MJFAS
Malaysian Journal of Fundamental and Applied Sciences

Salman *et al.* | Malaysian Journal of Fundamental and Applied Sciences, Vol. 19 (2023) 355-361

RESEARCH ARTICLE

Random Color Image Encryption Using the Genetic Algorithm

Hanan Abbas Salman*, Duha Amer Mahdi

Department of Computer System Techniques, Technical Institute of Najaf, Al-Furat Al-Awsat Technical University, Najaf, Iraq

Abstract This paper implements a combined pseudo-random sequence generator based on neural networks and chaotic, random variable color images based on an algorithm for chaotic encryption, secure image storage, and transmission. The generator that controls the operation of the encryption algorithm: the arrangement of pixel positions, the use of random color images of the AES algorithm to achieve encryption, creation algorithms, and neural networks by dynamically updating control parameters and numbers to increase the generated chaotic sequence randomness by using simulation MATLAB for getting output. The chaotic function's iteration of the neural networks. The experimental results are presented in the form of a pixel correlation coefficient and security analysis to prove the security and effectiveness of the proposed chaos-based ANN encryption.

Keywords: Cryptography, encryption, decryption, random key, genetic algorithm.

Introduction

Cryptography is the science of studying how to protect privacy. The cryptographic system used to protect data relies on the existence of an ample solution space to prevent attacks. In fact, when designing a cryptographic system, the critical point is that the underlying algorithm uses all possible possibilities of the algorithm to encrypt the target data to prevent attempts to crack it with so-called brute force attacks [1, 2].

Because of the headway of network and multimedia coding technology, multimedia data, for example, images, are regularly put away and sent utilizing the Internet and are defenseless against malicious use [3, 4]. In this manner, image encryption and security have become a well-informed region to guarantee protection and prevent unauthorized digital content access [5, 6]. However, the Advanced Encryption Standard (AES) [1, 7], its Traditional symmetric encryption, is designed with propagation characteristics and good confusion. Be that as it may, standard encryption strategies, for example, AES, do not appear to be reasonable for encrypting information, for example, images.

The suggested approach encrypts images utilizing essential substitution and transposition operations and algorithms to provide a high level of security for both encryption and decryption solutions for random images. The proposed approach will employ a proportionately big secret key (Represented with a hexadecimal number system) in the form of a byte matrix of size (16 × 16). This key was used for replacement operations and transposition and provides propagation characteristics with good obfuscation in an encrypted form [8-11].

Several literary studies have shown that the bias module's security level is deficient. In image encryption, if the histogram of the composite image does not change, it is sometimes invalid for statistical attacks. To further develop the encryption process and the confusion shortcoming, this paper's proposed method is a bit-level replacement dependent on the diffusion effect of the particular confusion [12].

***For correspondence:**
hananabbas@atu.edu.iq

Received: 25 Nov. 2022
Accepted: 11 April 2023

10.11113/mjfas.v19n3.2907

With the Basing on the inactive obfuscation and diffusion module, based on the original image's replacement and transposition. This process will be performed multiple times according to the size of the private key: the original image is divided into (16 x 16) pixel-sized blocks [13-15].

Materials and Methods

The proposed method for image encryption brings forth a highly secure and efficient solution that utilizes the principles of transposition and substitution operations and algorithms. To achieve this, a substantial secret key is employed in the form of a byte matrix measuring (16 × 16), expressed in the hexadecimal number system. This key acts as the backbone of the encryption process, providing a solid layer of obfuscation and security to the encrypted image. One of the main challenges in image encryption is the tendency for histograms to remain unchanged, thereby making the encrypted image susceptible to statistical attacks. To overcome this weakness, the paper introduces a novel approach of a bit-level replacement technique based on a specific confusion diffusion effect. The proposed method further improves the confusion aspect of the encryption process, ensuring that the encrypted image is secure and highly diffuse. The encryption process starts with the transposition and substitution of the original image, which is then repeated multiple times based on the size of the private key. Finally, the original image is split into blocks of (16 x 16) pixels, and the encryption phase is executed through a well-structured architecture, as depicted in Figure 1. The proposed approach guarantees a high level of security and offers a robust and efficient solution for image encryption and decryption.

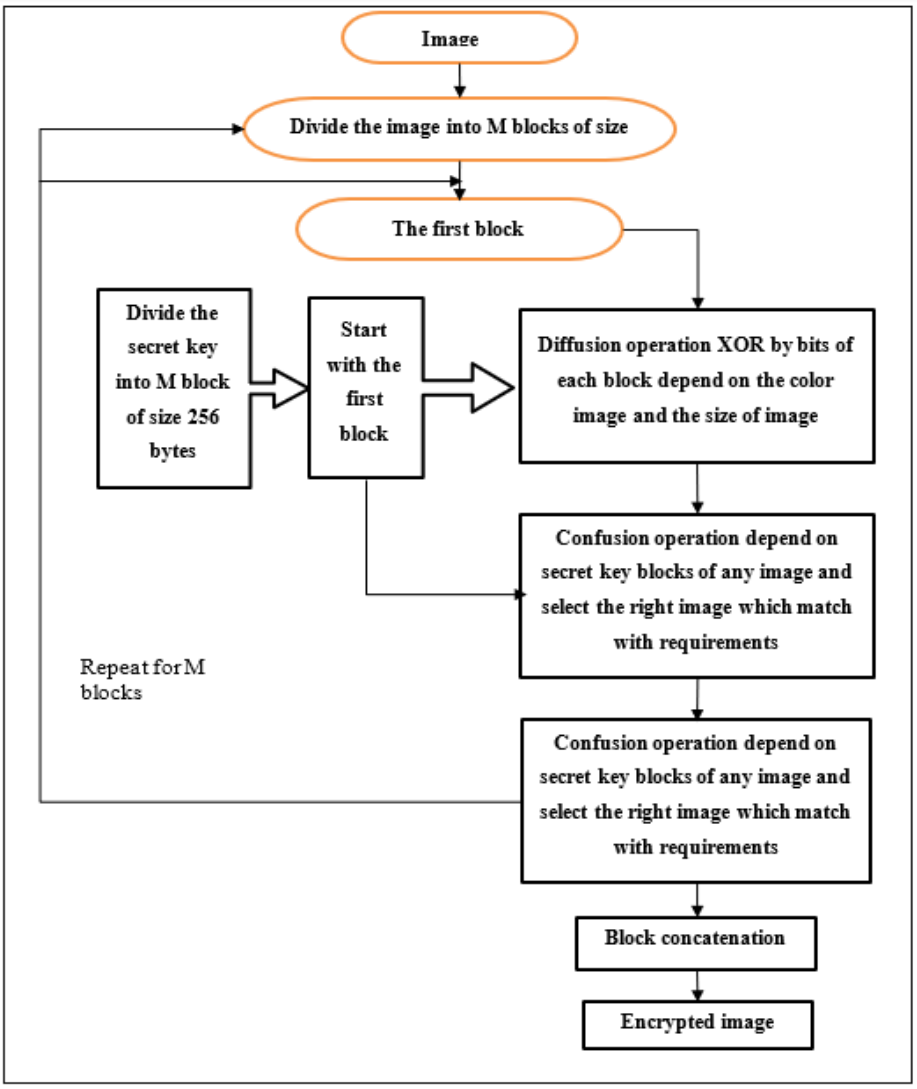

Figure 1. The design and approach of the suggested encryption process

The system design initially determines image input in this way. Then, the recommended method encrypts images using fundamental interpretation and replacement operation, as well as algorithms, to give a high-security encryption and decryption solution for random images. The proposed method will utilize a proportionately big secret key (Represented in the system of hexadecimal numbers) as a byte matrix of size (16 × 16). This key is utilized for substitution operations and transposition and gives great obscurity and propagation attributes in an encrypted structure.

As some writing studies have shown, the security level of the bias module is shallow. Moreover, in image encryption, if the histogram of the composite image does not transform, it is sometimes invalid for statistical attacks. To further develop the encryption process and confusion shortcomings, this paper proposes a bit-level substitution technique dependent on the impact of confusion diffusion. Based on the inactive obfuscation and diffusion module, because of the transposition and substitution of the first image. This process will be performed multiple times as indicated by the size of the private key: the original image is divided into (16 x 16) pixel-sized blocks.

To represent the methodology of the proposed algorithm, the terminologies and following definitions that we proposed:

Key length (length): the bytes of the number of the key image.

Secret Key (SK): bytes series might address a digital file like text, sound, image, etc. The secret key generation is too important to treat data encryption security. Moreover, the key's length must be as considerable as possible, and there are as many random bytes as possible.

Encryption Algorithm

Step 1: Retrieve the name of the key, referred to as SK, and its length, referred to as SK-L.

Step 2: Acquire the unique image S and determine its length, referred to as S length.

Step 3: In this step, the Original Image (OI) is split into "m" blocks of size (16 x 16), referred to as BN. The calculation for the number of blocks, M, is determined as follows: M = S length / (16 x 16), with the set of blocks being represented as BN (0) to BN (m-1).

Step 4: Initialize the value of Kind ex as 0.

Step 5: For each data block, BN, from Block = 0 to m-1, follow the below steps:
(a) Sequentially retrieve 256 bytes from the SK and set it as KB (i.e., SK(SKIndex) to SK(SKIndex+256)). If SKIndex equals SK-L (end of the SK), reset SKIndex to 0 (start of the SK).
(Block) For each element in the data block, from BN (Block, 0, 0) to BN (Block, F, F), do the following:
*) Create a block matrix of elements.
*) Perform a XOR (⊕) operation on the diffusion_substitution_process based on the bytes in BN (Block) and the series of elements in the element matrix.

For example, if the value of BN (Block, 0, 0) is 6E, the following occurs:

$$BN\ (Block, 0, 0) = BN\ (Block, 0, 0) \oplus KB\ (0,0)$$
$$BN\ (Block, 0, 0) = BN\ (Block, 0, 0) \oplus KB\ (B, 9)$$
$$BN\ (Block, 0, 0) = BN\ (Block, 0, 0) \oplus KB\ (0,7)$$
$$BN\ (Block, 0, 0) = BN\ (Block, 0, 0) \oplus KB\ (7,1)$$
$$BN\ (Block, 0, 0) = BN\ (Block, 0, 0) \oplus KB\ (F, 3)$$

*) The confusion process is accomplished by replacing the focal bytes in BN (Block) based on the series of elements in the following component matrix. For example, the value of BN (Block, 0, 0) is replaced with the values of BN (Block, B, 9), BN (Block, 0, 7), BN (Block, 7, 1), and BN (Block, F, 3).

Step 6: An encrypted image (EI) is generated from the encrypted data blocks.

Decryption Algorithm

Step 1: Retrieve the length of the secret key SK from storage.

Step 2: Acquire the encrypted image EI with its length from the user.

Step 3: Encrypted image EI as m blocks with size (16x16). Calculate M = Length / (16x16), and the set of blocks is named BN (0) ... BN (m-1).

10.11113/mjfas.v19n3.2907

Step 4: Set SKIndex to 0.

Step 5: For each data block BN from Block, repeat the subsequent actions:
*) Read 256 bytes from the SK in series and label them as KB (SK (SKIndex) ... SK (SKIndex + 256)). If SKIndex equals the length of the SK, reset SKIndex to 0 to go back to the starting of the SK.
*) For every element in the blocks of the data from BN (Block, 0, 0) to BN (Block, F, F),
(a) Create a Matrix of Next Element Block
(Block) Perform a diffusion_process by replacing the focal bytes in the BN (Block) according to the matrix's series of elements in the Following element.
(c) Perform XORing on the BN (Block) focal bytes established on the series of elements in the Next Element matrix.

Step 6: Build the OI from the decrypted set of the blocks of the data.

Visualization and analysis

The encryption and decryption methods were written in MATLAB and tested. The tests are implemented using pictures of varying sizes and 256 colors used in the experiments. Different pictures were used to assess the encryption and decryption procedures on the photographs. Images, as well as a variety of hidden keys, have been used. The outcome analysis is as follows:
The investigation was implemented for four distinct samples of pictures and four distinct secrets. The visual assessment of the histogram is critical in evaluating the findings—standard assessment of the picture and standard evaluation utilizing standard measurements [16, 17].
The results were obtained by experimenting with the four pictures of varying sizes of type (.bmp), as indicated in Figure 2.

Lena (128×128) Baboon (128×128) Pepper (128×95) Balloon (128×128)

Figure 2. Image samples

Figures 2, 3, 4, and 5 show the histogram results of an encrypted sample picture created using the suggested method.

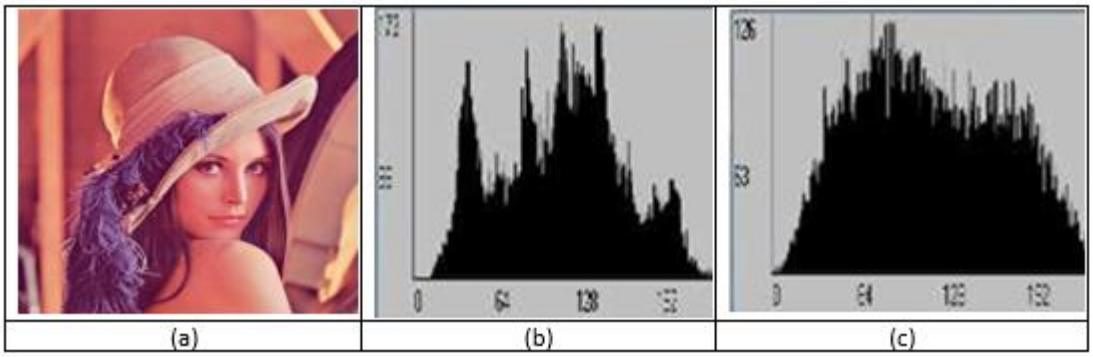

Figure 3. Histogram results (a) Lena image (Block) Original image histogram (c) Encrypted image histogram

Despite the Lena image being packed with a wealth of information, it has been thoroughly encrypted, causing much of its original form to be transformed through processing.

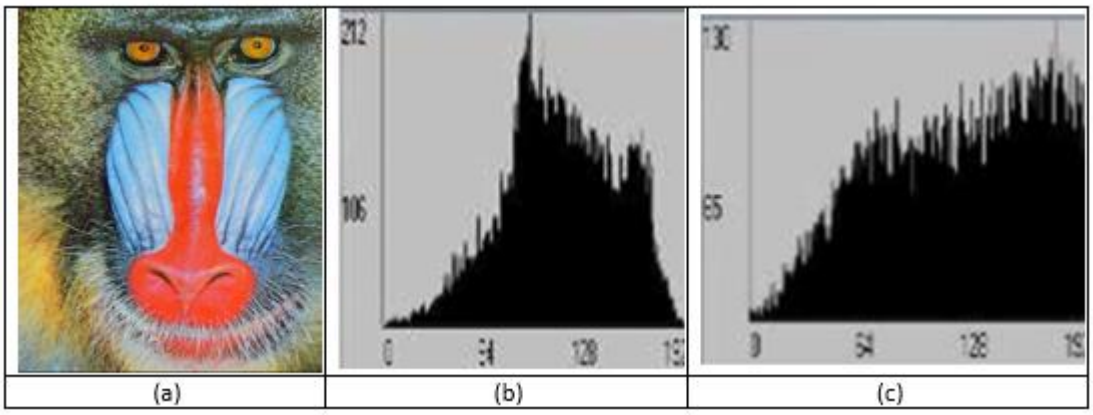

Figure 4. Histogram results (a) Baboon image (Block) Original image histogram (c) Encrypted image histogram

The baboon picture holds a bounty of information, yet it has been fiercely encrypted, resulting in the majority of its original appearance undergoing processing.

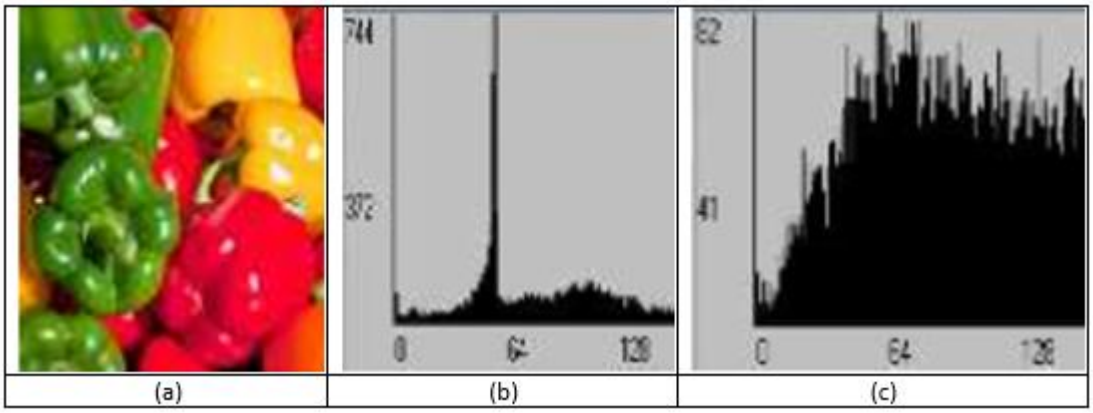

Figure 5. Histogram results (a) Pepper image (Block) Original image histogram (c) Encrypted image histogram

The histogram showcases encryption's proficiency by diminishing the primary data and enhancing the encrypted signal, a testament to its efficiency. Although the original data may be limited in scope, its validity remains unquestioned. The histogram is a vivid demonstration of encryption's achievements.

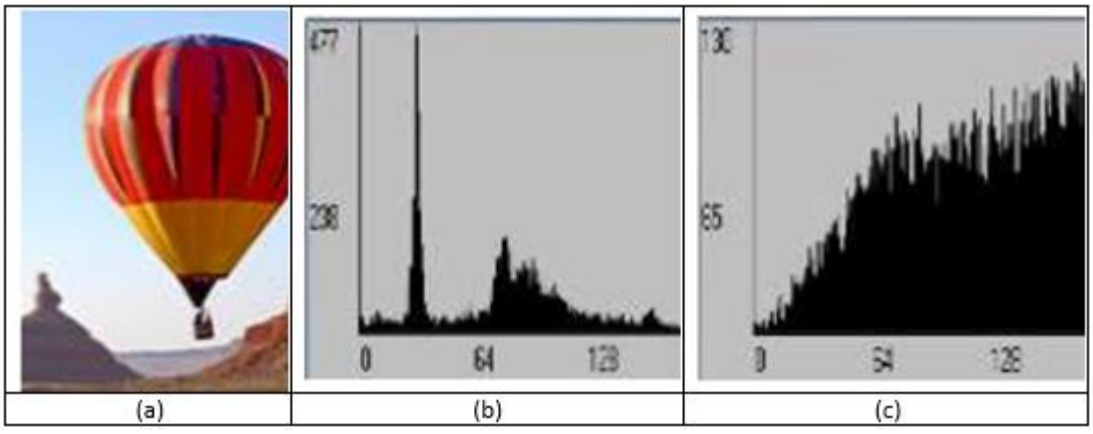

Figure 6. Histogram results (a) Balloon image (Block) Original image histogram (c) Encrypted image histogram

The balloon image histogram indicates a high data image; despite being heavily encrypted, most of the original image had been transformed.

Table 1. Proposed method results.

Image	Secret key	PSNR (dB)	SNR (dB)
Pepper	Image (4.19) KB	4.899	0.016
Baboon	Audio (4.61) KB	7.618	2.760
Balloon	Pdf (1.09) MB	5.397	1.251
Lena	Text (27.4) KB	7.075	1.822

Results and Discussion

The recommended algorithm underwent a thorough security evaluation, including a close examination of key sensitivity, a comprehensive analysis of the key space, and statistical analysis, all of which ultimately demonstrated the exceptional security benefits of the proposed method.

Analysis of the Key Space

The key space is the single most crucial element in determining the resilience of ciphering algorithms. The following formula may be used to locate the keyspace: 16*16*8* k
The dimension of the block is 16*16 inches in this case. Therefore, the 8 number is the color palette of (Red, Green, and Blue), and SK is the block number that could be determined by dividing the size of the secret file by 256.

Key Sensitivity

Regarding the key sensitivity for the suggested algorithm way, the one-bit alteration is made to the secret key, which disentangles the encoded image after it has been encrypted. Comparing the encrypted image obtained with the incorrect key to the decrypted image obtained with the correct key shows that the proposed encryption method is exceptionally key sensitive, so even practically ideal speculation of the key does not think twice about effectiveness.

Robustness

The proposed method has been shown to be effective in arranging chains of elements that adjust their position and value, which covers the elements due to the extended key integrated into the system.

Security image

A procedure of image encryption delivered data that was unintelligible; thus, no unauthorized individual access to the image that it is original or any other sort of sending information over broadcast systems. The technology gives a substantial degree of privacy and safety.

Conclusions

This research proposes a new image encryption algorithm that adds essential values. The algorithm used in this paper proposes a technology of image encryption that uses a key chain with 2048 bits (16 * 16 × 8), which is a minimum size. Therefore, the original image consists of a series of pixels divided by continuous byte blocks. Pixel by pixel is performed by a series of complicated, unconventional replacement and transposition processes, creating a long and random key. The proposed method provides a high level of protection for encrypted images. Furthermore, the encryption algorithm uses bitmaps effectively.

In addition, the proposed algorithm used in this paper achieves the best results among all experiments done recently, with higher certainty and less period. Furthermore, this work uses images (Pepper, Lena, and Baboon) to show the differences between the encrypted and the original images. Finally, by comparing the work related to this research, we will find that the method used depends much on it due to the longer key, its randomness, and its complexity.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

Acknowledgment

With gratitude, we extend our thanks to Asst. Lect. Fallah H. Najjar, Al-Furat Al-Awsat Technical University, for his invaluable aid and backing throughout the journey of research and publication.

References

[1] Ahmad, S., Alam, K. M. R., Rahman, H., & Tamura, S. (2015, January). A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets. *2015 International Conference on Networking Systems and Security (NSysS)* (pp. 1-5). IEEE.

[2] Al-Husainy, M. A. F. (2012). A novel encryption method for image security. *International Journal of Security and Its Applications*, *6*(1), 1-8.

[3] Auyporn, W., & Vongpradhip, S. (2015). A robust image encryption method based on bit plane decomposition and multiple chaotic maps. *Int. J. Signal Process. Syst*, *3*(1), 8-13.

[4] Bani, M. A., & Jantan, A. (2008). Image encryption using block-based transformation algorithm. *IJCSNS International Journal of Computer Science and Network Security*, *8*(4), 191-197.

[5] Boneh, D., Di Crescenzo, G., Ostrovsky, R., & Persiano, G. (2004). Public key encryption with keyword search. *In Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland*, May 2-6, 2004. Proceedings 23 (pp. 506-522). Springer Berlin Heidelberg.

[6] Chang, C. C., Hwang, M. S., & Chen, T. S. (2001). A new encryption algorithm for image cryptosystems. *Journal of Systems and Software*, *58*(2), 83-91.

[7] Delfs, H., Knebl, H., Delfs, H., & Knebl, H. (2007). Symmetric-key encryption. *Introduction to Cryptography: Principles and Applications*, 11-31.

[8] Guo, J., Ling, S., Rechberger, C., & Wang, H. (2010). Advanced meet-in-the-middle preimage attacks: First results on full Tiger, and improved results on MD4 and SHA-2. *Advances in Cryptology-ASIACRYPT 2010: 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore*, December 5-9, 2010. Proceedings 16 (pp. 56-75). Springer Berlin Heidelberg.

[9] Hathot, S. F., Jubier, N. J., Hassani, R. H., & Salim, A. A. (2021). Physical and elastic properties of TeO_2-Gd_2O_3 glasses: Role of zinc oxide contents variation. *Optik*, *247*, 167941.

[10] Khudhair, K. T., Kadhim, O. N., Najjar, F. H., Abedi, F., Jamaluddin, A. N., & Al-Kharsan, I. H. (2022, May). Soft edge detection by mamdani fuzzy inference of color image. *2022 5th International Conference on Engineering Technology and its Applications (IICETA)* (pp. 379-383). IEEE.

[11] Salim, A. A., Ghoshal, S. K., & Bakhtiar, H. (2021). Tailored morphology, absorption and bactericidal traits of cinnamon nanocrystallites made via PLAL method: Role of altering laser fluence and solvent. *Optik*, *226*, 165879.

[12] Sivakumar, T., & Venkatesan, R. (2013). A novel image encryption approach using matrix reordering. *WSEAS Transactions on Computers*, *12*(11), 407-418.

[13] Waheed, S. R., Rahim, M. S. M., Suaib, N. M., & Salim, A. A. (2023). CNN deep learning-based image to vector depiction. *Multimedia Tools and Applications*, 1-20.

[14] Salim, A. A., Ghoshal, S. K., & Bakhtiar, H. (2021). Growth mechanism and optical characteristics of Nd: YAG laser ablated amorphous cinnamon nanoparticles produced in ethanol: Influence of accumulative pulse irradiation time variation. *Photonics and Nanostructures-Fundamentals and Applications*, *43*, 100889.

[15] Huang, F., & Qu, X. (2011). Design of image security system based on chaotic maps group. *Journal of multimedia*, *6*(6), 510.

[16] Sivakumar, T., & Venkatesan, R. (2014). A novel approach for image encryption using dynamic SCAN pattern. *IAENG International Journal of Computer Science*, *41*(2), 91-101.

[17] Najjar, F. H., Khudhair, K. T., Khaleq, A. H. A., Kadhim, O. N., Abedi, F., & Al-Kharsan, I. H. (2022, May). Histogram Features Extraction for Edge Detection Approach. *2022 5th International Conference on Engineering Technology and its Applications (IICETA)* (pp. 373-378). IEEE.