zhao, X., Millspaugh, J., Moll, R., Sartwell, J. (2008). Energy-aware portable video communication system design for wildlife activity monitoring. *IEEE Circuits and Systems Magazine*, 25–37.
- [8] Chen, C.-P., Lin, C.-H., Lai, T.-W., Chuang, C.-L., Lin, T.-S., Jiang, J.-A., Hong, C.-H. (2011). Energy-Efficient Visual Eyes System for Wildlife. *IEEE 13th International Conference on High Performance Computing and Communications (HPCC)*, 869–874.
- [9] Zhang, L. (2011). An IOT System for Environmental Monitoring and Protecting with Heterogeneous Communication Networks. *6th International ICST Conference on Communications and Networking in China (CHINACOM)*, 1026–1031.
- [10] Edemacu, K., Kim, J. W., Jang, B., & Park, H. K. (2019). Poacher detection in African game parks and reserves with IoT: Machine learning approach. In *Proceedings - 2019 7th International Conference on Green and Human Information Technology, ICGHIT 2019* (pp. 12–17). IEEE.
- [11] Song, Y., Wang, H., Li, S., Xu, F., & Liu, J. (2019). CNN Based Wildlife Recognition with Super-Pixel Segmentation for Ecological Surveillance. *8th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, CYBER 2018*, 132–137. <https://doi.org/10.1109/CYBER.2018.8688356>
- [12] World Wide Fund for Nature. (2017). Camera Traps. Retrieved February 9, 2017, from <http://www.worldwildlife.org/initiatives/camera-traps>
- [13] Taha, H., Sazish, A. N., Ahmad, A., Sharif, M. S., & Amira, A. (2010). Efficient FPGA Implementation of a Wireless Communication System using Bluetooth Connectivity. In *Circuits and Systems (ISCAS), Proceedings of 2010 IEEE International Symposium on* (Vol. 4, pp. 171–182).
- [14] Chakraborty, P. (2012). A Survey Analysis for lossy image compression using Discrete cosine Transform. *International Journal of Scientific & Engineering Research*, 3(9), 1–6.
- [15] Jindal, H., & Mandal, D. (2012). Performance Analysis of Image Compression using Discrete Cosine Transform with Various Discrete Wavelet Transform. *Journal of Global Research in Computer Science*, 3(1), 13–16.
- [16] Katharotiya, A., Patel, S., & Goyani, M. (2011). Comparative Analysis between DCT & DWT Techniques of Image Compression. *Journal of Information Engineering and Applications*, 1(2), 9–18. Retrieved from www.iiste.org
- [17] Mohd Nadzri, M. M., Ahmad, A., & Amira, A. (2018). Exploiting LabVIEW FPGA in Implementation of DCT-based Wireless Image Transmission for Wildlife Surveillance System. In *2018 IEEE 16th Student Conference on Research and Development, SCORED 2018* (pp. 2–6). IEEE. <https://doi.org/10.1109/SCORED.2018.8710849>
- [18] Amalraj, A. J., & Jose, J. J. R. (2016). A Survey Paper on Cryptography Techniques. *International Journal of Computer Science and Mobile Computing*, 5(8), 55–59.
- [19] Horé, A., & Ziou, D. (2010). Image quality metrics: PSNR vs. SSIM. In *International Conference on Pattern Recognition* (pp. 2366–2369). <https://doi.org/10.1109/ICPR.2010.579>
- [20] Welstead, S. T. (1999). *Fractal and wavelet image compression techniques*. SPIE Optical Engineering Press.
- [21] Do, T. T. T., & Nguyen, B. P. (2010). A High-Accuracy and High-Speed 2-D 8x8 Discrete Cosine Transform Design. In *Proceedings of ICGCRCICT* (Vol. 1, pp. 135–138).
- [22] Jeevan, B., Bhatt, C. N., Krishna, C. V., & Sivani, K. (2014). FPGA implementation of secure image compression with 2D-DCT using Verilog HDL. In *Proceedings of the IEEE International Caracas Conference on Devices, Circuits and Systems, ICCDCS* (pp. 5–8). <https://doi.org/10.1109/ICDCSyst.2014.6926210>