VOL. 18, NO. 16, AUGUST 2023 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

AN ANALYSIS OF LOWEST ENERGY CONSUMPTION (CPU TIME) THROUGH RUNNING SEVERAL CRYPTOGRAPHY ALGORITHMS WITH DIFFERENT VIDEO FORMATS

Osama Alshannaq[1], Mohd Rizuan Baharon[1], Mohammad Mahmoud Nawafleh[1], Odai Yassin Nawafleh[1], Jamil Abedalrahim Jamil Alsayaydeh[2], Zikri Abadi Baharudin[3], Maslan Zainon[4] and Azwan Aziz[5]
[1]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, Durian Tunggal, Melaka, Malaysia
[2]Department of Electronics and Computer Engineering Technology, Fakulti Teknologi Kejuruteraan Elektrik and Elektronik (FTKEE), Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
[3]Centre for Robotics and Industrial Automation, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, Durian Tunggal, Melaka, Malaysia
[4]Centre of Smart System and Innovative Design, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, Durian Tunggal, Melaka, Malaysia
[5]Centre for Advanced Research on Energy, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, Durian Tunggal, Melaka, Malaysia
E-Mail: jamil@utem.edu.my

ABSTRACT

One persistent obstacle has been verified to be one of the main problems with the main developments in the electronics and technology fields, called: Data Security. The data should be encrypted in order to be quickly and securely linked via the electronic information transfer over the network. The procedure of transforming plain text to ciphered-text is called encryption, where cannot be changed or understood simply by undesirable individuals. It may similarly be described as the science that utilizes mathematics in decryption and encryption data processes. In this article, we consider different significant algorithms utilized for data decryption and encryption in whole areas, for making a comparative study for most vital algorithms. This paper focuses on various current cryptography algorithms types. This paper also analyses the algorithm's security and parameters that define the cryptosystem efficiency.

Keywords: energy consumption, memory usage, cryptography algorithms, video encryption, video decryption.

Manuscript Received 11 August 2023; Revised 15 October 2023; Published 27 October 2023

INTRODUCTION

Innovative progress of hardware capabilities combined with progressively low weight and small size offers several opportunities to use mobile devices, like tablet PCs, laptops, and, smart phones for business and entertainment at home, at office, in airport, i.e., everywhen and everywhere. A smartphone represents now the main devices of processing data to all users. Portio investigation forecasts that worldwide phone users will be 6.9 billion by the end of 2013 and 8 billion by the end of 2016. Ericsson similarly estimates that phone users will be 9 billion by 2017. smartphones are still restrained by resource and certain applications commonly require extra resources more than the prices of smartphone. To solve that challenge, a smartphone can acquire external source for more resources called Cloud Storage. It is not possible to keep the information and data on the smartphone. Thus, the phone users may use the resources from the cloud, which needs information and data migrations between the mobile devices and cloud. It contains of front-end users who own smartphones and back-end cloud servers [1].

The transfer of information to a Cloud Storage from the mobile device is called uploading, while the transfer of data to mobile device from the cloud storage is called downloading. Cryptography is a way to hide data through message encrypting. Several algorithms of encryption are commonly existing and utilized in security of information. They may be divided to Asymmetric (public) and Symmetric (private) key encryption. Only one key is applied for encrypting and decrypting information in Symmetric (secret) key encryption. The key must be allocated before transmission. A significant role is played by Keys [2]. If the algorithm uses a weak key, then everybody can decrypt the information. Symmetric key encryption Strength relies on the utilized key size. For the same algorithm, encryption utilizing extended key is more difficult for breaking than the one achieved using smaller key. The key distribution challenge is solved by public or Asymmetric key encryption. There are two keys utilized in Asymmetric keys; private and public keys. The Public and private keys are utilized for encryption and decryption, respectively. Since users prefer to utilize two keys: the public key recognized to the public and the private key recognized to the user only. Mobile devices are usually connected with each other and are accessible to other networks and channels of communication, so encryption is essential for keeping the information private from others. Secured information communication is similarly an important parameter to the whole governments / industries. Secured data transmission in universities, industries, defence, and other fields is an essential.

Cryptographic techniques can be implemented in a variety of ways. This paper will build several experimentations to find the best algorithms by calculated percentage usage of CPU energy of encryption and decryption. This paper will define the main techniques that

will use for studying the best algorithms, AES, MAES, DES, 3DES, RSA, and Blowfish for the data encryption and decryption or data streams. The video frame sequence is encoded utilizing the integrated version of AES, MAES, DES, 3DES, RSA, and Blowfish. Though, the suggested algorithm performance evaluation defends its important contribution to high-end compression access and high-quality assurance of encryption algorithm [3].

CRYPTOGRAPHY

It is a method utilized to prevent unauthorized access of information. For hiding the information from the intruders, the encryption process contains of multiple or single keys. Plaintext is the actual text before the encryption process. cipher text obtains after encoding the information with the key assistance. The encryption process has the ability to upgrade/ change at any moment the key and data of upgraded or changed key has been be recognized to both the parties. Figure.1 gives the encryption-decryption process.

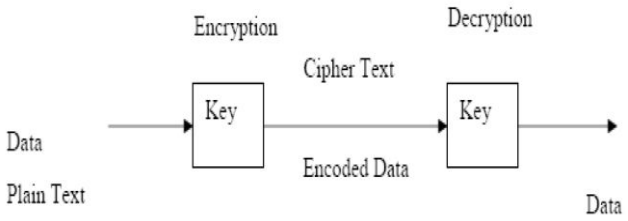

Figure-1. Encryption-Decryption process.

Plain Text: This is the actual message the individual wants to connect with others. The original message which has to be sent to others is assigned a specific term in cryptography as Plain Text. For instance, Alice would like to send a message to Bob that is "Hello Friend how are you". Now "Hello Friend how are you" is a plain text message.

Cipher Text: This is a meaningless message that no one can understand. In Cryptography, the actual message is converted to an unreadable message before the original message is transmitted. For instance, the Cipher Text of "Hello Friend how are you" is "Ajd672#@91ukl8*^5%".

Encryption: This represents the procedure of transforming Plain Text to Cipher Text. The encryption is used by Cryptography for sending private messages via an unsafe channel. The encryption process needs two items- a key and an encryption algorithm. An encryption algorithm denotes the process which has been utilized in encryption. Encryption happens on the hand of the sender.

Decryption: Which is a reverse process of encryption. It represents a technique of transforming Cipher to Plain Text. The decryption technique is utilized by Cryptography on the hand of receiver to get the actual message from unreadable message. The decryption process needs two items- a key and a decryption algorithm. A Decryption algorithm denotes the process which has been utilized in Decryption. Usually, the decryption and encryption algorithms are the same.

Key: Which is an alpha numeric, numeric or a special sign. The Key is utilized at the time of encryption in the Plain Text, and in the Cipher Text at the time of decryption. In Cryptography, the key selection is very significant as the users prefer to utilize two keys: public key and private key [4,5].

Two types of encoding are available. These two kinds are asymmetric and symmetric. Numerous of these algorithms will be involved like: SEAL, E-DES, 3DES, DES, BLOW FISH, AES, RC2, RC4 and RC6 which are relevant to bilateral algorithms. Unlike, ECC, RSA, DH, DSA, ELGAMAL ALGORITHM and EEE, that all have to do with unilateral algorithm. The key encoding techniques classification is presented in Figure-2.

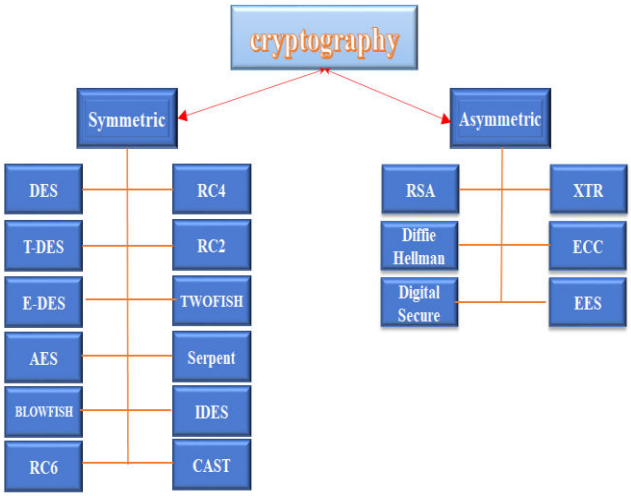

Figure-2. The Classification of Encryption Algorithms [6].

Table-1. Comparative analysis of various algorithms.

Algorithm	Year	Key length	Block size	No. of round
DES	1977	56-bits	64-bits	16
3DES	1978	128-bits, 112-bits, 56-bits	64-bits	48
AES	2000	128-bits, 192-bits, 256-bits	128-bits	10, 12, 14
BLOWFISH	1993	32-bits, 448-bits	64-bits	16
RSA	1977	1024 to 4096 bits	64-bit	-

RELATED WORK

Detailed analysis of the common symmetric key encryption algorithms like AES, Blowfish, DES, and TRIPLE DES is present by Agrawal *et al*. [7]. Symmetric Key algorithms has a faster run comparing to Asymmetric Key algorithms like RSA and the Symmetric algorithms require less memory than asymmetric encryption algorithms. Symmetric key encryption security is higher than Asymmetric key encryption. It was noted the Blowfish algorithm supremacy through AES, Triple DES and DES on the base of security and size of key. The Blowfish Algorithm F function gives a great security level for encrypting the 64-bit plaintext data.

A comparison study for three algorithms, RSA, AES and DES is done by Seth *et al*. [8] taking into account specific parameters like output byte, memory uses and computation time. It was found that RSA requires greatest time of encryption and memory consumption is likewise very huge yet byte of output is lowest in RSA algorithm. Depending on the files of text utilized and the experiment outcome it was noted that DES require lowest time of encryption and AES has lowest memory consumption whereas difference of encryption time is small in DES and AES algorithms.

The comparative between four maximums generally utilized Symmetric key algorithms: AES, Blowfish, DES and 3DES is done by Mandal [9]. A comparison has been done depending on parameters: decryption/encryption time, key size, size of round block, and process time of CPU in the structure of throughput and power spending. blowfish was noted to be better than other algorithms. Too, AES has benefit in terms of decryption time and throughput over the other 3DES and DES. Of all listed algorithms, 3DES has the lowest performance.

Three algorithms RSA, 3DES and DES are explained by Marwaha *et al*. [10]. DES and 3DES are symmetric key cryptographic algorithms while RSA are an asymmetric key cryptographic algorithm. Algorithms have been evaluated on their capability for securing information, needed time for encrypting information and required throughput of the algorithm. Based on the inputs, various algorithms performance was different. It was noted that scalability and confidentiality obtained by RSA over DES and 3DES is very high and makes it appropriate even DES requires fewer time and memory for encrypting and decrypting the data yet brute force technique can simply break DES security comparing to RSA and 3DES, making it the final safe algorithm.

The six most popular encryption algorithms like RC6, DES, 3DES, BLOWFISH, RC2and AES (Rijndael) were discussed by Elminaam *et al*. [11]. The performance of compared algorithms was assessed. For these encryption algorithms, a comparison was made for various settings for every algorithm like various data blocks sizes, various types of data, battery power usage, various size of key and lastly encryption/decryption speed. It was noted that once the findings are presented in Base 64 encoding or Hexadecimal Base encoding, there is no important modification. Second, in the packet size varying case, it was noted that BLOWFISH has superior performance than other popular encryption algorithms utilized, followed by RC6. It was also noticed that BLOWFISH, RC6 and RC2 have drawback over other algorithms in time usage, in the case of varying type of data like image rather than text. It was also noticed that 3DES has poorer performance than DES algorithm. Lastly, it can be noticed that greater size of key makes the change in the time and battery consumption clear, in the case of changing size of key.

Most popular algorithms of symmetric cryptography were compared by ALI *et al*. [12] such as CAST-256, BLOWFISH, AES and TWOFISH. The algorithms performance and behaviour were considered in the comparison once various data loads were utilized. The comparison was performed depending on those parameters: key size, block size, and speed. Blowfish was concluded to be outstanding to other algorithm, since it needs fewer time. Even once the size of data was slight this change was not noticeable. Yet it was obviously noticeable for a file larger than 100 KB.

Thakur *et al*. [13] explained a reasonable comparative between three maximum popular symmetric key cryptography algorithms: Blowfish, AES and DES. The primary issue was the algorithms performance in various settings, the existing comparisons consider the algorithms' performance and behaviour once using various data loads. The comparison was performed depending on these parameters: size of key, size of block, and speed. Java programming was used to execute the Simulation. Blowfish was concluded to have superior performance than other popular encryption algorithms utilized.

Alam *et al*. [14] argued efficiency and performance analysis of various block cipher algorithms (CAST-128, 3DES, DES, RC2, IDEA and BLOWFISH)

of symmetric key cryptography. Block cipher algorithms were compared depending on these variables: data input size (in the type of video, audio and text), time of encryption, time of decryption, decryption and encryption throughput of every block cipher and power usage. It was noted that 3DES has extra usage of power and fewer throughput than the DES mainly because of its triple phase characteristics.

Saini [15] analysed different algorithms performance - AES, DES, Blowfish, RC2, RC6 and 3DES. The best algorithm which is well documented and well known since they are well studied and well tested, that was noted from the results of simulation. A successful system of cryptographic maintains a balance between what is reasonable and appropriate.

Alazani *et al*. [16] performed the comparison study of three Encryption Algorithms (AES, 3DES and DES) in nine parameters like Cipher Type, Length of Key, Security, Size of Block, Possible Keys, Possible ASCII printable character keys and Time taken for checking the whole likely keys at 50 billion keys each second. Analysis displays that AES is better than DES and 3DES.

Arora *et al*. [17] analysed various security algorithms performance on a single processor and cloud network for various sizes of input. In this article, we are aiming to discover quantitative terms such as Speed-Up Ratio which improve of cloud resources utilizing to implement security algorithms (AES, MD5 and RSA) that are utilized by businesses for encrypting huge data volumes. Three various algorithms types are utilized – RSA (an asymmetric encryption algorithm), MD5 (a hashing algorithm) and AES (a symmetric encryption algorithm). The outcomes described in this article determine that the implemented algorithms on cloud environment (such as Google App) are more effective than utilizing them on single system. RSA consumes the maximum time while MD5 consumes the minimum, for cloud (Appengine) and uniprocessor (local) environments. Maximum Speed-Up rate is achieved in AES for low input file sizes and the Speed up rate clearly drops since the size of input file is raised. For every input size, the Speed- Up rate is maximum for AES, after that MD5 and minimum for RSA algorithm [18]-[22].

EXPERIMENTAL APPROACH

Traditional commerce requires security of data in all aspects of multimedia format and a very necessary requirement of traditional commerce. The applications associated in the real world as of video conferencing applications and VOD applications requires that the paid users only can access the multimedia information presented before the various user stream [23]-[26].

There is no doubt that mechanisms of authentication-controlled are existing for managing the accessibility of multimedia formatted data in distributed form. But, on formats of wireless networks, networks of satellite or any other IP network system the data in multimedia format cannot be only be secure through such mechanisms of authentication. Treating the complete data in the format of binary form confirms that it is one of the greatest famous techniques to secure underlying data in multimedia format. Further, the complete data is encrypted with the usage of secret key algorithms for encryption such as the Data Encryption Standard Algorithm also called as DES for short, IDEA, AES, etc. Secret key encryptions are complex and need heavily computed values. The problems faced are described in two implementations.

In the software, as the algorithms are implemented it shows that it is slow enough in processing the large data amount that are formed applications in the multimedia format. The other one is related to hardware where its applications in hardware format implementations additional costs are added at both the ends of data generators and also the receiving users. There are two main elements producing problem to multimedia data encryption. Firstly, huge size of typical multimedia data (the size for e.g., of any MPEG-1 video format of two hours is in and around 1GB). Secondly, processing of the data in multimedia formats has the need to get processed in the real-time-frame scenario. The video codec-device is put or overlaid with heavy burden when large or huge data is being processed in a very small timespan. Heavy affects are also seen on the requirements related with space and storage and also the network communications are drastically burdened. The application of algorithms of both encryption as well as decryption type aggravates the faults and causes the latency to increase either at the time or even after the phase of encoding [27]-[30].

The tests were performed on a Samsung laptop with Intel CORE i7 Processor, 2.4 GHz (4 CPUs), RAM of 8 GB, utilizing Windows 10 64-bit Operation System. Import a video object. The following outcomes are explicitly measured by simulating the Algorithm (AES, MAES, DES, 3DES, RSA, and Blowfish). The development and design phases of the suggested framework has been done utilizing MATLAB 2018. The two video files called 1.avi and 2.avi are taken into consideration to simulate the Algorithm in a parameterized test. The two files have the same pixel yet the duration time is different [31]-[33].

RESULTS FOR VIDEO ENCRYPTION

As the suggested framework has been incorporated with the latest Algorithm (AES, MAES, DES, 3DES, RSA, and Blowfish) for encrypting the video files. Furthermore, the development and design of the suggested system has been performed taking into consideration simulation tool instances. The experiment results show in table 2 the CPU time spent through encryption for the two video files.

Table-2. Video encryption.

Algorithm	Video 1 (CPU time)	Video 2 (CPU time)
AES	208.531	15.5625
MAES	622.25	35.6875
DES	544.891	87.3906
3DES	1371.69	40.7188
RSA	1365.86	86.5469
Blowfish	127.234	18.0313

Figure-3 shows the comparison between both video files for CPU time. The figure displays that consumption of energy for video 1 is further than video 2. This is because video 1 file duration is further than video 2 file duration. Though, for comparing algorithms, the Blowfish (video 1= 127.234, video 2= 15.5625) shows good performance with AES (video 1= 208.531, video 2= 18.0313), MAES (video 1= 622.25, video 2= 35.6875), DES (video 1= 544.891, video 2= 87.3906), 3DES (video 1= 1371.69, video 2= 40.7188), and RSA (video 1= 1365.86, video 2= 86.5469). While RSA and 3DES shows the high energy consumption.

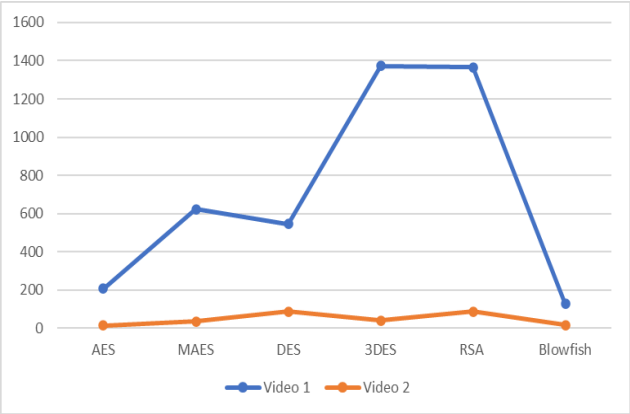

Figure-3. Comparison of different encryption videos.

RESULTS FOR DECRYPTED VIDEO

As the suggested framework has been incorporated with the latest Algorithm (AES, MAES, DES, 3DES, RSA, and Blowfish) for decrypting the video files. The experiment results are shown in Table 5.4 with decrypted video for both video files.

Table-3. Video decrypted.

Algorithm	Video 1 (CPU time)	Video 2 (CPU time)
AES	201.25	17.1570
MAES	600.3169	34.0688
DES	544.69	88.313
3DES	1361.3413	40.5425
RSA	1360.23	85.7058
Blowfish	122.34	14.25

Figure-4 shows the comparison between both video files for CPU time. The figure shows that consumption of energy for video 1 is further than video 2. Though, for comparing algorithms, the Blowfish (video 1= 122.34, video 2= 14.25) shows good performance with AES (video 1= 201.25, video 2= 17.1570), MAES (video 1= 600.3169, video 2= 34.0688), DES (video 1= 544.69, video 2= 88.313), 3DES (video 1= 1361.3413, video 2= 40.5425) and RSA (video 1= 1360.23, video 2= 85.7058).

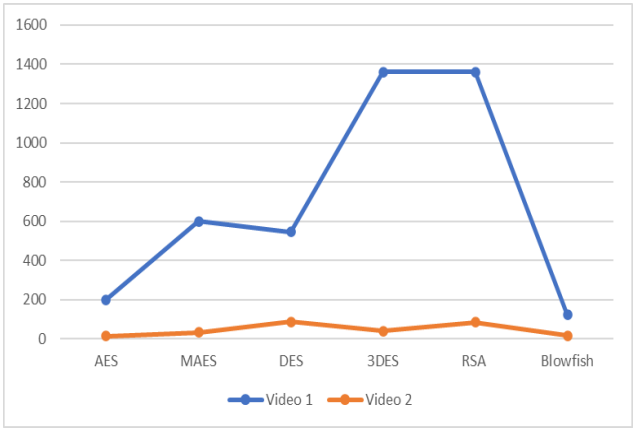

Figure-4. Comparison of different decryption videos.

EXPERIMENTAL RESULTS FOR DIFFERENT VIDEO FORMATS

The proposed framework has been integrated with different video formats through Algorithm (AES, MAES, DES, 3DES, RSA, and Blowfish). The experiment results are shown in table 4 with encrypted video for different video formats but same video size. Table 4 shows the comparison between different video formats for CPU time. The table shows that energy consumption for AVI video is less than other video formats. However, for comparing algorithms, the Blowfish (15.5625) displays good performance with AES, MAES, DES, 3DES and RSA.

Table-4. CPU time for different video formats.

Algorithm	AVI	MP4	WMV
AES	18.0313	19.25	18.6525
MAES	35.6875	36.75	37.65
DES	87.3906	89.96	88.60
3DES	40.7188	42.18	41.818
RSA	86.5469	86.6954	87.649
Blowfish	15.5625	18.3453	17.1003

CONCLUSIONS

Security in digital video transmission has its significance in image communications nowadays. Due to the growing number of using video in industrial processes, it is vital to secure the private information of video from unauthorized access, security of image and video is becoming a serious matter. This paper provides a review on symmetric and asymmetric algorithms also evaluates the selected algorithm performance (AES, MAES, DES, 3DES, RSA, and Blowfish).

This article displays a survey of the latest significant cryptography algorithms. These cryptographic algorithms well are analysed and studied to assist in improving the present cryptographic methods performance. The outcome displays the methods which are suitable for encryption in real time. All encryption approaches have shown their benefits and obstacles and have also shown to be suitable to various applications. The comparison between Asymmetric and Symmetric algorithms displays that Symmetric are quicker than Asymmetric.

The primary focus is on clearly presenting the energy consuming taken to encrypt the input video using which organizations can easily analyse the performance of different algorithms. Every algorithm has been compared with various parameter sets. From the outcomes, it has been shown that of all the symmetric encryption algorithms, Blowfish is the most efficient and secure algorithm.

REFERENCES

[1] M. V. Pedersen and F. H. P. Fitzek. 2012. Mobile clouds: The new content distribution platform. in Proceedings of the IEEE, May 2012, 100(SPL CONTENT): 1400-1403, doi: 10.1109/JPROC.2012.2189806.

[2] M. Sujithra, G. Padmavathi, and S. Narayanan. 2015. Mobile device data security: A cryptographic approach by outsourcing mobile data to cloud. in Procedia Computer Science, 47(C): 480-485, doi: 10.1016/j.procs.2015.03.232.

[3] P. Singh Karamjeet Singh. 2013. Image Encryption and Decryption Using Blowfish Algorithm in MATLAB. Int. J. Sci. Eng. Res., 4(7), [Online]. Available: http://www.ijser.org.

[4] Ali, Mohanad Faeq, Nur Azman Abu, and Norharyati Harum. 2017. A Novel Session Payment System via Internet of Things (IOT). International Journal of Applied Engineering Research. 12(23): 13444-13450.

[5] Ali Mohanad Faeq, Nur Azman Abu and Norharyati Harum. 2018. A Novel Multiple Session Payment System. Int. J. Adv. Comput. Sci. Appl. 9.6: 237-245.

[6] Abood Omar G. and Shawkat K. Guirguis. 2018. Enhancing Performance of Advanced Encryption Standard for Data Security. International J. Eng. Andin. Syst. 2.11: 32-38.

[7] M. Agrawal and P. Mishra. A Comparative Survey on Symmetric Key Encryption Techniques.

[8] S. M. and M. R. Seth. 2011. Comparative analysis of encryption algorithms for data communication.

[9] P. C. Mandal. 2012. Superiority of Blowfish algorithm. International Journal of Advanced Research in Computer Science and Software Engineering.

[10] M. Marwaha, R. Bedi, A. Singh and T. Singh. 2013. Comparative Analysis of Cryptographic Algorithms. Int. J. Adv. Eng. Technol. Int J Adv Engg. pp. 16-18.

[11] D. A. K. H. A. and H. M. M. Elminaam. 2009. Performance evaluation of symmetric encryption algorithms. Communications of the IBIMA.

[12] Ali, Mohanad Faeq, *et al*. 2019. Protecting IoT based transmitted data security using tokenized multiple layered encryption techniques.

[13] W. Www, J. Thakur and N. Kumar. 2011. International Journal of Emerging Technology and Advanced Engineering DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. [Online]. Available: www.tropsoft.com.

[14] M. I. and K. M. R. Alam. 2013. Performance and efficiency analysis of different block cipher algorithms of symmetric key cryptography. Int. J. Adv. Res. Comput. Sci. Softw. Eng.

[15] B. Saini. 2014. Survey on Performance Analysis of Various Cryptographic Algorithms. Int. J. Adv. Res. Comput. Sci. Softw. Eng.

[16] H. O. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani. 2010. New Comparative Study Between DES, 3DES and AES within Nine Factors.

[17] P. Arora, A. Singh, and R. K. Goel. 2012. Evaluation and Comparison of Security Issues on Cloud Computing Environment Himanshu Tyag.

[18] Oliinyk A., Fedorchenko I., Stepanenko A., Katschan A., Fedorchenko Y., Kharchenko A., Goncharenko D. 2019. Development of genetic methods for predicting the incidence of volumes of emissions of pollutants in air. 2019 2nd International Workshop on Informatics and Data-Driven Medicine, IDDM, CEUR Workshop Proceedings. 2488: 340-353.

[19] Al-gburi A. J. A., Ibrahim I. M., Abdulhameed M., Zakaria Z., Zeain M., Keriee H. H., Nayyef N. A., Alwareth H. and Khaleel A.D. 2021. A compact UWB FSS single layer with stopband properties for shielding applications, Przegląd Elektrotechniczny. (2): 165-168.

[20] Fedorchenko I., Oliinyk A., Stepanenko A., Svyrydenko A, Goncharenko D. 2019. Genetic method of image processing for motor vehicle recognition. 2019 2nd International Workshop on Computer Modeling and Intelligent Systems, CMIS, 2019, Zaporizhzhia, April 15-19, CEUR Workshop Proceedings. 2353: 211-226.

[21] Al-Gburi A. J. A., Ibrahim I. M., Zakaria Z., Nazli N.F.M. 2021. Wideband Microstrip Patch Antenna for Sub 6 GHz and 5G Applications. Przegląd Elektrotechniczny. 11, 26-29.

[22] Fedorchenko I., Oliinyk A., Stepanenko A., Zaiko T., Korniienko S., Burtsev N. 2019. Development of a genetic algorithm for placing power supply sources in a distributed electric network. European Journal of Enterprise Technologies, issue 5/101, 6-16, doi: 10.15587/1729-4061.2019.180897.

[23] A. Al-Gburi, I. Ibrahim and Z. Zakaria. 2017. Band-notch effect of U-shaped split ring resonator structure at ultra wide-band monopole antenna. International Journal of Applied Engineering Research. 12(15): 4782-4789.

[24] Oliinyk A., Fedorchenko I., Stepanenko .Rud M., Goncharenko D. 2021. Implementation of evolutionary methods of solving the travelling salesman problem in a robotic warehouse // Lecture Notes on Data Engineering and Communications Technologies. 48, pp. 263-292.

[25] I. Ibrahim, A. J. A. Al-Gburi, Z. Zakaria and H. Bakar. 2018. Parametric Study of Modified U-shaped Split Ring Resonator Structure Dimension at Ultra-Wide-band Monopole Antenna. Journal of Telecommunication, Electronic and Computer Engineering (JTEC). 10(2-5): 53-57.

[26] Fedorchenko, I., Oliinyk, A., Stepanenko, Zaiko, T., Korniienko S., Kharchenko A. 2020. Construction of a genetic method to forecast the population health indicators based on neural network models //Eastern-European Journal of Enterprise Technologies, 1(4-103): 52-63. DOI: 10.15587/1729-4061.2020.197319.

[27] A. J. Abdullah Al-Gburi, I. Ibrahim and Z. Zakaria. 2020. Gain Enhancement for Whole Ultra-Wideband Frequencies of a Microstrip Patch Antenna. Journal of Computational and Theoretical Nanoscience. 17(2): 1469-1473, doi: https://doi.org/10.1166/jctn.2020.8827.

[28] Jamil Abedalrahim Jamil Alsayaydeh, Mohd Faizal bin Yusof, Asyraf Salmi and Adam Wong Yoon Khang. 2023. Fertigation TechnologyMeets Online Market: A Multipurpose Mobile App for Urban Farming. International Journal of Advanced Computer Science and Applications (IJACSA), 14(6): 806-813. http://dx.doi.org/10.14569/IJACSA.2023.0140686.

[29] Osama Alshannaq, Jamil Abedalrahim Jamil Alsayaydeh, Montaser B. A. Hammouda, Mohanad Faeq Ali, Mohammed Abdul Razaq Alkhashaab, Maslan Zainon and Abdul Syukor Mohamad Jaya, 2022. Particle swarm optimization algorithm to enhance the roughness of thin film in TiN coatings. ARPN Journal of Engineering and Applied Sciences. (VOL. 17 NO. 2) pp. 186-193.

[30] Jamil Abedalrahim Jamil Alsayayadeh, Mohd Faizal bin Yusof, Muhammad Zulhakim Bin Abdul Halim, Muhammad Noorazlan Shah Zainudin and Safarudin Gazali Herawan. 2023. Patient Health Monitoring System Development using ESP8266 and Arduino with IoT Platform. International Journal of Advanced Computer Science and Applications (IJACSA), 14(4): 617-624. http://dx.doi.org/10.14569/IJACSA.2023.0140467.

[31] Osama Alshannaq, Mohd Rizuan Baharon, Jamil Abedalrahim Jamil Alsayaydeh, Montaser B A Hammouda, Khalid Hammouda, Mohammad

Mahmoud Nawafleh and A I A Rahman. 2022. Analysis of the Lowest Memory Consumption (Memory Usage) Through Running Different Cryptography Techniques for Different Types of Images. Journal of Physics: Conference Series, Volume 2319, International Conference on Robotic Automation System 2021 (ICORAS 2021) 25/10/2021 - 26/10/2021 Online. Osama Alshannaq *et al* 2022 J. Phys.: Conf. Ser. 2319 012027.

[32] Jamil Abedalrahim Jamil Alsayaydeh, Irianto, Maslan Zainon, Hasvinii Baskaran and Safarudin Gazali Herawan. 2022. Intelligent Interfaces for Assisting Blind People using Object Recognition Methods. International Journal of Advanced Computer Science and Applications(IJACSA), 13(5): 734-741. http://dx.doi.org/10.14569/IJACSA.2022.0130584.

[33] Jamil Abedalrahim Jamil Alsayaydeh, Irianto, Azwan Aziz, Chang Kai Xin, A. K. M. Zakir Hossain and Safarudin Gazali Herawan. 2022. Face Recognition System Design and Implementation using Neural Networks. International Journal of Advanced Computer Science and Applications (IJACSA), 13(6): 519-526. http://dx.doi.org/10.14569/IJACSA.2022.0130663.