IHJPAS. 37 (2) 2024
Ibn Al-Haitham Journal for Pure and Applied Sciences
Journal homepage: jih.uobaghdad.edu.iq
PISSN: 1609-4042, EISSN: 2521-3407

A Modern Encryption Approach to Improve Video Security as an Advanced Standard Adopted

Baydaa Jaffer Al-Khafaji[*1,2] **and Abdul Monem S. Rahma**[3]

[1] Iraqi Commission for Computers and Informatics, Informatics institute for postgraduate studies, Baghdad, Iraq
[2] Department of Computer Science College of Education for Pure Science Ibn Al-Haitham University of Baghdad, Iraq
[3] Department of Computer Science, Al-Maarif University College, Ambar, Iraq
*Corresponding Author.

Received: 10 January 2024 Accepted: 24 March 2024 Published: 20 April 2024
doi.org/10.30526/37.2. 3907

Abstract
While transmitting data across a network, it is important to keep in mind that some fields may contain sensitive information. One of the most pressing concerns, then, is the protection of private information. The confidentiality and integrity of an online video are the primary concerns of the suggested approach in this work. Video compression using Moving Picture Experts Group (MPEG), video encryption, and video decryption are the three components that make up the proposed study. The data is encrypted using one of the most used block cipher algorithms, the Advanced Encryption Standard (AES) technique. The real-time needs of frame decoding can be satisfied by a software implementation. Our research leads us to believe that this has the potential for use in safe, real-time video transmission. In this case, the compressed domain is where the video stream encryption takes place. As a result, the compression and decompression time cycles are maintained. Because of this, it is able to cut encryption time by 90% compared to the method that encrypts the entire video. However, the most bits that can be encrypted using this method are 128 bits. As a result, far fewer calculations are needed to get satisfactory encryption results. The software solution has to be fast enough for frame decoding to work in real-time. Based on our findings, this might be utilized for secure, real-time video communication. We are applying the C++ programming language for coding.

Keywords: Video compression, Moving picture experts group, Video encryption, Block cipher, Advanced encryption standard.

1. Introduction

A cryptosystem is a system that can encrypt and decode data. Combining the original material in plaintext with one or more key numbers or sequences of characters known only to the transmitter and/or receiver is a common step in encryption algorithms. Cryptography produces what is called cipher text as its output [1]. When it comes to real-time applications' security and resource savings, cryptographic techniques are crucial. [2, 3].

The field of study known as cryptography deals with the safe transmission of data via networks. An operation in the client-server paradigm is present in cryptography. Encryption takes place on the server. To prevent unauthorized users from accessing sensitive information, encryption transforms plaintext data into cipher text. The client receives encrypted data transferred via the network [4, 5]. Decryption, the process of transforming cipher text into plaintext, is executed on the client side. Two types of cryptographic algorithms, the symmetric key algorithm and the asymmetric key algorithm, are available for use in cryptographic systems to safeguard data [6, 7]. The transmitter and recipient sides of a symmetric key algorithm share the same key [8, 9]. The third. Cryptographic algorithms that use symmetric keys include the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). On the other hand, Algorithms that employ asymmetric keys, such as Rivert Shamir Adleman (RSA), use two separate keys. It is more effective to use the AES algorithm for both software and hardware implementations when transmitting data at fast speeds. Implementing hardware with a high level of security is crucial for wireless video communication systems [10-15]. For most video processing needs, the most practical standard is MPEG (Moving Picture Experts Group), which stands for moving picture expert group. Forms of multimedia communication include video conferencing, video on demand, multimedia email, and video broadcast. As the video's redundancy decreases, the video becomes more secure since attackers are unable to deduce as many details about it. Groups of images (GOPs) are the basis of MPEG video [16, 17]. A GOP (group of images) is made up of a sequence of frames labeled I, P, and B. In I-frames, no reference to other frames is made; in P frames, a prior I or P frame is used for predictive coding; and in B frames, data is interpolated in both directions from both the I and/or P frames that came before and after it [18]. There are two ways to encrypt an MPEG video stream for safety: either partially or completely [19, 20]. Algorithms that use all of the available data are considered heavyweight, whereas algorithms that use only some of the available data are considered lightweight. Complex computations are involved in both of these methods [23]. Lightweight algorithms offer an adequate level of security with a reasonable computing cost for MPEG video applications, whereas heavyweight algorithms annoy the problem and increase the time. In this paper, we introduce an effective AES-based MPEG video encryption method for use in real-time video transmission. A lightweight selective encryption technique was introduced here for safe MPEG transmission. The Video Encryption Algorithm (VEA) is its foundation. Built on the foundation of DES and IDEA, VEA is a lightweight algorithm for selective encryption. Using AES to encrypt data dramatically improves security. By processing within the bounds of the maximum number of bits used, this approach reduces computing time [20-23].

2. Literature Review

Despite the fact that video encryption has become an important topic because of the vast amounts of data carried via networks, relatively few studies have really addressed this specific issue. The most significant algorithms for video encryption are presented in the following works:

In order to demonstrate a high degree of security and improved picture encryption, Shakerian R., Hedayati M., and Rahmani M. employed the altered advanced encryption method. To make the change, tweak the shift-row transformation. This article compares the outcomes of the original AES algorithm with those of the updated AES algorithm. [24].

Nguyen Van Loi and Hoang Trang's work results in an architecture with little complexity, which in turn allows for fast throughput and low latency. With a 128-bit block and key size and an S-box lookup table implementation, the design employed an iterative looping technique [25].

Malladar and Kunte's work focuses on encrypting only the part of the frame that Video on Demand (VoD) cares about the most. The entropy-based video encryption that was used for this study was evaluated using unique metrics like correlation coefficient, PSNR, NPCR, and histogram. Applications of the method in VoD have taken advantage of the results, which have given almost optimal values [26].

The authors in [27] suggested that data encryption methods are crucial to modern information system security. A number of new models have put chaos and image encryption approaches in the spotlight. This research presents a new hybrid encryption method that uses three separate chaos maps, Baker, Arnold, and Henon, applied to one red-green-blue channel each. Information security is enhanced in the proposed paradigm since unlocking encryptions requires three distinct keys.

In [28], the authors provide a novel method for encrypting grayscale images that makes use of the cross-coupling of two piece-wise linear chaotic maps (PWLCM). This approach does both the permutation and diffusion operations using cross-coupled PWLCM devices. The row-column diffusion operation uses the sorted iterated sequences of cross-coupled PWLCM systems, and the row-column permutation operation uses the indexed sequences that go with them. The cross-coupled chaotic map improves chaos's discrete dynamics by getting rid of the problem of using a single chaotic map for permutation-diffusion operations. The cipher output is produced by combining multiple chaotic orbits, which makes cryptanalysis of the cipher picture more complicated when a cross-coupled chaotic map is used. Cross-coupling a single type of chaotic map, specifically a PWLCM system, further improves the algorithm's software and hardware efficiency. Additionally, the algorithm's encryption speed is enhanced by utilizing the PWLCM mechanism. Additionally, the suggested method protects the algorithm from known-plaintext and chosen-plaintext attacks by using the Secure Hash Algorithm SHA-256.

3. Cryptography

When transmitting data over insecure lines, cryptography is the study of utilizing mathematical models to encrypt (transform readable information or plaintext) and decode data for security purposes. Attackers are those who can break encrypted communication without authorization through cryptanalysis, which is the study of deciphering the cipher text to its original plain text. Encryption is the definition that is most commonly attached nowadays. In other words, the encryption process changes the original data from plain text to a secret cipher text, while the decryption process returns the cipher text to its original form.

3.1 Asymmetric Key Cryptography

Essential Basic Two distinct keys, a public key, and a private key are utilized in asymmetric cryptography, often known as cryptography. The public key is freely circulated, while the private key is kept secret. The recipient can decode a message using their private key, which is the same as the public key used for encryption, using this approach [29].

3.2 Symmetric Keys Cryptography

In symmetric cryptography, the key used to encrypt and decode data remains unchanged from one operation to the next. Both parties must participate in the message exchange and keep this shared key secret. Hidden crypto algorithms include DES, AES, and RC6. Two types of symmetric ciphers exist, though: stream ciphers and block ciphers [30-34].

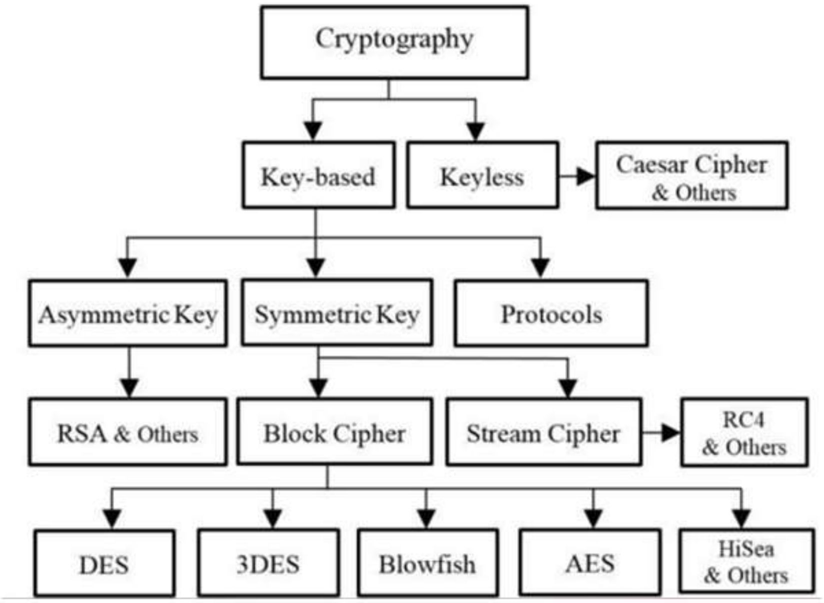


Figure 1. Types of Cryptography Algorithms

4. Proposal for the Modern Security Protocol (AES)

The National Institute of Standards and Technology has officially selected AES as its standard encryption technology. National Institute of Standards and Technology is used to guarantee facts when conversing. To function, AES relies on a substitution permutation network. AES uses a capacity of 128 bits for blocks and a possible key size of 128 bits, 192 bits, or 256 bits. Everything in the algorithm is divided into two parts: the area for key expansion and the state central processing unit. The number of rounds is 10 when dealing with 128 of the key's bits (12) when the key length is 192 bits and 14 when the key size is 256. Each encryption cycle includes the following: It consists of four stages:

1. Byte substitution.
2. Row shifting.
3. Mixing. Column headings.

4. Include a rounded key. Next, do an XOR operation.

The procedure combines the results of the prior three stages with four phrases taken from the essential schedule. Look at the table below for a comparison of various video methods for encrypting data. Down below, you can see the block diagram of the suggested solution for real-time video encryption.

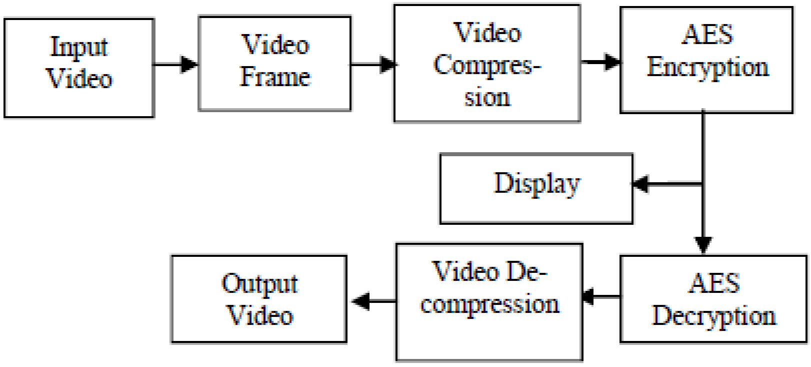


Figure 2. The MPEG Video Encryption and Decryption Block Diagram

The three steps of video compression, AES encryption, and AES decryption are illustrated in the picture above. Each step is described in detail below.

I-Video encoding

At one point, footage shot by the camera with a fixed resolution of 256 by 256 pixels is put in. The compression process is applied to the video frame sequence. Luminance (Y) and chrominance (UV) are the two components that make up a frame. First, this frame's RGB values are converted to grayscale. The grayscale frame uses fewer bits per pixel because of this. This grayscale picture becomes a floating-point one. The image used for DCT analysis is floating-point. Then, retrieve the value of the DCT coefficient by applying it to the float picture. The frame sign bit is the value of this DCT coefficient. Determine the AES-specific sign bit value of the DCT coefficient. Apply the 128-bit Advanced Encryption Standard (AES) algorithm to the first frame's sign bit value. Motion vectors may be obtained from frames I and D. Next, find the vector's sign value.

II. Advanced Encryption Standard (AES)

Protected data transmission using AES SSL. The National Institute of Standards and Technology (NIST) has selected AES as the standard. For this procedure, a block cipher of 256 bits, 128 bits, or 192 bits was utilized. In this case, we chose a 128-bit encryption algorithm. After being transformed into a state matrix, the array of plaintext serves as the input to the cipher. Keys for transformation rounds are never explicitly stated but are instead an extension of cipher keys. The four most basic transformations, including Add Round Key Byte Sub, Shift Row, and Mix Column, are all that is required for a round transformation. The transformation is applied again 10 times.

Our video compression process yields an array of sign bit values for each frame and motion vector. We feed this data into the AES algorithm, which encrypts the data using a secret key. The cipher's input is a 4x4 matrix containing differential values. After ten rounds of AES encryption, a cipher output is produced; only the owner of the secret key can decipher it.

III. Advanced Encryption Standard Decryption

Except for performing inverse operations during decryption, the encryption and decryption algorithms are identical. Upon completion of the decryption procedure, the user will be notified. When decryption is complete, reverse DCT will propagate the modified coefficients.

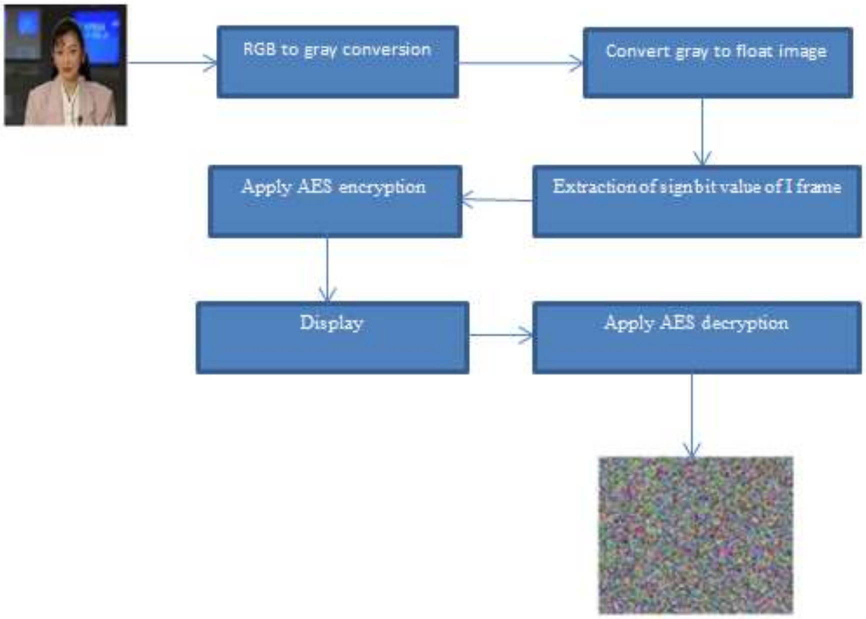
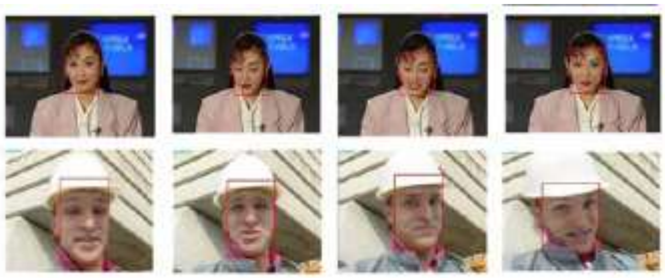


Figure 3. Block diagram of the proposed system

5. Results and Simulation Test

Experiments were carried out using real-time MPEG video. Ubuntu, an operating system based on the Linux platform, is used to introduce a secure video communication system. I use the C++ programming language for my coding. While communicating in real-time, encryption is performed on the server side, and decryption is performed on the client side. In this case, just one system was found to be server-side. We couldn't possibly fit all the picture frames here. Instead, we display a single frame from the whole video sequence in order to showcase our method. If we encrypt the sign bits of all the DCT coefficients in only one frame, we have an unintelligible video recording. We are currently using a medium level of encryption, as shown in **Figure 4.**

Without decrypting the sign bits and motion vector coefficients, the video picture becomes unintelligible. The vector of motion is collected from the reference frame and the I-frames. When you combine motion vectors with a P frame, you can extract the difference between the two. Utilizing AES on the sign bits of the motion vector difference yields a more robust encryption level compared to the prior one. **Figure 5**



Figure(4) video before encryption

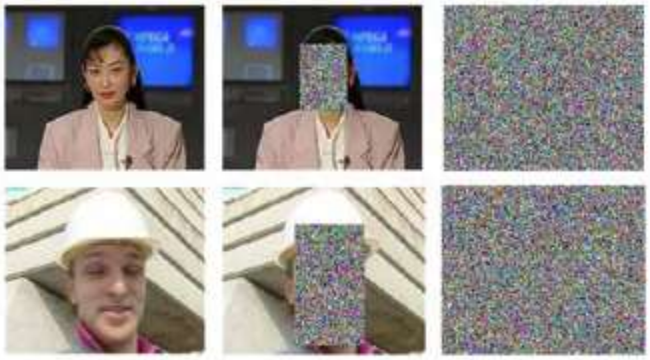


Figure 5. video after encryption

As far as anyone can tell, the key played a significant part in the encryption process, which greatly enhanced security, fortified the algorithm, and made it resistant to attackers. As is well known, the results of the NIST key tests were generally positive; furthermore, the enciphered image could not be deciphered even with a slight difference in key values **Table 1**.

Table 1. Values of NIST Tests

Type of Test	P-Value	Status
Frequency test (Mono bit)	0.9605226524	Random
Frequency test within a Block	0.0290851864	Random
Runs test	0.9582660454	Random
Longest Run of Ones in a Block	0.5973225710	Random
Binary Matrix Rank	0.5608014420	Random
Discrete Fourier Transform (Spectral)	0.6531751671	Random
Non-Overlapping Template Matching	0.5214836922	Random
Overlapping Template Matching	0.1631537766	Random
Maurer's Universal Statistical	0.2487526006	Random
Linear Complexity	0.4604387067	Random
Serial test	0.0407380230	Random
Approximate Entropy	0.6553999692	Random
Cumulative Sums (Forward)	0.9085205277	Random
Cumulative Sums (Reverse)	0.9144078012	Random
Random Excursions (+1)	0.4939534908	Random
Random Excursions Variant (+1)	0.3326976824	Random

The consideration of speed in encryption procedures is crucial when encrypting video **Table 2**.

Table 2. Full Encryption time for five frames to each video sample

Video size	Frame name	Encryption time	Decryption time
2.33 MB	Frame 1	18.871 22.337	18.871 22.337
	Frame 2	20.410 18.246	20.410 18.246
	Frame 3	22.120 19.508	22.120 19.508
	Frame 4	21.915 18.940	21.915 18.940
	Frame 5	21.024 17.899	21.024 17.899
4.21 MB	Frame 1	18.871 22.337	18.871 22.337
	Frame 2	20.410 18.246	20.410 18.246
	Frame 3	22.120 19.508	22.120 19.508
	Frame 4	21.915 18.940	21.915 18.940
	Frame 5	21.024 17.899	21.024 17.899

6. Conclusion

A portion of the video is encrypted only when using a selective encryption technique. Going the full AES route for video encryption takes more time than either option. When looking at MPEG frames, it was discovered that sign-bits only take up around 10% of the total video bitstream in typical MPEG-1 films. This allows it to significantly reduce encryption time, up to 90%, compared to the technique that encrypts the full movie. In any case, the maximum number of bits that this technique can encrypt is 128 bits. Achieving adequate encryption results requires far fewer calculations. For frame decoding to work in real-time, a software implementation must be quick enough. Our research leads us to believe that this has the potential for use in safe, real-time video transmission. The results demonstrate the efficacy of the proposed algorithms. Future work will center on improving security by cryptographically signing and encrypting key images, as a single key picture is used for both encryption and decoding. Time may be recorded by using the chosen encryption method.

Acknowledgement

I extend my thanks to the College of Education for pure science Ibn Al-Haitham, University of Baghdad for assisting in completing this work by opening private laboratories and providing scientific facilities by the staff of the Computer Department to help support the research project.

Conflict of Interest

The authors declare that they have no conflicts of interest.

Funding: None.

References

1. Shukur, A.; Badrulddin, A.; Nsaif, M. K. A proposed encryption technique of different texts using circular link lists. *Periodicals of Engineering and Natural Sciences*. **2021**, *9*, 1115-1123,
2. AlKhafaji, J; Salih, M; Shnain, S; Nabat, Z. Improved technique for hiding data in colored and monochrome images. *Periodicals of Engineering and Natural Sciences*. **2020**, *8(2)*, 1000–1010.
3. Iptehaj, Alhakam; Nassir, H Salman. An Improved Probability Density Function (PDF) for Face Skin Detection, *Iraqi Journal of Science*, **2022**, *63(10), 4460–4473* https://doi.org/10.24996/ijs. 63.10.31
4. Shukur, WA; Kubba, ZMJ. Arabic and English Text Encryption Using a Proposed Method Based on the Coordinates System. *International Journal of Advances in Soft Computing & Its Applications*. **2023**, *15(2)*, https://doi.org/10.15849/IJASCA.230720.17
5. AlKhafaji ,J; Salih, M; Shnain, S.; Nabat, Z .Segmenting video frame images using genetic algorithms, *Periodicals of Engineering and Natural Sciences* **2020**, *8(2)*, 1106–1114. http://dx.doi.org/10.21533/pen.v8i2.1351
6. J Kromka, O Kováč, J Šaliga, M Ultiwavelet Toolbox for MATLAB, *International Conference Radioelektronika (RADIOELEKTRONIKA)*, https://doi.org/1109/RADIOELEKTRONIKA54537.21-22 April 2022 - ieeexplore.ieee.org
7. Shi and Bhargava, A Fast MPEG Video Encryption Algorithm, *Proceedings of the 6th ACM International Conference Bristol*, UK, pp. 81–88, September **1998**.
8. Lian, Multimedia Content Encryption: *Techniques and Applications*, CRC, **2008**.
9. Agi and L. Gong, An Empirical Study of MPEG Video Transmission, *Proceedings of the Internet Society Symposium on Network and Distributed Systems Security*, pp. 137–144. San Diego, CA, February **1996**. https://doi.org/10.1109/NDSS.1996.492420
10. S. Harba,E.S. Harba, S. SH. Hussein, and M. K. Farttoos, Improving accuracy of CADx systems by hybrid PCA and backpropagation, *IEEE Xplore*, **2018**. https://doi.org/10.1109/CATA.2018.8398681
11. SH. Hussein, S. SH. Altyar, and I.A. Abdulmunem, Improve the Fully Convolutional Network Accuracy by Levelset and the Deep Prior Method, *Iraqi Journal of Science*, **2023**, *Vol. 64*, *No. 5*, pp. 2575–2588. https://doi.org/10.24996/ijs.2023.64.5.39
12. SH. Altyar, S. SH. Hussein, and M. J. Mohammed, Human recognition by utilizing voice recognition and visual recognition, *Int. J. Nonlinear Anal. Appl.* 13 (**2022**) *No. 1*, 343–351, 2021. https://doi.org/10.22075/IJNAA.2022.5501
13. Adam J. Slagell. Known-Plaintext Attack Against a Permutation Based Video Encryption Algorithm. Available from: http://eprint.iacr.org/2004/011.pdf.(Accessed on March 2, **2009**)
14. Karthik Thiyagarajan. Low Computational Overhead Video Encryption for Wireless Multimedia Devices, Dalhousie University. **2014**. http://hdl.handle.net/10222/54564
15. Ali, H.; Abdullah, W. N. A survey of similarity measures in web image search. *International Journal of Emerging Trends in Technology in Computer Science*, **2016**, *4(4).*
16. Katoch, S.; Chauhan, S. S.; Kumar, V. A review on genetic algorithm: past, present, and future. *Multimedia tools and applications*, **2021**, *80*, 8091-8126. https://doi.org/10.1007/s11042-020-10139-6
17. AlKhafaji, B.J.; Salih, M.A.; Shnain, S.A.; Rashid, O.A.; Rashid, A.A.; Hussein, M.T. Applying the Artificial Neural Networks with Multiwavelet Transform on Phoneme recognition. IOP Publishing. *Journal of Physics: Conference Series* **2021**, *1804 (1)*, 012040. https://doi.org/10.1008/1742-6596/1804/1/012040

18. Rahma, AM; Rahma, MA; Rahma, MA. Automated analysis for basketball free throw. In *IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*. **2015**, 447–453. https://doi.org/10.1109/IntelCIS.2015.7397259
19. Abdullatif, FA; Shukur, WA Blind Color Image Steganography in Spatial Domain. *Ibn Al-Haitham Journal for Pure and Applied Science*. **2011**, *24(1)*, 338–346-346 cy44
20. Mozaffari, S. Parallel image encryption with bitplane decomposition and genetic algorithm. *Multimedia Tools and Applications*. **2018**, 77*(19)*, 25799-25819.
21. Gupta, M.; Gupta, K. K.; Shukla, P. K. Session key-based fast, secure, and lightweight image encryption algorithm. *Multimedia Tools and Applications*. **2021**, *80*(*7*), 10391–10416. https://doi.org/10.1007/s11042-020-10116-z
22. Mahdi, M. S.; Azeez, R. A.; Hassan, N. F. A proposed lightweight image encryption using ChaCha with hyperchaotic maps. *Periodicals of Engineering and Natural Sciences (PEN)*. **2020**, *8*(*4*), 2138–2145. http://dx.doi.org/10.21533/pen.v8i4.1708
23. Wei, D.; Jiang, MA. Fast image encryption algorithm based on parallel compressive sensing and DNA sequence. *Optik*. **2021**, *238*, 166748. https://doi.org/10.1016/j.ijleo.2021.166748
24. Kamali, S.H.; Shakerian, R.; Hedayati, M.; Rahmani, M. A new modified version of advanced encryption standard based algorithm for image encryption. In *International Conference on Electronics and Information Engineering*. **2010** *1*, V1-141. https://doi.org/10.1109/ICEIE.2010.5559902
25. Hoang, Trang; Nguyen Van Loi. An Efficient FPGA Implementation of the Advanced Encryption Standard Algorithm. *IEEE International Conference on Computing and Communication Technology*, Ho Chi Minh City. **2012**, 1–4.
26. Malladar, R.; Sanjeev Kunte, R. Selective video encryption based on entropy measure. *Integrated intelligent computing, communication and security*. **2019**, 603-612. https://doi.org/10.1007/978-981-10-8797-4_61
27. Elshamy, A.M.; Hussein, A.I.; Hamed, H.F.; Abdelghany, M.A.; Kelash, H.M. Color image encryption technique based on chaos. *Procedia Computer Science*. **2019,** *163*, 49-53. https://doi.org/10.1016/j.procs.2019.12.085
28. Patro, K. A. K.; Acharya, B. A secure block operation based bit-plane image encryption using chaotic maps. In *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)* **2020,** 411-416. IEEE. https://doi.org/10.1109/ICPC2T48082.2020.9071483
29. Shivan Othman, P.; Reber Ihsan, R.; Masoud Abdulhakeem, R. The Genetic Algorithm (GA) in Relation to Natural Evolution. *Academic Journal of Nawroz University*. **2022**, *11*(*3*), 243–250. https://doi.org/10.25007/ajnu.v11n3a1414
30. Hussein, S. SH.; Altyar, S. S.; Tawfeeq, L. A.; Harba, E. S. Reconstruction of Three-Dimensional Objects from Two-Dimensional Images by Utilizing Distance Regularized Level Algorithm and Mesh Object Generation, *Baghdad Science Journal*. **2020**, *17(3)*, 899–908. DOI: http://dx.doi.org/10.21123/bsj.2020.17.3.0899
31. Bushra Kh AlSaidi; Baydaa Jaffer Al-Khafaji; Suad Abed Al Wahab. Content-Based Image Clustering Technique Using Statistical Features and Geneti, *Algorithms Engineering, Technology, and Applied Science Research*. **2019**, *9(2)*.
32. A. M. Sagheer; M. S. Al-Ani; O. A. Mahdi, "Ensure Security of Compressed Data Transmission," *2013 Sixth International Conference on Developments in eSystems Engineering*, Abu Dhabi, United Arab Emirates, **2013**, 270-275, https://doi.org/10.1109/DeSE.2013.55.

33. Al-Khafaji, B.J.; Rahma, A.M.S. A Modern Encryption Approach to Improve Video Security as an Advanced Standard Adopted. *Ibn AL-Haitham Journal For Pure and Applied Sciences*, **2024**,*37(2),* ,460-470. https://doi.org/10.30526/37.2.3907
34. May A. Salih; Shaymaa AbdulHussein Shnain; Baydaa Jaffer AlKhafaji. Using RC6 in embedding information in spatial parts of image construction, *Turkish Journal of Computer and Mathematics Education*, **2021**, *12, 11*.