International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Facial Image Encryption & Compression for Secure Image Transmission on Cloud Storage

[1]Pranali Dahiwal, [2]Anagha Kulkarni

Submitted: 24/09/2023 **Revised**: 16/11/2023 **Accepted**: 26/11/2023

Abstract: Image transmission and face image recognition have grown quite popular among cloud computing users in today's world via different mobile devices. However, because the data is personal, the privacy and security of such data are critical while using the cloud platform. Security features must be used while transmitting images through the cloud. picture encryption is a form of such secure picture communication technology. However, because picture transmission is commonly utilized for face image identification for authentication purposes, the transmission time is critical. In this study, we solve this issue by encrypting images using the Advanced Encryption Standards (AES) and the XOR technique. We propose utilizing the XOR encryption technique to encrypt segmented images. We conducted picture transmission experiments employing 3*1,3*2 and 3*3 images that were segmented with an encryption method and discovered that our suggested XOR-based image segmentation surpassed the existing AES approach in terms of time complexity.

Keywords: *Image Segmentation, Image Encryption, AES, XOR, Authentication, Privacy, Security*

1. Introduction

Cloud computing has emerged as a viable technique for on-demand computing and storage resources. Cloud computing removes the need to install sophisticated software and expensive hardware. The cloud enables customers to maintain their services highly accessible at a cheap cost: they simply need to sequester their information in the cloud and pay for the precise quantity of needed storage; users may then access this data whenever and wherever they choose. Because the cloud-based system is public, it requires a robust authentication technique. A textual password is the most often used authentication technique. Dictionary assaults, attacks by insiders decreasing, and the use of social engineering are all well-known downsides of this method. Some techniques focused on creating a random and long password can help to safeguard the system. The biggest issue, though, is the hustle and bustle of remembering such passwords. On the other hand, several studies have found that legitimate users prefer short, easy-to-remember passwords. Unfortunately, these passwords were subjected to online/off-guessing assaults. Other methods include passwords that appear on screens and biometrics. Furthermore, these two systems have other drawbacks, such as finger prints, DNA, and face recognition, which need additional hardware/software.[1]

Nowadays, cloud-based systems and other devices such as personal computers (PCs) are used. Image-based authentication is also being used on mobile phones, which is beginning to gain popularity among consumers. The picture is stored locally for authentication reasons and does not cause any difficulties with image authentication. The passing on of digital photographs through the cloud poses security and privacy issues. Image digitalization, on the other hand, becomes extremely vulnerable to malicious assaults via cloud computing. Users often change the data that is stored in the cloud, necessitating authorization each time they log in. One of the biggest issues is the user's authority. [2][3].

Image encryption methods can help with image authentication. Image encryption is being used in communication via the internet, imaging applications, database management systems, digital media systems, telemedicine, and other fields. To protect the integrity of digital pictures has recently received more attention, and numerous image encryption algorithms have been proposed to improve image transmission security. . Image encryption techniques seek to create a new digital file that is difficult to identify. Additionally,

[1]*Savitribai Phule Pune University, Pune, India*
[2]*Cummins College of Engineering for Women, Pune, India Corresponding author email: pranali.dahiwal@viit.ac.in anagha.kulkarni@cumminscollege.in*

image decryption recovers the original picture from the encoded image. The picture encryption approach provides benefits over text password for authentication, but it has the disadvantage of being more time consuming than textual password authentication. [4][5].

Taking both of these concerns into account, our suggested approach results in the development of an image encoder for password authentication utilizing XOR and AES encryption, which can be used for cloud verification with minimal execution time. For picture authentication, we employed 3*3,6*6 and 9*9 grid segmentation approaches and evaluated our system using 3*3,6*6 and 9*9 grid segmentation. The primary contribution of this study is the development of a unique approach to picture authentication based on segmentation and sophisticated XOR encryption algorithms. The work is focused on the encryption as well as the decryption time complexity, and it is discovered that the time required for picture encryption was relatively short.

The following is an outline of our paper. The review of literature is included in Section 2. Section 3 focuses on the approaches employed in the proposed endeavour. Section 4 describes the outcomes of our suggested system. Finally, Section 5 alludes to the paper's conclusion.

2. Related Work

The use of encryption is a widely used technique and practice in digital information security systems. Encryption technology works by encoding the original data. The privacy and confidentiality of information stored on the internet can be safeguarded if the encryption technology is secure and reliable enough.[6][7][8][9]. As a result, digital picture encryption technology and techniques study is an essential direction for digital photo security protection.

In paper [9], Based on a 2D-CIMM chaotic map, an image encryption technique with greater security uses the hash values of the original picture to update its starting value in real time. Furthermore, the encryption process's permutation and diffusion are all conducted at the bit level to improve method security. This approach has a coefficient of correlation between neighbouring pixels that is near to zero, as well as random and homogeneous statistical properties in the encrypted picture, and it is resistant to differential assaults and known/chosen plaintext attacks.

Sura F. Yousif, Ali J. Abboud, and Hussein Y. Radhi developed an image security technique that uses a scanning system, the El-Gamal asymmetric key cryptosystem, and chaotic systems to protect digital pictures. For the resulting permuted images, the Lorenz chaotic system is used to confuse the relationship between the gray pixels of the image by adjusting the position of them, while the Rössler chaotic system is used to diffuse the image pixels by differing their color values in order to achieve an additional layer of encryption. This technique is successful against statistical, different, and exhaustive assaults, and it is resistant to the majority of common attacks. [10].

A method of encrypting images [11] on the basis of a chaotic normal map and bit-level permutation, the algorithm not only alters the positions of picture pixels but also their values to increase randomization. The bit-level recombination features enable bit-level ambiguity and dependent dispersion to improve the cryptosystem's security. The text of the article [12] provides a bit-level randomization and dynamic overlap diffusion-based picture encryption and decryption technique. To begin, the simple picture has been distorted at the bit level, shifting the pixel location while altering the value of each pixel using an algorithmic Arnold transform to produce the permutation image. The permutation picture is then subjected to dynamic overlap diffusion in accordance with the encryption security criteria. Simultaneously, the real-world information entropy and variance are employed to update the diffusion key in five-dimensional hyper-chaotic networks to accomplish encryption key plaintext correlation. When encrypting various pictures, Arnold transformations and adaptive overlap diffusion are employed to ensure that alternative key streams are created. As a result, known-plaintext and chosen-plaintext assaults cannot be used to crack this method. When doing research [13], A One-Dimensional Chaotic System (1DSCS) with good chaotic properties and a wide parameter space is proposed, and an image encryption strategy is explored and tested on its basis. This 1DSCS is employed in the generation of chaotic sequences. Images are encrypted using a hybrid scrambling approach and a dynamic dilution method based on 1DSCS. This method provides strong encryption and can withstand typical assaults. An image encryption technique must be vulnerable to cryptanalysis attacks such as chosen-plaintext assaults, chosen-cipher-text attacks, and so on. The article[14] provided an effective approach for creating safe dynamic S-boxes derived by means of the Henon map. The dynamic S-box is used to build an image encryption system with a variety of security measures to prevent chosen-plaintext and chosen-

cipher-text assaults. In addition, Elliptic Curve Cryptography (ECC) is used to safeguard the encryption keys against cryptanalysis. As a result, even in the unusual situation of recovering a short-lived S box or key-stream, recovering secret keys is as difficult as solving the elliptic curve discontinuous logarithm issue.

The article [15] has presented a dynamic spiral scrambling method in conjunction with the randomized pixel value filling operation and the Deoxyribonucleic Acid (DNA) operation for picture encryption. The dynamic spirals scrambling method scrambles the pixels that are part of the plaintext picture by dynamically combining chaotic sequences with them. The crambling method is no longer fixed as a result of this process, and location changes are extremely sensitive to chaotic sequences; any minor change yields a radically different outcome. The output is then combined with the DNA encoding and tweaked to further perplex pixel values. This technique provides strong encryption and can withstand typical assaults such as choose plaintext assaults, cropping, and noise attacks.

The document [16], when compared to previous 2D maps in the literature, has proposed a second order two-Dimensional (2D) mapping with exceptionally complicated chaotic behaviour and unique big positive Lyapunov exponent over a wide variety of parameters. And, a new reliable secure, image encryption scheme combining the associated chaotic pseudo-orbits of the fractional order 2D map with the advantages of elliptic curves in public key cryptography is suggested and applied to colour images. This hybrid system may validate trustworthy secret key exchange as well as very obscure and concealed sent data packets.

The paper [17] suggested a colour picture encryption technique made up of a double-chaos network and bit-level DNA computing. This approach scrambles the three shaded elements of the plaintext picture using the Arnold algorithm, and the number of repetitions is decided by the pixel mean of each part, which increases the scrambling impact of the Arnold algorithm. Then, three sets of chaotic sequences were constructed for the diffusion operation of three scrambled components utilizing the modified double-chaos system constituted of Lorenz catastrophic mapping with variables, parameters, and fourth-order Rossler hyper-chaotic mapping. Then, using the process of DNA coding and DNA computing, the three groups of pictures are diffused, and lastly, the three sets of cypher-text components are combined to produce the final cypher-text image.

In the document [18] a colour picture compression encryption technique based on a Back Propagation (BP) neural network and a fractional-order hyper-chaotic system has been suggested. The dynamical properties of a fractional-order hyper-chaotic entity exhibit a wide parameter range and excellent unpredictability. As a result, a fractional-order structure is more suited for picture encryption methods. The picture may be effectively compressed by using a BP neural network. As a result, our picture compression and encryption technique is useful for the secure transfer of image data in practical communication applications.

In [19] the authors offer a Modified AES-Based Image Encryption Algorithm. Encryption is the most often used technology for picture security. Image and video have several uses, including internet communication, multimedia systems, medical imaging, telemedicine, and military communication. Image protection methods in the form of vector quantization are available. There are many vector quantization methods in which the picture is divided into vectors and the encoding and decoding operations are done vector by vector or by splitting the image into suitable shapes and creating a huge number of shadow that ensure the image is invisible to unlawful users. In [20] The authors provide AES-based safe picture encryption. Security is the most important concern in today's globe. The transmission of pictures for communication has expanded, and protecting data from illegal access is a key concern. It is tough to offer security to a person. There are several approaches for preventing unauthorized individuals from accessing data. AES is used for picture encryption and decryption, where the image is changed into a form that cannot be recognized by the key and then transformed back to the original format by an authorized receiver. In [21] The authors demonstrate AES-based picture encryption and decryption. The AES method for the encryption and decryption of data is used in the construction of good security for picture transmission. AES has surpassed its predecessor, the Data Encryption Standard (DES) in terms of security. AES key expansion employs a 128-bit key for encryption, employing bitwise exclusive or image set pixel operations. In [22] the authors provide Image Encryption using AES Key Expansion. The picture has unique properties such as a high rate of data transfer with restricted bandwidth, redundancy, bulk capacity, and pixel correlation. These are the qualities

that must be considered while encrypting a picture. As a result, the AES method is utilized with key expansion, and the process of encrypting is carried out by employing bit-wise exclusive or function of the picture pixels set in conjunction with a 128-bit key. The key is produced on both the transmitter and recipient sides using the AES Key Extension algorithm.

3. Methodologies

This section explains the different picture encryption and compression algorithms employed in this research effort for the use of the facial recognition system. First, the original picture was split into several grid combinations, and then we used encryption techniques such as Advanced Encryption Standards (AES), XOR.

3.1 AES Encryption and Decryption Operations:

AES is an incremental cipher, not a Feistel cipher. It is built on a 'substitution-permutation network'. It is made up of a sequence of connected tasks, some of which require substituting inputs with particular outputs (substitutions) and some of which entail rearranging bits (permutations).

Surprisingly, AES does all of its calculations on bytes and not on bits. As a result, AES considers a plaintext block's 128 bits as 16 bytes. These 16 bytes are organized into four columns and four rows, which are needed for matrix processing.

In contrast to DES, the number of rounds in AES is flexible and is determined by the length of the key. AES employs ten rounds of encryption for 128-bit keys, twelve rounds for 192-bit keys, and fourteen rounds for the 256-bit keys. Each of these encryption rounds use a unique 128-bit round key derived from the beginning of the AES key.

The AES architecture is depicted schematically in the following figure 1–

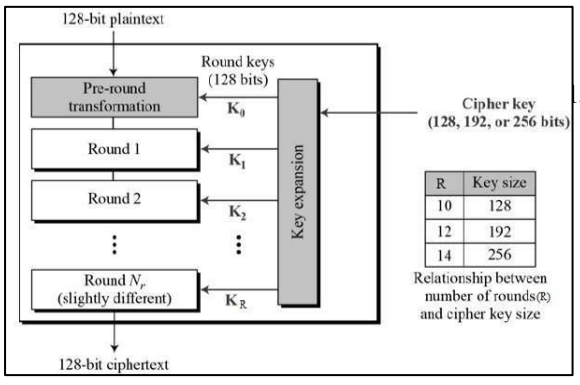

Fig 1: Architecture of Advanced Encryption Standards

3.2 Encryption Process

Here, we limit ourselves to describing a typical round of AES-256-bit encryption. Each cycle is divided into four sub-processes. The first round of the procedure is shown below in figure 2.

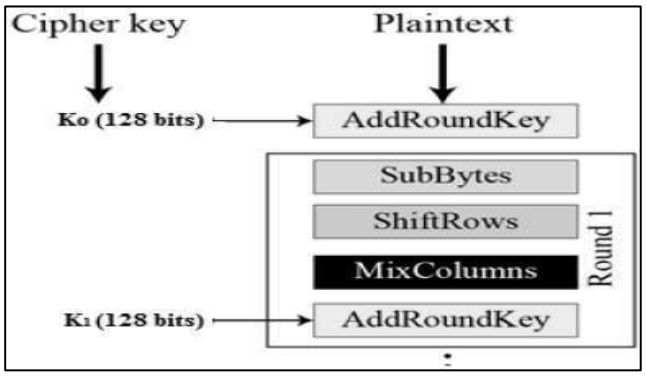

Fig 2 : AES-256-bit encryption

3.1.1.1 Byte Substitution (Sub Bytes)

The 16 input bits are replaced by searching a fixed table (S-box) provided in the design. The end result is a matrix with a total of four rows and four columns.

3.1.1.2 Shift rows

Each of the matrix's four rows is moved to the left. Any entries that 'fall off' are returned on the row's right side. The following is how the shift is carried out: −

- The first row has not been moved.
- The second row is moved one (byte) to the left.
- The third row has been moved two spaces to the left.
- The fourth row has been moved three spaces to the left.
- As a consequence, a new matrix with a total of 16 bytes but moved in relation to each other is created.

3.3 Mix-Columns

Each four-byte column is now changed using a unique mathematical formula. This method takes four bytes from one column as input and returns four fully new bytes that replace the original data in that column. As a consequence, a new matrix with 16 additional bytes is created. It should be pointed out that this phase was not completed in the previous round.

3.1.1.4 Add-round-key

The matrix's 16 bytes are now regarded as one hundred eighty-eight bits and are XORed with the round key's 128 bits. If this is going to be the final round, the output will be the cipher text. Otherwise, the resultant 128 bits are decoded as 16 bytes, and we repeat the process.

3.1.2 Decryption Process

The technique of decrypting an AES cipher text is identical to the process of encryption in reverse order. Each cycle consists of four procedures performed in reverse order. −

- Include a circular key.
- Mix columns
- Shift rows
- Byte substitution

Because the sub-processes in each stage are reversed, unlike in a Feistel Cipher, each of the algorithms for encryption and decryption must be implemented individually, although being extremely closely linked.

3.2 XOR Encryption and Decryption

As a key element in increasingly sophisticated cyphers, the XOR operators is quite prevalent. A basic XOR cipher can be easily cracked using frequency analysis when employing a constant repeating key. The key can be exposed if the contents of any communication is likely to be guessed or else known. Its main advantage is that it is easy to carry out and that the combination of two values is relatively cheap. In circumstances when no special security is required, a basic repeating XOR (i.e. utilizing the same key per XOR operations on the whole data) cipher is occasionally used to hide information. With the goal of making reverse engineering more difficult, the XOR cypher is frequently employed in computer virus.

The XOR encryption is a basic yet effective cryptographic mechanism for data security. In its most basic version, only a secret key is required to accomplish decryption as well as encryption using the bit-wise exclusive OR operation, which is sometimes indicated by a circle plus, ⊕.

To encrypt, just XOR a plain-text message M with the secret key K, resulting in MK = E. We just XOR the message that is encrypted with E using the same key, EK = M, to decode it. This indicates that the same action (or software, in our instance) has the ability to encipher and decipher (or encrypted and decrypt).

If a fixed-length key is shorter than the message and is used frequently to encrypt pieces of the message, subsequently a technique known as frequency analysis could be employed to break the encryption of text messages (similar to how you or your parents might have broken cryptogram problems in the publication, which rely on the fact that certain letters and mixtures appear more frequently than others).

If the encryption key is as lengthy as the information, the only method to decrypt it is to test every conceivable key. In fact, this is sometimes referred to as a brute-force assault, and it is unlikely since an N-bit secret has 2N possibilities. Exchanging a long key in a secure manner is just as challenging as exchanging a long message. Furthermore, even the usage of a lengthy key for numerous messages is vulnerable to frequency-based attacks. One solution to these issues is to produce an unexpected but repeatable stream of keys using a so-called pseudo-Random Number Generator (RNG). Then, if you and your partner have access to the same generator, just the (far shorter) starting seed for that generator has to be communicated. Each message block is then turned into an encryption using the generator's following keys.

4. Results And Discussion:

The findings were obtained by segmenting the picture into different matrices such as 3*1,3*2, and 3*3, implying that the image was segmented into 3,6, and 9 segments. Following segmentation, pictures are encrypted using a combination of the XOR and AES algorithms, as explained in section 3. All measurements were obtained on the single core of an Intel Core i5 Central Processing Unit (CPU) running at 2600 MHz with 8 GB RAM, and tests were run in the NETBEANS 8.2 IDE using Java as the programming language.

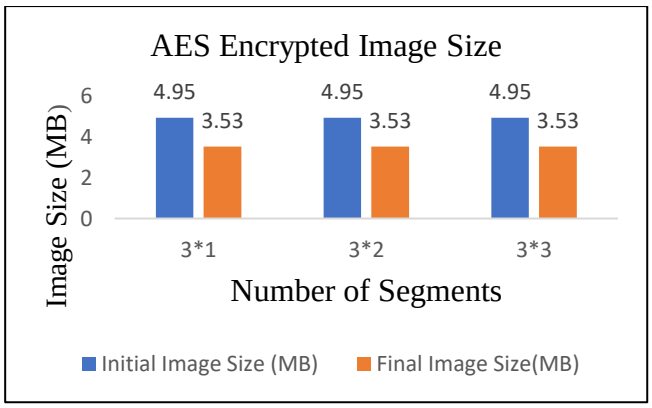

Fig 3: Encrypted Image Size Comparison

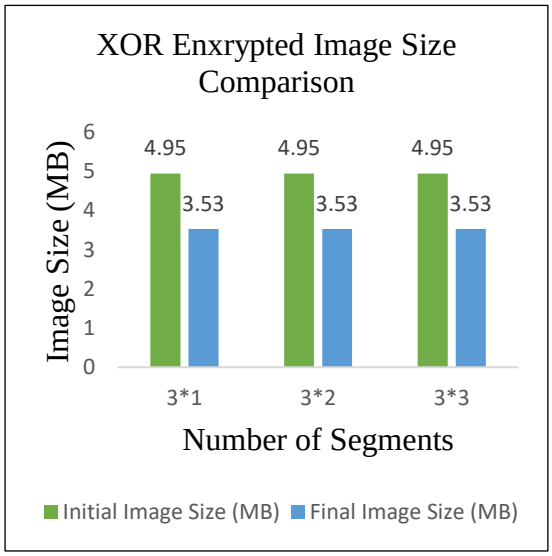

Fig 4:XOR Encrypted Image Size Comparison

Figure 3 and figure 4 demonstrate that the initial file is encrypted using AES and XOR operations with 3*1,3*2,3*3 segmentation, and the encrypted file size is smaller than the original size. Furthermore, the password-protected file size in the case of the XOR and AES encoders is the same.

In all three segment matrices the XOR image encryption process takes less time to encrypt the picture than the AES scheme. The most crucial element in our performance investigation is the time difficulty for secure picture authentication on the

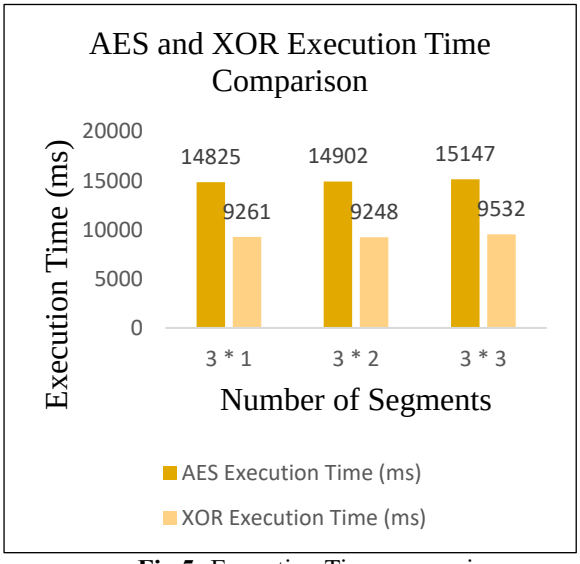

Fig 5: Execution Time comparison

cloud. In this regard, XOR outperforms AES encryption significantly and is 63-68% quicker. Figure 5 shows that the XOR image encryption time ranges from 9261 ms to 9532 ms as compared to 14825 ms to 15147 ms for different types of image segmentation techniques. The suggested XOR technique with picture segmentation has been shown to be much quicker than the current AES approach. The recommendation for the algorithm is 1.5 times faster than the existing algorithm. The suggested approach has been demonstrated to be effective in picture transmission.

5. Conclusion:

The proposed approach presents a strong compression, encryption, and picture segmentation approaches for safe image transmission. The picture encryption algorithms AES and XOR have been compared for this purpose. The photos were divided into 3*1,3*2 and 3*3 matrix before the encryption algorithms were performed. In terms of temporal complexity, the suggested XOR with picture segmentation encryption scheme outperforms the existing AES solutions. The current AES approach is 1.5 times slower than the suggested XOR image segmentation techniques. This suggested technology will be used in the future for picture transmission and authentication through cloud storage.

References:

[1] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan. 2011, doi: 10.1016/J.JNCA.2010.07.006.

[2] J. Katz and M. Yung, “Scalable protocols for authenticated group key exchange,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2729, pp. 110–125, 2003, doi: 10.1007/978-3-540-45146-4_7/COVER.

[3] Y.-J. Yang, J. Weng, and F. Bao, “On the Limits of Anonymous Password Authentication,” Sep. 2023.

[4] R. Kaur, “Image Encryption Techniques:A Selected Review,” *IOSR J. Comput. Eng.*, vol. 9, pp. 80–83, Jan. 2013, doi: 10.9790/0661-0968083.

[5] Z. Oleiwi, W. Abdallah, W. Alisawi, A. Alfoudi, and L. Al-Farhani, *Overview and Performance Analysis of Encryption Algorithms*. 2020.

[6] U. 4b2, “Digital information infrastructure and method for security designated data and with granular data stores,” Apr. 2009.

[7] Z. Han, S. Huang, H. Li, and N. Ren, “Risk assessment of digital library information security: A case study,” *Electron. Libr.*, vol. 34, pp. 471–487, Jun. 2016, doi: 10.1108/EL-09-2014-0158.

[8] C. Zhou, Y. Guo, W. Huang, H. Jiang, B. Li, and J. Chen, "Information security defense method of electric power control system based on digital watermark," no. Icmemtc, pp. 174–179, 2016, doi: 10.2991/icmemtc-16.2016.32.

[9] E. Chisanga and E. K. Ngassam, "Towards a conceptual framework for information security digital divide," *2017 IST-Africa Week Conf. IST-Africa 2017*, Nov. 2017, doi: 10.23919/ISTAFRICA.2017.8102398.

[10] S. F. Yousif, A. J. Abboud, and H. Y. Radhi, "Robust Image Encryption with Scanning Technology, the El-Gamal Algorithm and Chaos Theory," *IEEE Access*, vol. 8, pp. 155184–155209, 2020, doi: 10.1109/ACCESS.2020.3019216.

[11] A. Gamal, N. Korany, and S. El-Khamy, "New DNA Coded Fuzzy Based (DNAFZ) S-Boxes: Application to Robust Image Encryption Using Hyper Chaotic Maps," *IEEE Access*, vol. 9, pp. 14284–14305, Jan. 2021, doi: 10.1109/ACCESS.2021.3052161.

[12] J. Wang, J. Li, X. Di, J. Zhou, and Z. Man, "Image Encryption Algorithm Based on Bit-Level Permutation and Dynamic Overlap Diffusion," *IEEE Access*, vol. PP, p. 1, Aug. 2020, doi: 10.1109/ACCESS.2020.3020187.

[13] X. Wang and P. Liu, "A New Image Encryption Scheme Based on a Novel One-Dimensional Chaotic System," *IEEE Access*, vol. 8, pp. 174463–174479, Jan. 2020, doi: 10.1109/ACCESS.2020.3024869.

[14] I. Saleh and A. Alharbi, "Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography," *IEEE Access*, vol. 8, pp. 194289–194302, Jan. 2020, doi: 10.1109/ACCESS.2020.3032403.

[15] X. Wang and S. Chen, "Chaotic Image Encryption Algorithm Based on Dynamic Spiral Scrambling Transform and Deoxyribonucleic Acid Encoding Operation," *IEEE Access*, vol. PP, p. 1, Sep. 2020, doi: 10.1109/ACCESS.2020.3020835.

[16] A. Alkhedhairi, A. Sonbaty, A. Elsadany, and E. Hagras, "Hybrid Cryptosystem Based on Pseudo Chaos of Novel Fractional Order Map and Elliptic Curves," *IEEE Access*, vol. PP, p. 1, Mar. 2020, doi: 10.1109/ACCESS.2020.2982567.

[17] Q. Liu and L. Liu, "Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System," *IEEE Access*, vol. PP, p. 1, Apr. 2020, doi: 10.1109/ACCESS.2020.2991420.

[18] F. Yang, J. Mou, Y. Cao, and R. Chu, "An Image Encryption Algorithm Based on BP Neural Network and Hyperchaotic System," *China Commun.*, vol. 17, no. 5, pp. 21–28, May 2020, doi: 10.23919/JCC.2020.05.003.

[19] A. Hadj Brahim, A. Ali Pacha, and N. Hadj Said, "An image encryption scheme based on a modified AES algorithm by using a variable S-box," *J. Opt.*, pp. 1–16, May 2023, doi: 10.1007/S12596-023-01232-8/METRICS.

[20] P. Shete and S. Kohle, "Image Encryption using AES Algorithm: Study and Evaluation," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 9, pp. 1134–1137, Sep. 2022, doi: 10.22214/IJRASET.2022.46619. paavni gaur, *AES Image Encryption*. 2021. doi: 10.21203/rs.3.rs-1179585/v1.

[21] J. Amador and R. Green, "Symmetric-key block cipher for image and text cryptography," *Int. J. Imaging Syst. Technol.*, vol. 15, pp. 178–188, Jan. 2005, doi: 10.1002/ima.20050.