Academic Journal of Nawroz University (AJNU), Vol.12, No.3, 2023

https://doi.org/10.25007/ajnu.v12n3a1643

Image Encryption based on AES Algorithm and XOR Operation

Veman Ashqi Saeed[1], Bareen Haval Sadiq[2]

[1]Technical College of Administration, Information Technology Management Dept., Duhok, KRG – Iraq
[2]Technical Collage of Administration, Duhok Polytechnic University, KRG – Iraq

Abstract

Sending digital pictures across open networks has emerged as a major privacy risk in recent years. Despite the environment's adaptability and the many benefits it offers, there are, however, a significant number of threats to one's privacy and safety. A great number of cryptosystems have been proposed in the literature on picture encryption in an effort to make communication more secure. For the purpose of data transmission, the AES algorithm is utilized due to the increased efficiency it offers in the block. This paper proposes image encryption techniques based on the AES algorithm and Henon map. The plain image has been encrypted using the AES algorithm at the first step. Then, the Henon map is used to generate a random key which is required to provide the second step of encryption. This step of encryption has been performed using the XOR operation. The results of the studies demonstrate that the strategy proposed resolves the issues that are present in conventional techniques of encryption. The histogram of the encryption picture is consistently spaced despite being different from the histogram of the original image. The recommended approach is extremely sensitive to the key value; even minute adjustments result in a distinct visual representation. As a result, apps that provide real-time picture encryption while operating over unsecured networks are suitable for the unique technique.

Keywords: Image encryption, Grayscale image, AES, XOR operation.

1. Introduction

In recent years, as a result of the rapid growth of technology for network connection, the options for people all over the world to use the Internet have grown increasingly popular, and the frequency with which information and data are shared has increased [1]. There is already multimedia and visual material, and it is widely employed in many different disciplines, such as the exchange of private data in the healthcare and military fields. Techniques of cryptography are not only utilized in picture and multimedia files, but they are also essential for the protection of sensitive user information (such as credit card data), cloud computing, and other areas. It is of the utmost importance to have a reliable encryption system in place to safeguard the transfer of sensitive information [2]. As a result, the technology behind encryption is garnering an increasing amount of attention. The picture encryption technique that is based on chaotic systems has been the subject of a significant amount of research, and its intrinsic properties, including initial sensitivity, unpredictability, and pseudo-randomness [3], have also been investigated. This demonstrates the intimate connection that exists between chaotic systems and cryptography. Because of the vast volume of picture data and the high computational cost, the impact of image encryption utilizing DES and AES for text information encryption is not especially suitable. Even while classic encryption methods such as DES and AES have produced excellent outcomes in text encryption, these technologies have not been able to produce acceptable results in image encryption. The unpredictability of chaotic systems and their tendency to hybridize are reminiscent of the scrambling and diffusion processes used in cryptography [4].

There are two components to any encryption and decryption procedure: the algorithm, which is used to encrypt and decrypt data, and the key, which is needed to access encrypted data. The security provided by the cryptographic process is, however, dependent on the key that is employed both during encryption and decryption. There are two different kinds of cryptographic mechanisms: symmetric key cryptography, in which the same key is used for both encryption and decryption; and asymmetric key cryptography, in which different keys are used for each function. In the case of asymmetric key cryptography, the process of encrypting and decrypting data requires the use of two distinct keys. When compared to the asymmetric key technique, the symmetric key approach is considerably quicker, less difficult to build, and requires less amount of computer power [5]. The process of transforming data that can be understood and read into data that cannot be understood or read is known as encryption. In addition, the process of decryption, which is the

reverse of encryption, returns the data to its understandable original form. This process alters the information. In addition, there are two distinct methods for encrypting data: symmetric encryption, which utilizes a secret key, and asymmetric encryption, which makes use of a public key. Data may be encrypted and decrypted with symmetric encryption techniques by employing a single secret key. Both the sender and the recipient have access to the secret key, but this information must be kept strictly confidential. In addition, the vast majority of software and hardware standards that make use of symmetric encryption rely on one of the most used symmetric algorithms, such as the Advanced Encryption Standard (AES) [6]. In the case of asymmetric encryption methods, the process of encrypting and decrypting data requires the use of two distinct keys: a private key, which must be kept a secret, and a public key, which may be made available to anybody. Furthermore, the majority of software and hardware standards algorithms that employ asymmetric encryption for encryption and decryption rely on one of the most frequently used asymmetric algorithms, such as the Rivest-Shamir-Adleman (RSA) algorithm [7], which was developed by Ronald Rivest. In today's world, there is a growing interest in the field of picture encryption within the scientific community in order to safeguard precious photos from being read by unauthorized parties. Therefore, in order to accomplish this objective, many encryption al-algorithms, such as AES and RSA algorithms, were utilized in the process of encrypting digital images.

This paper focuses on the implementation and evaluation of image encryption using the Advanced Encryption Standard (AES) algorithm a widely recognized and extensively studied symmetric encryption scheme. AES has earned its reputation as one of the most secure and efficient cryptographic algorithms, making it a prime candidate for safeguarding visual information against modern threats. In this study, we explore the application of AES in the context of image encryption, considering its ability to protect against unauthorized access, data tampering, and other malicious activities. AES employs a block cipher structure with variable key lengths, offering a high degree of flexibility and scalability to accommodate the specific security requirements of different image data types and sizes. Furthermore, we investigate the performance of AES in comparison to other image encryption techniques, including traditional methods and alternative modern cryptographic algorithms. By subjecting AES to a battery of tests, including security analysis, computational efficiency assessment, and resistance to attacks, we aim to provide a thorough understanding of its strengths and potential vulnerabilities in the domain of image encryption.

2. Related Work

The Advanced Encryption Standard (AES) is an effective symmetric cryptosystem that has the benefit of a great capacity to withstand assaults; as a result, it is utilized extensively in the data encryption industry. The current consensus among a number of professionals in the field of picture encryption is that AES is a reasonably secure algorithm, but that it cannot be used to encrypt photographs. The reason for this is that the data associated with the images are much larger and include a higher degree of redundancy than text data. On the other hand, Zhang et al. developed a picture encryption technique using AES [8]. The authors organize the pixel values that make up the basic picture into data blocks that have a length of 128 bits each. They do a permutation on the starting vector as well as the first data block. After then, more data blocks are encrypted with the AES using the cipher block chaining method. Even though the creators of the technique said that it is capable of high encryption speed, the efficiency may still be further improved. Priya S. and colleagues [9] have suggested a visual meaning of complete picture encryption as a means of protecting the medical image, the patient's electronic health record (EHR), and the fingerprint of the attending physician in order to guarantee the validity of the image. To create a watermarked medical image, the EHR was incorporated into the primary medical image using a watermarking approach. This produced the watermarked medical image. After that, the watermarking of the medical image and the doctor's fingerprint are both encrypted using the Integer Wavelet Transform (IWT) in conjunction with a regular reference image. IWT may be undone without causing any data loss by first decrypting the encrypted medical picture and then comparing the decrypted fingerprint to the fingerprint of the treating physician. The electronic health record (EHR) as well as the medical image may be encrypted into a seemingly insignificant image using this method, and the sender's authentication can be verified using the physician's fingerprint.

Comparing the Advanced Encryption Standard (AES) with the Rivest-Shamir-Adleman (RSA) encryption algorithms in picture encryption with the help of MATLAB [10] is the purpose of this investigation. The quality of the picture encryption provided by each technique is evaluated as part of the comparison

process. In addition, an analysis of the correlation findings and the histogram. According to the findings, the AES method provides superior picture encryption quality, as seen by the histogram's greater number of converging columns. Bahrami et al. [11] provided a method for the partial encryption of pictures by making use of an orthogonal transform known as the Discrete Cosine Transform (DCT). This method is effective for the compression of multimedia data. Quantization of the DCT coefficients is followed by the calculation of the entropy coding to obtain a compressed version of the image. After that, the picture that has been compressed is ciphertext using a stream cipher, with the encryption key being created in a manner analogous to that of the AES key creation procedure. Then, a distinct stream cipher technique is used for each coefficient in order to encrypt it. [12] presents a novel algorithm for Dynamic AES that was built by key dependent dynamic S-Box employing dynamic irreducible polynomial and affine constant approach. Both color and grayscale photos are used in the analysis process. Standard AES and Dynamic AES are utilized in the process of encrypting and decrypting both of the pictures. Image Histogram Analysis, Adjacent Pixel Correlation Analysis, Image Entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), and Encryption Quality are some of the characteristics that are used to evaluate the algorithm's quality and the amount of protection it provides.

Priynka Sharma [13], the researchers suggested making a tweak to the key expansion of the algorithm used by AES. Because the keys that are used are generated by the sender and the receiver based on the key expansion process of modified AESS, the initial key only involves a single participant rather than the entire set of keys. The pictures that were employed to evaluate how well the algorithm performed were created by drawing standard bench and mark images from the USCC-SIPII database. These images were then utilized in the evaluation. The outcomes of the security efficiency tests performed on the modified method demonstrate that it provides a flawless battle against brute force, key sensitivity tests, and statistical crypt analysis. Abhinav Gupta and Aayush Gupta, [14], have explored a unique photo encryption technique in their research article. their approach has its roots in the improved AES algorithm. This explored method has various benefits in comparison to the already available picture encryption methods. These benefits include reduced computational complexity and a shorter time required for image encryption, both of which are in great demand around the globe for the effective and speedy transmission of images via communication channels. The suggested technique is more secure and quick, and it maintains the secrecy of the photos despite numerous noise attacks by several strikers across the communication channel while the pictures are being sent for a variety of different reasons. Sarah Jassim and Sarab M. Hameed [15]the researchers in the study presented a modified AES named (M--AES) to enhance the efficiency" of the AES algorithm by upgrading the security algorithm to implement the technique for encrypting color pictures. The researchers titled their proposal Increasing the Efficiency of the AES Algorithm. The "well-known AES algorithm" has had its Shift-Rows transformation modified in order to accommodate the adjustment. The effectiveness of the modified M-AES method is evaluated by analyzing a large number of examples taken from the picture dataset maintained by the Signal-and-picture-Processing Institute (SIPI). According to the findings, the suggested change to the original AES algorithm produces satisfactory outcomes when applied to the task of picture encryption.

The related work section focusing on image encryption using the AES algorithm is still considered open research to improve image encryption techniques. Despite the vast amount of research dedicated to encryption techniques, there appears to be a lack of comprehensive studies specifically exploring the application of the AES algorithm for securing images. While AES is widely acknowledged as a robust and widely-used encryption standard for textual data, its suitability and effectiveness when applied to image encryption have not been extensively investigated. Existing research primarily focuses on AES for general data encryption or text-based scenarios. Future studies should concentrate on evaluating the performance, security, and efficiency of the AES algorithm specifically in the context of image encryption, thereby contributing valuable insights to the field of image security.

3. Methodology

Before getting into the specifics of discussing the suggested scheme, it is necessary to first describe three essential operations that collectively form the ciphering process. The first step in the process is known as the encryption phase, and it refers to the procedure of encrypting data with the AES algorithm. The procedure of producing a key by making use of the Henon map constitutes the second phase. The XOR operation is the third type of procedure that may be used. The three procedures that were just outlined are broken down into their individual steps in the

following subsections. The whole process for the diagram is depicted in Figure 1.

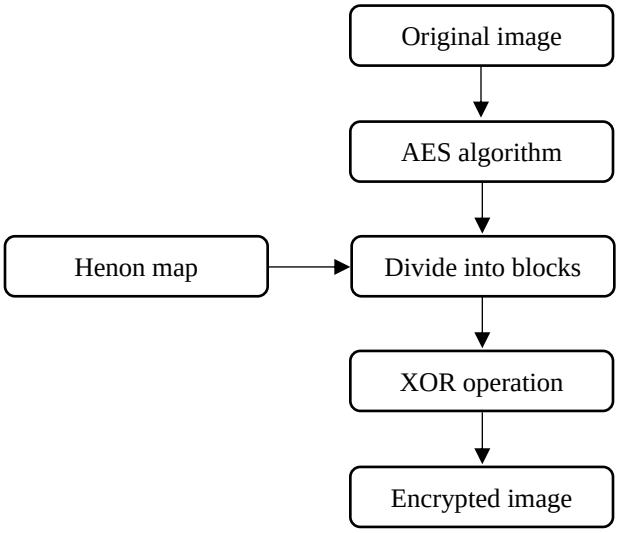


Figure 1: Block Diagram of General Methodology

3.1 AES Algorithm

The AES algorithm is an encryption technique that utilizes a block cipher and has a cipher length of 128 bits. 1997 was the year that saw Vincent Rijmen and Joan Daemen develop it further. In addition, the AES algorithm is comprised of 10, 12, or 14 processing rounds, depending on whether the key being used is 128,192, or 256 bits [16]. This method begins by deriving the set of round keys from the encryption key. After that, it initializes the state array with the block data (plaintext) in order to begin the process of operating the rounds. The initial round is referred to as the AddRoundKey round, and it involves carrying out an XOR operation between the working state and the round key at each loop of the round. Then, all of the rounds that come in between the first round and the final round are the same and are made up of four different operation blocks, as seen in Figure 2. AES makes use of four different procedures.

1. The SubBytes operation is an operation that replaces every byte of the state with a new byte by utilizing an 8-bit S-box.
2. The ShiftRows operation moves the ith row of the state to the left by *i* a number of bits. This is accomplished via the ShiftRows operation.
3. The MixColumns operation acts on the columns of the state; more specifically, each column is independently altered by making use of an operation matrix.
4. AddRoundKey operation: The XOR operation is used in the AddRoundKey operation, which combines each column of the state with the round key.

During the process of encryption, the plain text is first changed into a state, after which the AddRoundKey operation is carried out and the encrypted data is passed on to subsequent rounds. There are a total of four operations in each round, with the exception of the final round, which only includes three. Additionally, the last round does not include a MixColumns operation. The Key Expansion mechanism is responsible for the generation of round keys that are utilized in the AddRoundKey action. The round key and the cipher key are two very separate things. The sole difference between encrypting something and decrypting it is that in decryption we utilize the inverse of the procedures that were used in the encryption, with the exception of the AddRoundKey action. The following is a list of the benefits that would result from implementing the system that has been proposed: Using this strategy will not compromise the safety of the data. The fact that the information is encrypted means that none of the users will be able to access it directly. Last but not least, the data may be decrypted by legitimate users only if they have the appropriate decryption key.

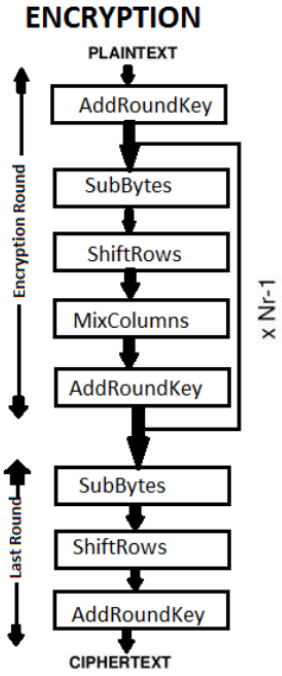


Figure 2: The Process of the AES Algorithm

3.2 Henon map

Henon is a two-dimensional dynamic system that was suggested [17] to simplify the Lorenz map [18], and its definition is (1). It shares the same features as the Lorenz map. It's possible that putting this into practice will be simpler than working with the equations for differential equations of the Lorenz system. Consider:

$$x_{i+1} = y_{i+1} + 1 - \propto x_i^2, \quad y_{i+1} = \beta x_i \tag{1}$$

The first parameters are and the starting point is at (x0, y0) in the coordinate system. Through the use of the Henon map, each point (xn, yn) is transformed into a brand new point (xn+1, yn+1). When is equal to 1.4 and is equal to 0.3, the Henon function exhibits chaotic behavior, and the iterations have a chaotic attractor in the shape of a boomerang. The contour of a two-dimensional plane for the Henon map is shown in Figure 1. This plane was generated by performing a certain number of iterations beginning at the point (0.1, 0.1) that was selected as the initial point. Minor shifts in the starting point can result in substantial behavioral differences and significant alterations.

3.3 XOR operation

The output of the AES algorithm, as well as a key, are both required inputs for this method. It implements byte substitution in addition to doing an XOR encryption with a key length that is configurable. It is possible to perform a variety of various combinations involving these two encryptions, with the decryption carrying out the inverse of the stages that were done in the opposite order [19].

The XOR encryption step of the method treats the picture as a stream of bytes, and subsequently divides the image into groups, which are one-dimensional blocks. After this, the image is encrypted. Suppose the input picture contains *n* bytes, and the key has *b* bytes, which will be referred to as key [0] through key [b-1] in this example. The picture is broken up into numerous different bytes, and group number *j* will include key [i] bytes if and only if $j = (b \times c + i)$ for some positive integer *c*. For instance, if a key is 16 bytes long and the value of its key[5] is 70, then the picture will have groups that are each composed of 70 bytes. These groups will be numbered 5, 21, 37, 53, 69, etc., and they will be scattered across the image.

3.4 Decryption process

The user will now attempt to upload the encrypted file into the application as input, and the user will be prompted to enter the generated password in order to decrypt the file. This is the final step in the process. If the user of the data enters the correct password, then the data may be decrypted and shown in a form that is more similar to a plain picture. If the right password is not entered, the data will not be able to be decrypted and shown in its original plain-text form. The procedure for decryption is quite similar to the algorithm for encryption; in both cases, each of the processes described above may be readily reversed. The inverted processes are carried out in the opposite sequence, and the decryption successfully recovers the initial picture with no data being corrupted in the process.

4. Results

Combining these two different kinds of encryption processes namely, employing AES encryption and the XOR operation is what gives the new method its enhanced level of safety. The encryption may become susceptible to brute-force and plaintext attacks if AES encryption is employed on its own. If you just use XOR to encrypt data, you can leave yourself open to statistical assaults. A large amount of resistance to all of these different kinds of assaults may be achieved by the combination of these two encryption methods.

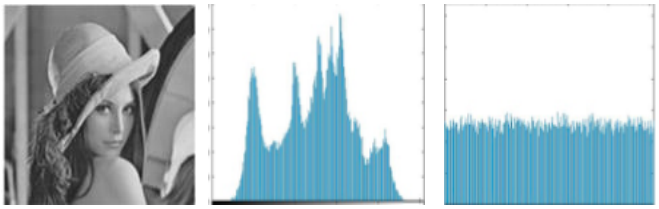
4.1 Key sensitive

A well-chosen method should be sensitive to any modification in the key, even if that change is only very little, because the key is the most important part of the equation. Consider the following scenario: after successfully encrypting a picture with the right key, we decide to alter it in any way, even by just one bit. The picture that was encrypted using the right key and the image that was encrypted using the changed key are indistinguishable from one another. To provide evidence that we encrypted Lena's picture using the appropriate key. The picture that was encrypted with the right key is displayed in Figure 3. We attempted to decode the picture by utilizing the original key as well as a modified version of the key. In the instance where the right key was used, the picture was effectively encrypted to the plain image again, as shown in Figure 3. On the other hand, when the plain image was changed, it was not possible to successfully decode the plain image, as shown in Figure 3.

Figure 3: Key Sensitive Analysis: Encrypted Image, Decrypted Image Using Correct Key, and Decrypted Image Using Modified Key

4.2 Histogram Analysis

The histogram has the ability to display the statistical aspect of the distribution of pixel values. The histogram of the encrypted picture must always be uniform for a system of encryption to be considered useful. The histogram plot depicts the distribution of an image's pixel count across its various intensity levels. It is important that an encrypted image have a consistent or balanced distribution of its pixel data in order to have effective encryption. For the sake of this investigation, Lena has been encrypted using both the traditional AES algorithm and the suggested approach. The histogram of the original Lena is shown in Figure 4(b), while the histogram of the suggested approach is shown in Figure 4(c). Figure 4(a) depicts the original Lena. The findings of the experiment reveal that the distributions of all of the histograms are identical, which is a significant departure from the initial Lena.



(a) (b) (c)

Figure 4: Histogram Analysis for Proposed Methodology

4.3 Entropy Analysis

Entropy is defined as the measure of unpredictability in image processing, and it may be understood as the average uncertainty of the information source. Entropy is measured in bits per second. The formula for calculating entropy is Equation (2).

$$H(x) = -\sum_{i=0}^{2^{N-1}} p(x_i) log\, p(x_i) \quad (2)$$

where the probability of the symbol *xi* is denoted by the variable *P(xi)*. Now, the number of grey levels for grayscale photos is either 256 or 28, and if the probability of grey levels is the same, then by using Equation (2), entropy must equal 8. Table 1 presents the entropy values for the three samples that were taken. The findings shown in Table 1 demonstrated that the entropy values for the approaches that we offered can effectively encrypt the image.

Table 1: Entropy Results of the proposed methodology

Image	Entropy (original image)	Entropy (proposed)
Lena	7.3712	7.9623
Peppers	7.3933	7.9902
Baboon	7.1394	7.8662
Cameraman	6.1087	7.8105

4.4 NPCR and UACI

Both the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are approaches that may be utilized to evaluate the resistance of encrypted data to a variety of differential assaults [20]. These are utilized to test how alterations of a minute nature made to the initial picture would impact encryption. These approaches compare the original picture data with the encrypted image data in order to determine the degree to which the two sets of data differ from one another. To achieve excellent encryption, there should be significant differences between the original picture and the encrypted image data. These differences should be able to withstand a variety of differential assaults. Calculating the UACI requires comparing the pixel values of two photos and estimating the average intensity of the differences that occur between the two images. It is a percentage that can vary anywhere from 0 to 100, with larger values suggesting a bigger disparity between the two pictures. It is given as a percentage. Before attempting to compute the UACI, it is necessary to first identify the disparities that exist between the pixel values of the two pictures. After that, these discrepancies are averaged, and the final result is stated as a percentage by dividing the average difference by the highest possible difference between the pixel values and then multiplying the result by 100. Calculations for an image's NPCR and UACI may be written as Equation (2) and Equation (3), respectively.

$$NPCR = \frac{1}{W \times \mathrm{H}} \sum_{i=1}^{W} \sum_{j=1}^{H} d_{ij} \times 100\% \quad (3)$$

$$UACI = \frac{1}{255 \times W \times \mathrm{H}} \sum_{i=1}^{W} \sum_{j=1}^{H} \left| C_{ij}^{1} - C_{ij}^{2} \right| \times 100\% \quad (4)$$

$$d_{ij} = \begin{cases} 0, & C_{ij}^{1} = C_{ij}^{2} \\ 1, & C_{ij}^{1} \neq C_{ij}^{2} \end{cases}$$

where *M* and *N* denote the width and height of the picture, respectively, and *c1* and *c2* are two cipher images that were created by altering the location of one pixel in their respective initial plain images.

Table 2: NPCR and UACI of the proposed methodology

Image	NPCR	UACI
Lena	99.4059	33.2492
Peppers	99.2248	33.1881
Baboon	99.2492	32.9805
Cameraman	99.32361	33.2903

5. Conclusion

The author of this research developed a novel method for encrypting images that operates in three stages. The first thing that we do is encrypt images using a technique called AES. This is the first step. We will go on to the next level once we have generated a random key by utilizing the Henon map. After that, we block pixels in the picture, and after that, we do an XOR operation between the result of the first step and a key that we produce. Numerous tests, such as key sensitivity, entropy, NPCR, and UACI, have been carried out as part of the process of validating our suggested methodology. The findings have demonstrated that our method has satisfactory performance when it comes to picture encryption.

References

1. Wu, J.; Liao, X.; Yang, B. Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. *Signal Process.* 2017, *141*, 109–124.
2. Amigo, J.M.; Kocarev, L.; Szczepanski, J. Theory and practice of chaotic cryptography. *Phys. Lett. A* 2007, *366*,211–216.
3. Jakimoski, G.; Kocarev, L. Chaos and cryptography: Block encryption ciphers based on chaotic maps. *IEEE Trans.Circuits Syst. I Fundam. Theory Appl.* 2001, *48*, 163–169.
4. Cao, C.; Sun, K.; Liu, W. A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. *SignalProcess.* 2018, *143*, 122–133.
5. Padate, R., & Patel, A. (2015). Image encryption and decryption using AES algorithm. *International Journal of Electronics and Communication Engineering & Technology*, 23-29.
6. Mellu, P., & Mali, S. (2011), AES: Asymmetric key cryptographic System II, International Journal of Information Technology and Knowledge Management, 4(1), 113-117.
7. Adi Shamir Ronald Rivest and Len Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21:120–126, 1978.
8. Zhang, Y.; Li, X.; Hou, W. A fast image encryption scheme based on AES. In Proceedings of the 2nd International Conference on Image, Vision and Computing (ICIVC), Chengdu, China, 2–4 June 2017; pp. 624–628.
9. Priya, S.; Santhi, B. A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images. *Mob. Netw. Appl.* 2021, *26*, 2501–2508.
10. Alsaffar, D. M., Almutiri, A. S., Alqahtani, B., Alamri, R. M., Alqahtani, H. F., Alqahtani, N. N., & Ali, A. A. (2020, March). Image encryption based on AES and RSA algorithms. In *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-5). IEEE.
11. Bahrami et al, 2013. "encryption of multimedia content in partial encryption scheme of DCT transform coeffiecent using a light weight stream algorithm," optik, Elsevier, pp. 3693-3700.
12. Singh, A., Agarwal, P., & Chand, M. (2019, April). Image encryption and analysis using dynamic AES. In *2019 5th international conference on optimization and applications (ICOA)* (pp. 1-6). IEEE.
13. Priynka Sharma, "A new image encryption using modified AES algorithm and its comparison with AES", international journal of engineering research of technology (IJERT), vol.9, no. 8, august 2020.
14. Abhinav Gupta1 and Aayush Gupta, "A New Technique of Image Encryption using Modified AES Algorithm", International Journal of Multidisciplinary Innovative Research. ISSN: 2583-0228 vol. 1, no.1, pp. 34-43, Jul' 2021.
15. Sarah Jassim and Sarab M. Hameed, "A Modified Advanced Encryption Standard for Color Images", Iraqi Journal of Science, vol. 63, no. 1, pp. 294-312, 2022.
16. Moumen, A., & Sissaoui, H. (2017). Images encryption method using steganographic LSB method, AES and RSA algorithm. *Nonlinear Engineering*, *6*(1), 53-59.
17. M. He´non, "A two-dimensional mapping with a strange attrac- tor," *Communications in Mathematical Physics*, vol. 50, no. 1, pp. 69–77, 1976.
18. E. Lorenz, "Deterministic nonperiodic flow," *Journal of Atmo- spheric Sciences*, vol. 20, no. 2, pp. 130–141, 1963.
19. Tamimi, A. A., & Abdalla, A. M. (2015). An image encryption algorithm with XOR and S-box. In *Proceedings of the International Conference on Image Processing, Computer Vision, and Pattern Recognition (IPCV)* (p. 166). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
20. C. Unal, K. Sezgin, P. Ihsan and Z. Ahmet, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons and Fractals*, vol. 95, pp. 92-101, 2017.