Original Research Article: full paper

(2021), «EUREKA: Physics and Engineering»
Number 1

ADVANCED ENCRYPTION STANDARD USING FPGA OVERNETWORK

Hind Ali Abdul Hasan
Department of Laser & Optoelectronics Engineering
Alkut College University
Kut, Wasit, Iraq, 50001
hind.ali@alkutcollege.edu.iq

Safaa Maijd Mohammed
Department of Medical Instrumentation
Al-Farahidi University
Alqadisyiah, Qatr al-nada street, Baghdad, Iraq, 10011
Safa.suffi33@gmail.com

Noor Hayder Abdul Ameer
Department of Computer
University of Technology
Al-Sinaa street, Baghdad, Iraq, 10066
110048@uotechnology.edu.iq

Abstract

The increase number of eavesdropping or cracker to attack the information and hack the privacy of people. So, the essential issue is making system capable of ciphering information with rapid speed. Due to the advance in computer eavesdropping and cracker that made them to analysis the way of ciphering in rapid speed way. The development in the computer especially in the rapid processer in the last decade create the breaching of any system is a matter of time. Owing to most of breaching ways are based on analysis of system that requireы to be breached and to try brute force on that system to crack it. However, the lacking of influential processers that are capable of breaching system since earlier processors are limit to number of instructions. It can be done in second, which was not sufficient trying to break the system using brute force. In addition, the time required is far away from getting valuable messages in the time that needed. So, the research gives the focus on performing rapid system for ciphering the information rapidly and changing the ciphering every few milliseconds. The changing of ciphering in every millisecond helps system form preventing the eavesdropping and cracker from imposing brute force on the system and hacking the messages and images. The system that created is based on Advanced Encryption Standard (AES), which is it very best performing algorithm in ciphering and deciphering since it doesn't need complex mathematical formula. The research is about designing system that capable of performing AES by using high processer designed on Field programmable gate Area (FPGA). The ciphering of AES using FPGA helps minimize the time required to cipher the information. Also, the research will focus on ciphering and deciphering of images by AES using FPGA.

Keywords: FPGA, Advanced Encryption Standard, VHDL, security by AES, 256-AES , encryption by AES.

DOI: 10.21303/2461-4262.2021.001613

1. Introduction

The evolution that happens in the computer and the rapid processer that occur during the last decade make the breaching of any system is a matter of time [1]. Due most of breaching ways are based on analysis of system that need to be breached and to try brute force on that system to crack it [2, 3]. However, the lacking of powerful processers that are capable of breaching system since pervious processors are limit to number of instructions. It can be done in second, which was not sufficient trying to break the system using brute force [4]. In addition, the time required is far away from getting valuable messages in the time that needed [5, 6]. Due to these reasons, the research gives the focus on performing rapid system that capable of ciphering the information in rapid way and changing the ciphering every few milliseconds [7, 8]. The changing of ciphering in every millisecond helps system form preventing the eavesdropping and cracker from imposing brute force on the system and hacking the messages and images [9].

National Institute of standards and technology (NIST) used the Advanced Encryption Standard (AES) as a replacement for 3DES and IDES which was the most used for ciphering in

their time. The difference in the way of the AES than the 3DES and IDES is that AES is not based on Feistel Structure. The advantage of this structure is that AES can perform the whole block of data in single matrix [9].

The system that created is based on AES, which is it very best performing algorithm in ciphering and deciphering since it doesn't need complex mathematical formula [3, 10]. And it has flexibility in use because of it can used in ciphering message or images [10, 11]. Also, the AES is chosen based on preforming of the algorithm. It was the top on security scoreboard during the two previous decades. The evolution of this algorithm that develops pervious these years to became the best ciphering ways in network and banking security [12].

The system that created in this research is AES using the FPGA. The FPGA is device that capable of designing processer that capable of performing special algorithm based on the program that injected in the FPGA. The special processer that design in FPGA is capable of performing AES on images and message depending on the way that needed in attach that insert to the FPGA as input [13]. The FPGA is rapid the time that required to ciphering any text message in microsecond and enhanced the AES by ciphering and deciphering time required. Due to capability of parallel processing on FPGA [14]. The FPGA gives the opportunity to changing the ciphering ever millisecond in rapid ways since it only required a microsecond to cipher or decipher any messages [10]. This will help in sending information through the network will never be breaching due to rapid changing of ciphering.

A Huge amount of application of AES algorithm used because its ability in cipher data and invincible to break and the flexibility in usage [15, 16]. Also, it doesn't require massive amount of resources and that made it powerful in ciphering and deciphering. The AES consisting of four element or steps as shown in **Fig. 1 [**17].

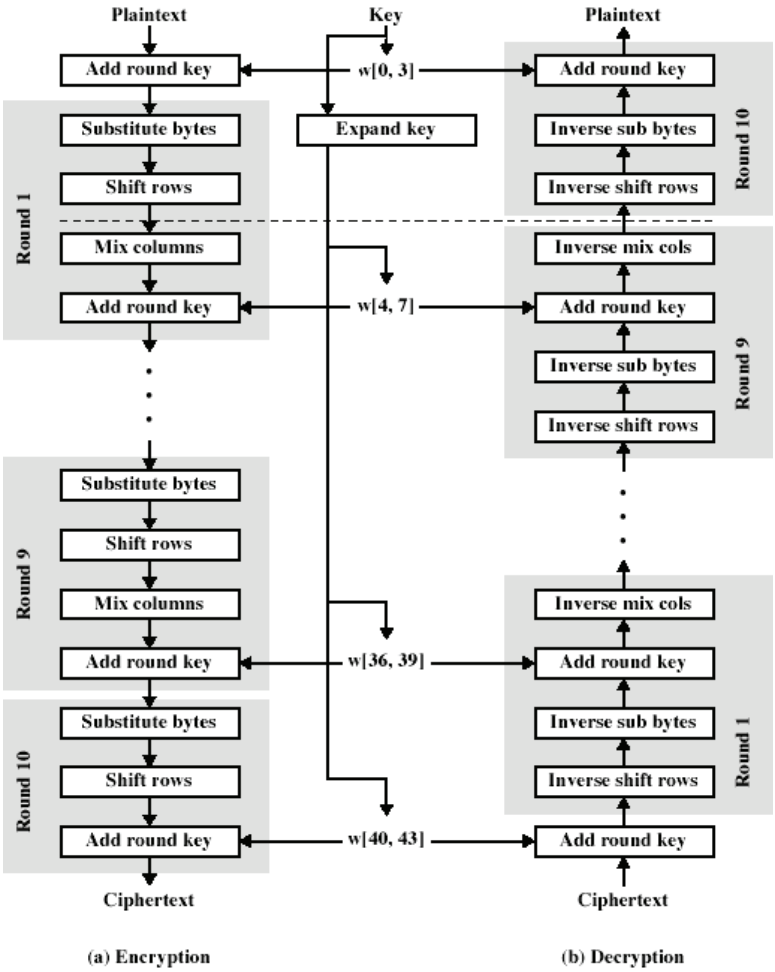

Fig. 1. The Overall structure of AES

As shown in the **Fig. 1** each round consist from various steps which these steps are **SubBytes**, which used to divide the bytes of messages into pieces in order to encrypt this message and exchange each pixel that want to be ciphering with value that located in S-Box. On the other hand, the second steps are **ShiftRows**, which will shift each row in amount that may be different from others row in the message or images. The last but not least step is **MixColumns** that will mix four bytes of each column and it will explain later in ciphering section. The last step is **ADDRoundKeys**. This step is used to add key in every round of the ciphering process. These steps are power of AES since it very complex and truck steps that made to create the mighty of AES algorithm.

2. AES with FPGA

The AES composed from four steps as mentioned before and can be shown in **Fig. 2**. As the initial step, the AES algorithm is subject to the data needed to be ciphering. It will deter the step if the data is required to be cipher as plane text for first operation for changing the plain text to state array [15]. Otherwise, if the data is consist from image it will not require to make array state since the images will represent as array state. This research uses 256×256 images for ciphering and deciphering. The first deterring of program is not needed since the images are represented as array. That means the image will go to the following process which will substitute all pixels with a value located in S-Box that corresponding to its location. The S-Box is constructed from 16×16 array. The number of values that S-Box consisted is 256 values and each one of these values are different from others in the same matrix that needed to be ciphered.

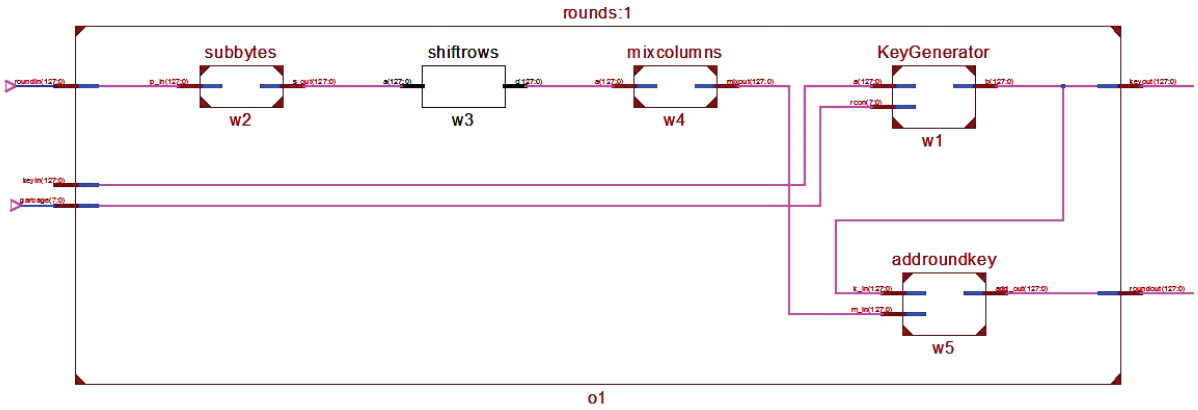

Fig. 2. AES Steps

The second step is simply substitution of every pixel in array with value that corresponding to the value in S-Box. Since the S-Box is an array and this size of this array is 16 by 16. The S-Box contains 256 values in it and each value is different from other that located in the same matrix. The operation of substitution of pixels in array with its corresponding value in S-Box can be shown in **Fig. 3**.

ShiftRows will be the Second step after complete the substitution of all pixel in array with its corresponding pixel in S-Box. The ShiftRows as its name mean that shifting all rows in the state array to the left. The shifting will be differ from row to row in the same state array matrix and the shifting will depends on their location. The shifting process based on Anti-Clock wise and the shifting process can be shown in **Fig. 4**.

In last step but not least the MixColumn, from its name its transform columns. The MixColumn will divide every column into 4 bytes block and each block will be transformed into polynomials equation by Galois function GF(2^8). These polynomial equation will be multiplied by its modulo $x^8+x^4+x^3+x^1+x^0$ as shown in **Fig. 5** [18].

Then the last step will applied which is KeyGenerate and AddRoundKey. This step is first generate key for XORed the 16 bytes of the key generated with its corresponding 16 bytes of array of image. The key is generated based on the schedule of the algorithm. **Fig. 6** shows the AddRoundKey process. Finally, when all these steps applied on the state array. The steps will repeat again for 10 more round on state array to encrypt the system as shown in **Fig. 7**.

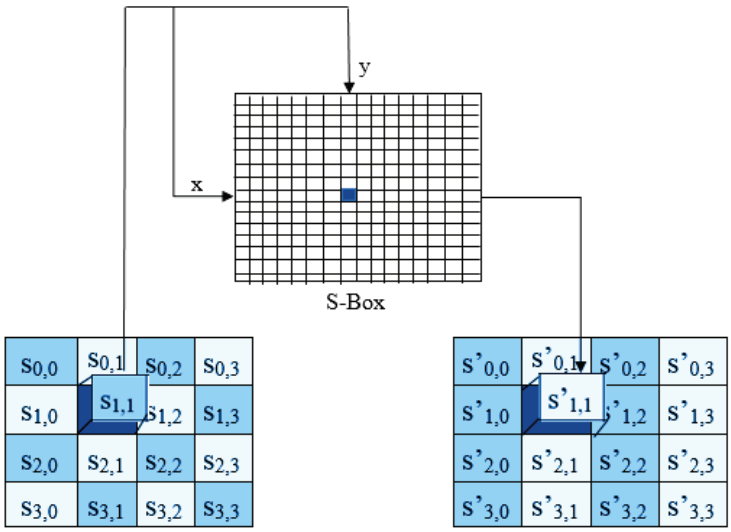

Fig. 3. Transformation of pixel [17]

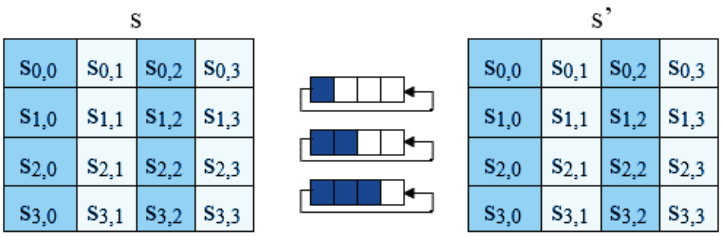

Fig. 4. ShiftRows processing

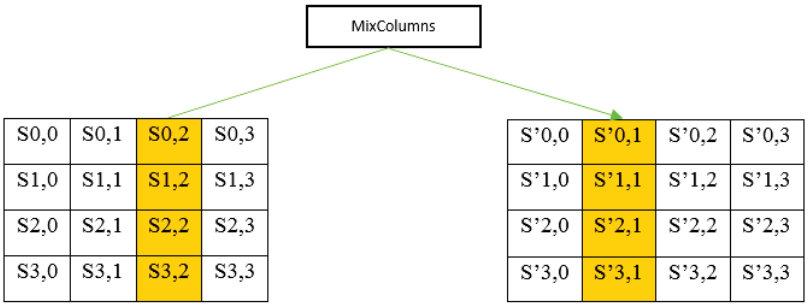

Fig. 5. Mix column transformation [19]

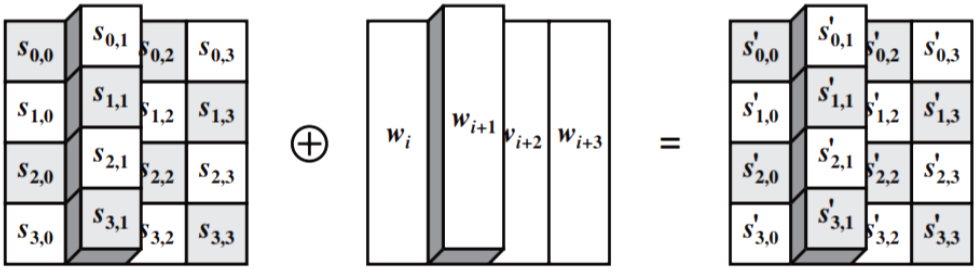

Fig. 6. Round Key transformation

The deciphering process will be as reverse to the steps of ciphering. It will start with AddRoundKey and back to all previous round. Then, this step completes the results of first round will be input to inverse of MixColumn. MixColumn will return each 4 byte to its original results by multiply each 4 bytes with module of GF(8) equation. Then the results of this will go to the third step. The Shift Row will shift return the offset of each row to its position. Once all rows return to its

order and location before Shifting Row. The final step will be applied when Sub Byte will return each value of the state to its real value based on the S-Box. The results of Sub Byte will be the original images or the plain text.

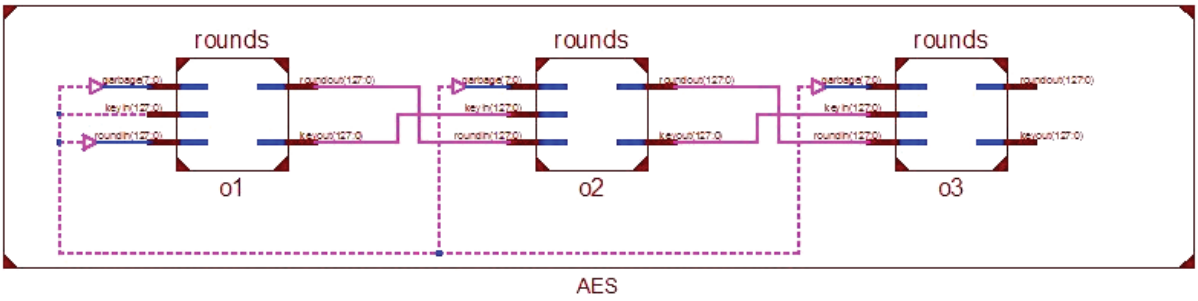

Fig. 7. Three Rounds of AES

3. Material and methods

Spartan 3AN is used for the implementation of the proposed algorithm as the device to implement the algorithm and has been programmed using Very High-level Design Language (VHDL). VHD L is used in this project for configuring and applying the AES algorithm in the FPGA. This language is one of the most famous languages that used in programming and configurable the FPGA. As known FPGA is very complicated devices specially in coding and working while in contrast it gives great results compare to other devices in the same field. The VHDL is used in Synthesis, simulation and generating the programmable file code for each structure and sections of AES algorithm in the FPGA and it can be shown in **Fig. 7.** The flexibility of fully utilizing and programing FPGA to achieve great results in ciphering and deciphering of AES in FPGA is noted.

4. Results

Rapid ciphering of information is most important in our days since the evolution of massive information need ciphering to transmit to their recipient. However, the using of FPGA help to improve of rapid ciphering of Image using AES. The combination of AES algorithm requires massive resource and injected on FPGA help to rapid ciphering of images. The time required to cipher 256×256 image is only 20 nanoseconds as shown in **Fig. 8**. This time is very helpful since it can cipher and decipher multiple images with no time.

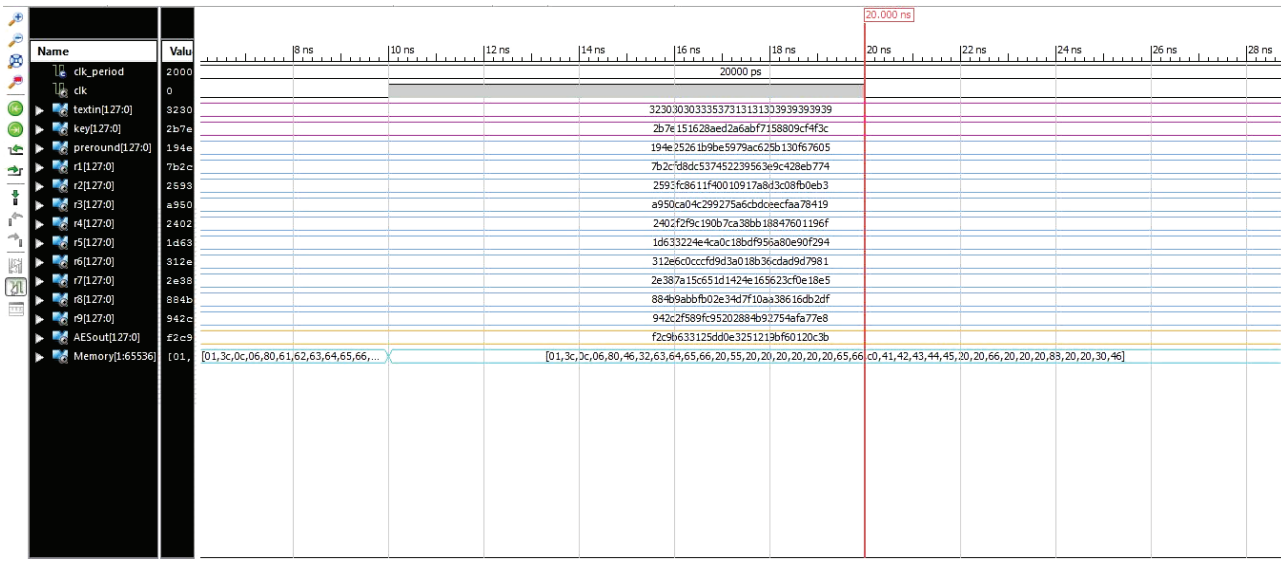

Fig. 8. Time required to cipher 256×256 image

Also, the resources of AES that toke from the FPGA resource are small as shown in **Table 1**. The FPGA that used in this experiment is Spartan 3AN and a frequency. The FPGA faster the operation of ciphering of image since it used parallel processing that means perform multiple tasks in same time if none of these tasks related to each other. The AES algorithm took the advantage of FPGA since most of their procedure is not related to each other. The resource that allocated in FPGA when injecting AES on it is explained as shown below.

Table 1
Adopted FPGA Resources

Logic Utilization	Used	Available	Utilization
Number of Slices	2000	5888	34 %
Number of Slice Flip Flops	812	11776	7 %
Number of 4 input LUTs	950	11776	8 %
Number of bonded IOBs	12	372	3 %
Number of GCLKs	1	24	4 %

In addition, the program is used to changing the ciphering with every millisecond. It will allow to give more confidently to the system and this will not be happening if the FPGA not here. The proposed is compared with different algorithm and different types of FPGA devices and these different algorithms are used different types of approach to encryptions data. However, the results that have been taken from this proposed algorithm is more greats than other as shown in **Table 2.** The table shows that all the proposed approach used 128 bits for ciphering compare to 256 bits which is more security and more reliable than other methods. However, this cost the proposed approach more time than other for ciphering due to the large size of the algorithm. Also, the results shows that the number of slices that is used is small compared to other since the algorithm used 256 bits types of algorithm compared to 128 bits for other methods. Also, it can be shown that the throughput of the algorithm is less than Harshali Zodpe and Ashok Sapkal due to two facts the first they used faster FPGA devices so the throughput is faster the other is that the algorithm used 256 bits in ciphering compared to 128 bits in the other methods.

Table 2
Comparative between different types AES approach [20]

Design	Device	Bit width (bits)	No. of Slices	Throughput (Gbps)
Proposed	Spartan 3 AN	256	2000	4.23
Wang and Ha	XC6VLX240T	128	15,612	1.88
Qiang et al.	XC4VLX60	128	1975	2.06
Harshali Zodpe and Ashok Sapkal	XC7VX690T	128	4089	6.34

5. Discussion of experimental results

Defending the data is the most important as for world international or personal to saves data. Every year many algorithms are either formed or add new features to the previous algorithms to enhance the security of algorithms. This research used the most effective algorithm which is AES. FPGA is used in this research for speed-up the process of the algorithm and had made major effect to the speed of the algorithm with only 20 ns for complete the ciphering of nine round. The algorithm used the 256 bits for ciphering which is great enhancement in the security to cipher text due to the fact the eavesdropping needs more time to deciphering and more

sophisticated computer to break the system compared to 64 or 128 AES algorithm. There is no limitation in 256 AES algorithm in this research due to using the FPGA for ciphering and deciphering since the FPGA used the parallel processing that allow to perform multiply process in the same and this save time for performing the 256-AES. However, without the FPGA used 256-AES for ciphering and deciphering is bit slower since it required more process for ciphering than other 64 or 128 AES algorithm. The enhanced for this research is to use on high quality image and tried to compress the image and also tried to used multiple single processors like using multiple raspberry-pi or Arduino to provide the same results like FPGA.

6. Conclusion

The massive resource of information increases in every day the advance of the computers that used by eavesdropping to attack these data. It gives the essentiality to find way to rapid ciphering and to changing ciphering from time to time to make it invincible to eavesdropping to hack system. This done by union the FPGA and AES since the AES has the best scoring in security scoreboard and FPGA is special device. It allows to create special processor to do the AES operations. The FPGA help in festering the ciphering of AES in only 20 nanoseconds for image sized 256×256 pixels. And this done due to the ability of FPGA in performing the parallel processing and support of the AES algorithm to work in parallel. The next steps in this research will applied the algorithm on larger image size and to perform the algorithm on other devices to like Raspberry Pi and Arduino in parallel mode.

References

[1] Ekert, A. K., Huttner, B., Palma, G. M., Peres, A. (1994). Eavesdropping on quantum-cryptographical systems. Physical Review A, 50 (2), 1047–1056. doi: https://doi.org/10.1103/physreva.50.1047

[2] Omran, S. S., Al-Hillali, A. A. (2015). Quarter of Iris Region Recognition Using the RED Algorithm. 2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim). doi: https://doi.org/10.1109/uksim.2015.70

[3] Babitha M.P., Babu, K. R. R. (2016). Secure cloud storage using AES encryption. 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT). doi: https://doi.org/10.1109/icacdot.2016.7877709

[4] Barriga, L., Blom, R., Gehrmann, C.,Naslund, M. (2000). Communications security in an all-IP world. Ericsson review, 2, 96–107.

[5] Nishikawa, N., Amano, H., Iwai, K. (2017). Implementation of Bitsliced AES Encryption on CUDA-Enabled GPU. Lecture Notes in Computer Science, 273–287. doi: https://doi.org/10.1007/978-3-319-64701-2_20

[6] Abdullah, A. M. (2017). Advanced encryption standard (AES) algorithm to encrypt and decrypt data. Cryptography and Network Security.

[7] Maharjan, R., Shrestha, A. K., Basnet, R. (2019). Image Steganography: Protection of Digital Properties against Eavesdropping.arXiv.org. Available at: https://arxiv.org/abs/1909.04685

[8] Peake, T. M. (2005). Eavesdropping in communication networks. Animal Communication Networks, 13–37. doi: https://doi.org/10.1017/cbo9780511610363.004

[9] Alanazi, H. O., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., Al-Nabhani, Y. (2010). New Comparative Study Between DES, 3DES and AES within Nine Factors. Journal of Computing, 2(3), 152–157.

[10] Stallings, W. (2011). Cryptography and Network Security Principles and Practice.Prentice Hall.

[11] Ueno, R., Morioka, S., Homma, N., Aoki, T. (2016). A High Throughput/Gate AES Hardware Architecture by Compressing Encryption and Decryption Datapaths. Cryptographic Hardware and Embedded Systems – CHES 2016, 538–558. doi: https://doi.org/10.1007/978-3-662-53140-2_26

[12] Banik, S., Bogdanov, A., Regazzoni, F. (2017). Compact circuits for combined AES encryption/decryption. Journal of Cryptographic Engineering, 9 (1), 69–83. doi: https://doi.org/10.1007/s13389-017-0176-3

[13] Jumma, L. F.,Omran, S. S. (2018). Design of Superscalar SHA-1 & SHA-2 MIPS Processor Using FPGA. Association of Arab Universities Journal of Engineering Sciences, 25(3), 88–99.

[14] Omran, S. S., Al-Hilali, A. A. (2018). Comparative Study Between Different Rectangle Iris Templates. 2018 International Conference on Advanced Science and Engineering (ICOASE). doi: https://doi.org/10.1109/icoase.2018.8548913

[15] Al-Hilali, A. A., Jumma, L. F., Amory, I. A. (2019). High-Quality Image Security Implementation Using 128-Bit Based on Advanced Encryption Standard algorithm. Journal of Southwest Jiaotong University, 54 (6). doi: https://doi.org/10.35741/issn.0258-2724.54.6.32

[16] Çavuşoğlu, Ü., Kaçar, S., Zengin, A., Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. Nonlinear Dynamics, 92 (4), 1745–1759. doi: https://doi.org/10.1007/s11071-018-4159-4

[17] Messerges, T. S. (2001). Securing the AES Finalists Against Power Analysis Attacks. Fast Software Encryption, 150–164. doi: https://doi.org/10.1007/3-540-44706-7_11

[18] Elsherif, S., Mostafa, G., Farrag, S., Alexan, W. (2019). Secure Message Embedding in 3D Images. 2019 International Conference on Innovative Trends in Computer Engineering (ITCE). doi: https://doi.org/10.1109/itce.2019.8646685

[19] Al-Fedaghi, S., Alsulaimi, M. (2018). Privacy Thinging Applied to the Processing Cycle of Bank Cheques. 2018 3rd International Conference on System Reliability and Safety (ICSRS). doi: https://doi.org/10.1109/icsrs.2018.8688874

[20] Zodpe, H., Sapkal, A. (2020). An efficient AES implementation using FPGA with enhanced security features. Journal of King Saud University – Engineering Sciences, 32 (2), 115–122. doi: https://doi.org/10.1016/j.jksues.2018.07.002

Received date 16.08.2020
Accepted date 25.01.2021
Published date 29.01.2021