 ISSN:2302-8149
e-ISSN:2540-9719

Digital Image Confidentiality using New Encryption Method

[1]Yaseen Hikmat Ismaiel, [2]Omar Muayad Abdullah, [3]Yasir Mahmood*
[1,2,3]Computer Science Department, College of Computer Science and Mathematics University of Mosul, 41002 Mosul, Iraq
*e-mail: yaser.ali@uomosul.edu.iq

(***received*:** 8 January 2026 , ***revised*:** 12 February 2026 , ***accepted*:** 8 March 2026)

Abstract

The significant development in mobile phone cameras, in terms of the clarity and high-resolution images captured, the wide utilizing of mobile phones and other communication devices among all segments of society, and the increasing use of social networking sites and the exchange of millions of digital photos daily, all have been pointed with a great importance of digital images and the need to provide adequate security and protection for these images. Digital images contain a large amount of information and recently they have an effective and easy tools of communication without the need for a determined text.Given that digital images contain important, personal, and sensitive information, there is a great need to protect these images and prevent unauthorized persons from applying any changes to the image's contents. There is a great deal of work in this field, most of which uses encryption methods to achieve this protection. As is well known, there are two types of encryption systems (symmetric and asymmetric). Symmetric encryption systems are fast but require a secret key distribution process, while asymmetric encryption systems are relatively slow, involving complex processes. Therefore, they are not suitable for use in social networking applications that require rapid performance and interaction. In this research, a proposed method for digital image encryption is proposed, which includes the use of logical XOR operation to encrypt the digital image based on two proposed levels with scrambling operation to provide a high degree of diffusion and confusion for the resulting encrypted image. The proposed method was evaluated through a set of efficiency measurement metrics (NPCR, UACI, MSE, PSNR, SSIM, Entropy, and Correlation) and it gave results showed a difference between the original image and the image resulting from the first level of encryption. We also noted that the image resulting from the second level had a higher percentage of difference and randomness compared to the original image. Therefore, the proposed encryption method is suitable in terms of speed and confidentiality for use in encrypting digital images and thus maintaining their privacy.

Keywords: *cryptogrsaphy, image encryption, xor encryption, xor gate*

1 Introduction

Digital images are considered as a most important interactive media that is applied for exchanging information on social media networks and websites. An image contains a significant amount of information and is a concise and alternative method for expressing a large amount of information. Compared to voice recording, which requires a special environment, including low noise and high sound quality, a digital image is the best option in this case. Capturing images using advanced mobile phones has been characterized by high speed and accuracy. Digital images are used in all fields as tools used for exchanging information. In the military field, the images can be presented as an attack plan, the enemy's movements or location changing, or the quantity of weapons and equipment available [1].

In the medical field, an image may be used to describe a patient's case, such as vital signs, the case of a wound, the type of treatment, the patient's position, etc. Transferring image files over the internet exposes them to the risk of attackers accessing or manipulating their contents by unauthorized individuals. Encrypting operation for the digital images protects them and prevents unauthorized individuals from accessing and changing their contents. We have two kinds of encryption systems: symmetric encoding, that has one key for encoding and decoding, and asymmetric encoding, which, means using two different keys that have been linked by a mathematical relationship, one for encryption and the other for decryption. Figure (1) explain symmetric and asymmetric encryption

 ISSN:2302-8149
e-ISSN:2540-9719

systems. There are many of studies and researches that have used different encryption systems to protect digital images and maintain their confidentiality [2] [3].

Some of these methods have used standard encryption methods, including older ones (RSA, DES) and newer ones (AES, BLUFISH). Other researchers have combined these methods to create a hybrid method that offers better features. Others have used chaotic and random functions to provide additional features. All methods have been characterized by the time-consuming nature of image encryption and decryption [4].

Since we need a cost- and time-efficient encryption method that can be used to encrypt images exchanged over social media easily and efficiently, we need to develop a method that is both cost-effective and time-efficient [1] [5].

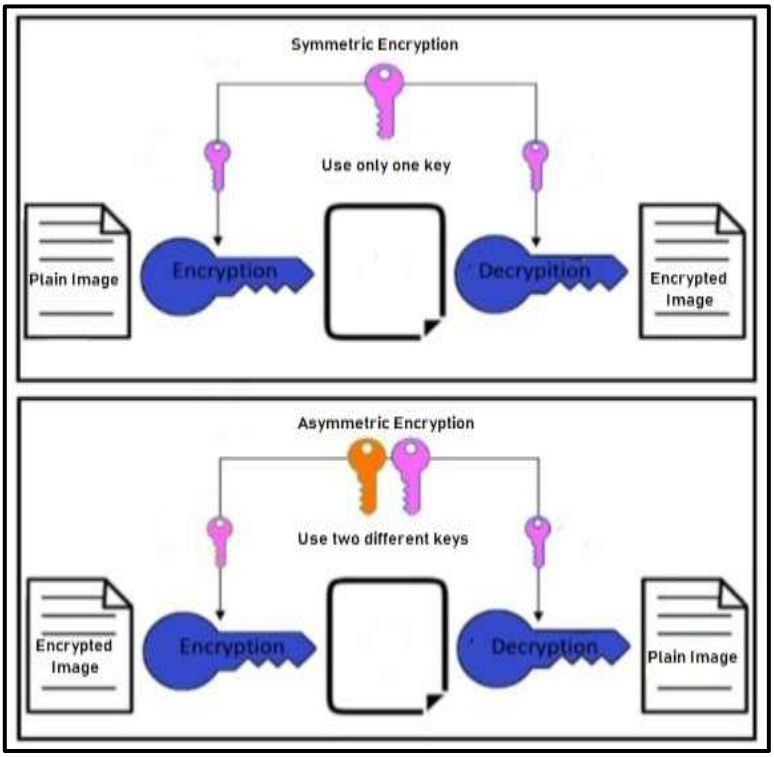
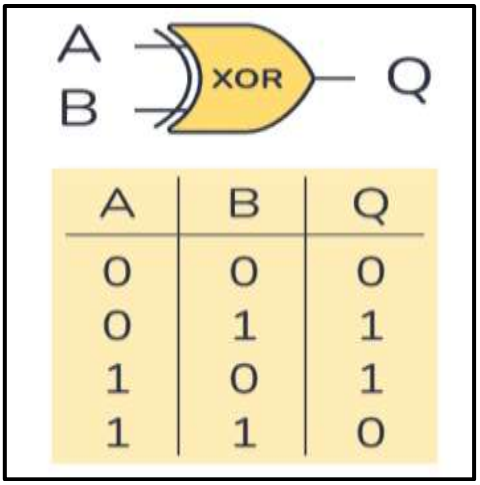


Figure 1 Symmetric and asymmetric encryption systems [5]

The logical XOR operation is an important operation used in encryption methods. It deals bits and has two inputs and one output. It is characterized by the fact that when the output is available in addition to one of the two inputs, the other input can be resulted through applying the same XOR operator. Figure 2 illustrates the logical XOR operation [6].



A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

Figure 2 logical XOR operation [6]

 ISSN:2302-8149
e-ISSN:2540-9719

In this research, the logical XOR operation was used to present an efficient encryption method for digital images. The method includes two levels of encryption based on the advantages of the XOR operation. The proposed method does not use a key for encryption and decryption, relying solely on the digital image data (in binary format). The method is characterized by its speed and encryption efficiency.

2 Literature Review

Image encryption is an important method for maintaining the confidentiality and privacy of images. There are many methods used to encrypt digital images, some of which rely on standard encryption methods, while others combine these methods with other technologies to improve their efficiency and increase their security. Essaid and et al. suppose a proposed schematic image encoding depending on confusion and diffusion to secure colored and grayscaled arrays using an improved tilted chaotic map (ESTM). First, they optimize the chaotic behavior of the ESTM to produce a robust chaotic key which is considered suitable for image encoding. Then, traditional confusion and diffusion techniques are applied to the original image, which is divided into 1×256 blocks. Simulation results demonstrate the validity of the proposed scheme [7].

Researcher Afifi presented a modification of the Henon chaotic map, which was used before and after modification at two different levels to spread confusion and noise in the image bits, thus obtaining an encrypted image. The proposed encryption method included two levels. In the first level, the modified Henon map with n cycles was used to confuse and blur the image pixels, while the second level included the use of the standard Henon chaotic map. The outcomes of applying the supposed encryption procedure showed that both the encoding and decryption processes were successfully performed using the same secret keys, achieving high security for grayscale images by distributing grayscale values in a quasi-random manner [8].

The researchers used chaotic functions to generate two ordered strings of random numbers. The digital image encryption method involved two levels: the first encoded the image data using the first string of random numbers with a logical xor operation, while the second level shuffled and reordered the encrypted data generated by the first level. A set of metrics demonstrated the method's effectiveness in encrypting digital images [9].

Yao and et al. used the Gyrator transform (GT) to encrypt an image by considering spectral units as input to the transformation algorithm, multiplying these values with phase values, and finally using the Fourier transform to produce the encrypted image. The randomization of phase values helps strengthen the encryption method and make it resistant to many attacks. The researchers built a simulation model to measure the efficiency and robustness of the encryption method [10].

New image encoding method depends on Forwarded LSTM algorithm and the 2-D Couple Map (2DCML) fraction system has been supposed. The reference image has been partitioned into number of blocks of image, and every block is considered as an input to the LSTMS as sub sequence of pixels. According to the chaotic sequences that is derived by the 2DCML fractional system, the determined factors of the input gate, output gate and memory unit of the LSTM have been initialized, and the determined pixel positions also have been changed at the same time when we change the pixel values, and this will lead to synchronizing the permutation and diffusion operations, therefore improves the performance of image decoding and reduces the consumption of the time. Many simulation results show that the proposed scheme has higher security and efficiency comparing with previous schemes [11].

In this paper, a proposed method is considered for image encoding based on a strong chaotic mechanism and Fibonaci Q-matrix. The reference image has been disoriented in the proposed method, using the numbers that generated randomly using the 6-Dimension strong chaotic system. Then, the image that has been swapped is diffused using the Fibonaci Q-matrix. The supposed image encoding algorithm is examined using cut attacks for both noise and data, histogram, key space, and sensitivity. The supposed method is achieved a high secure position and execute the existing image encryption algorithms [12].

Bai and et al. used the concept of visual cryptography and proposed a new method that generates a set of meaningful (clear) fractal images that are completely different from the original image. At the receiving end, these fractal images are used to create a set of keys that are the basis for retrieving the

 ISSN:2302-8149
e-ISSN:2540-9719

original image. The proposed encryption method is considered to have low computational complexity and thus low time cost with a good level of security. In addition, this method is different from the concept of data compression and reduction, which is used in many encryption methods [13].

This research supposes a double-domains images encoding method depending on hyperchaotic and wavelet partitioning. The process of combining both the wavelet and diffusions processes has been included in the supposed method in order to understand the process of combining the spatial and frequency domain encoding. First, partitioning the referenced image into blocks, then using the sequence of random numbers in order to manage the block scramble policy, and produce a scramble array; then through calculate the Hamming distance for the plaintext, select the class of the wavelet, applying the process of decomposition of wavelet, and producing the coefficient array of the wavelet; Re-inputting the plaintext of the image to the (SHA512) method in order to produce the first value for the strong chaotic. The chaotic policy then produces the chaotic key array by applying the iteration process; then the scrambled array will be rotated, and then the process of Zigzag transform will be used in order to produce the key array; Finally, the wavelet coefficient array, the chaotic key array, and the key array are faced to bitwise XOR operator to understand the pixel diffusion values and getting the final encoded image [14].

In this research, a proposed digital image encoding policy is supposed depending on "bit replacing" method, chaotics systems and the DNA-coding strategy. First, in the proposed policy every determined pixel in the image has been translated into its equivalent sequence of binary form that is consisting of 0's and 1's bits. The "0" bit is changed to (1 and 0) bits and the "1" bit is replaced by (0 and 1) bits. Second, the derived images have been encoded by the highly "dimensional chaotic systems" depending on the concept of permutation and diffusion procedures. Third, the derived encrypted images have been encoded using the adopting-DNA method policies and then these determined images are grouped using additional DNA process. In the last step, the coded DNA images are decrypted in order to get the resultant encrypted image [15].

A cryptosystem novelty is previewed that is depended on a "6-D hyperchaotic system" and "random signal insertion". In order to improve the dynamic efficiency of the strong chaotic system, we added some signals that are considered random into the determined variables of the system during iteration process. The derived summation value of all plaintext pixels will be used to create the initial values of the system. Thus, the supposed cryptosystem is related to the plain image. Splitting a pixel into two equivalent segments and create a larger matrix. Scrambling, "cycle shift", and diffusion are dealing with the new matrix. Finally, we obtain the encoded image. The simulation creates reveal that the supposed policy has a very huge key space, high key sensitivity and robustness, and is cable of resisting many different attacks. It has high secure than many other image encryption mechanisms [16].

New algorithm of image encoding with using Advanced Encryption Standard (AES) method and the chaotic maps. This procedure is consisting of both the substituting and the permutation levels. The round keys are created by AES using "key expansion algorithm". The sensitivity that derived from this technique is that it is depended on the initial values and the input image. S-boxes in AES both introduce non-linearity, confusion, improving security and resistance to cryptographic attacks by substituting the blocks of bytes in the encryption level. The results of these tests show that this technique has high security and resistant towards any attacks [17].

Zhou and Zhu proposed algorithm of image encryption depending the "hybrid heterogeneous time-delay chaotic systems". The proposed strategy uses a group of sequences that is created by multi-"heterogeneous time-delay chaotic systems", rather than sequences from a "single chaotic system". especially, the three sequences that have been randomly determined to the image pixel scrambling and diffusion processes. Our proposed encryption method is developed by a variety of time-delay chaotic systems, by increasing the space of the determined key, security enhancement, and making the encoded image harder to crack. Simulation experiment results are verify that our algorithm exhibits superior encryption efficiency and security compared to other encryption algorithms [18].

3 Research Method

The proposed method relies on the logical XOR operation to encode color digital images. After reading the digital image and converting it to binary format, it is represented as a two-dimensional

 ISSN:2302-8149
e-ISSN:2540-9719

array of binary numbers (rows and columns). As we demonstrated, the property of the XOR operation is that if one of the two inputs and an output are available, an XOR operation can be performed between them to obtain the other input.

The first level of encryption involves XORing every two consecutive lines and storing the XOR result as a new line in the resulting matrix, plus a line containing two halves of the original matrix (which were XORed). The XOR result is placed with the original halves at variable locations in the resulting matrix to add randomness and increase confusion and diffusion in the resulting matrix, which represents the encrypted image data (the intermediate stage). Figure 3 illustrates the first level encryption process of the proposed method.

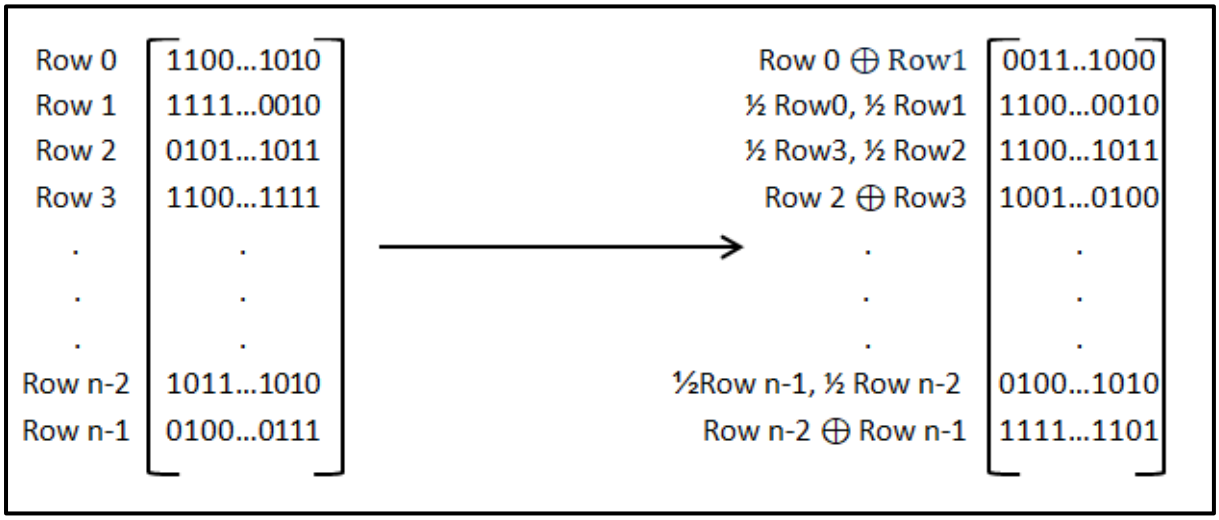


Figure 3 The first level encryption process

From the Figure 3, we can see that the resulting intermediate encryption matrix can be swapped in two ways:

1. The position of the resulting row is changed by the XOR operation, so that it is in the first position once and the second position another time.
2. For a row containing two parts of the original matrix, the positions of the two parts are swapped, so that the first part is part of the first row of the original matrix, followed by the second part, which is part of the second row. Conversely, in the following two lines, the first part is part of the second row, followed by the second part, which is part of the first row of the original matrix.

The original matrix can be recovered from the intermediate encryption matrix by performing an XOR operation between each two consecutive lines, as shown in Figure 4.

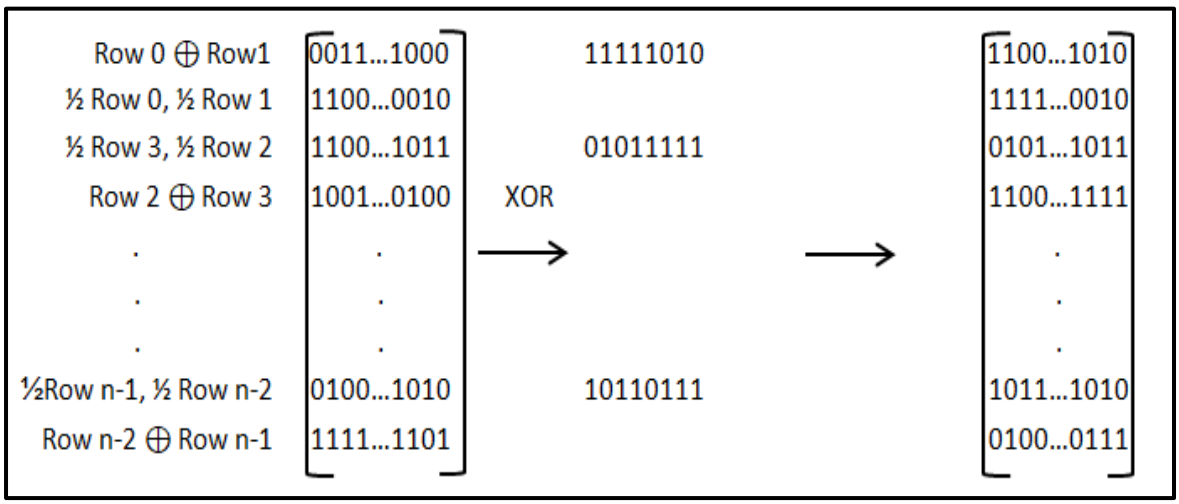


Figure 4 Original matrix recovering

 ISSN:2302-8149
e-ISSN:2540-9719

The second level of encryption is also done using the XOR operation between successive lines of the intermediate encryption matrix, so that the resulting matrix contains a line that represents the output of the XOR operator for two successive lines of the intermediate matrix, followed by a line that represents the output of the XOR operator for two successive lines of the original matrix, meaning that the encryption matrix resulting from the second level is a series of successive lines that represents the output of the XOR operator once for lines of original matrix and once for the lines of the intermediate matrix, as shown in Figure 5.

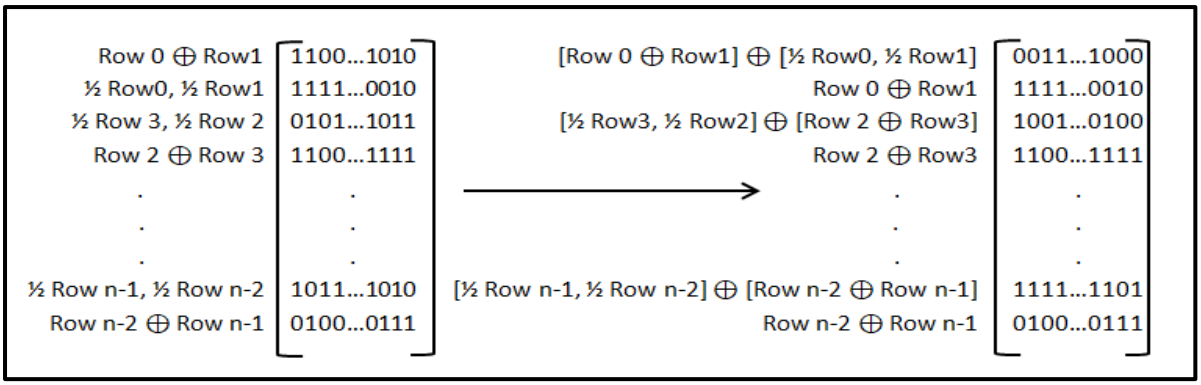


Figure 5 The second level encryption process

To increase the randomness of the resulting encryption matrix, the matrix is divided into blocks of 8 rows and columns, representing the division of the matrix's columns into two parts. The threshold value (8- rows) selected to give more balancing between the efficiency of permutation and the randomness. Confusion and diffusion rate is increased by swapping the values in each block according to the following steps:

1. Swap the elements of each part of the matrix rows.
2. Swap the elements of the matrix columns, as shown:

i.e.
row 0 part 1 ↔ row 7 part 2 and row 0 part 2 ↔ row 7 part 1
row 1 part 1 ↔ row 6 part 2 and row 1 part 2 ↔ row 6 part 1
row 2 part 1 ↔ row 5 part 2 and row 2 part 2 ↔ row 5 part 1
row 3 part 1 ↔ row 4 part 2 and row 3 part 2 ↔ row 4 part 1
row 4 part 1 ↔ row 3 part 2 and row 4 part 2 ↔ row 3 part 1
row 5 part 1 ↔ row 2 part 2 and row 5 part 2 ↔ row 2 part 1
row 6 part 1 ↔ row 1 part 2 and row 6 part 2 ↔ row 1 part 1
row 7 part 1 ↔ row 0 part 2 and row 7 part 2 ↔ row 0 part 1

Figure 6 illustrates the process of switching between sites.

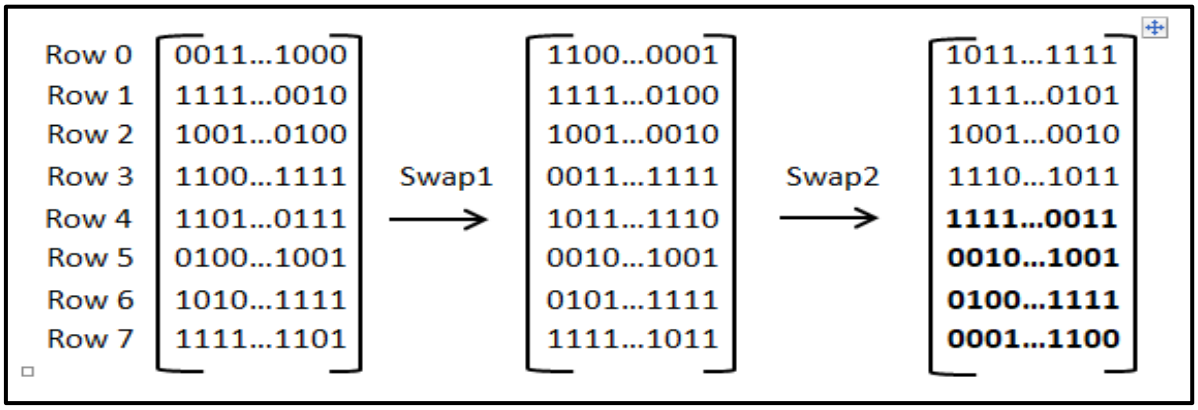


Figure 6 The process of switching between array sites

 ISSN:2302-8149
e-ISSN:2540-9719

4 Results and Analysis

To evaluate the performance of the proposed image encryption algorithm, five different images with many statistical and perceptual metrics are employed. The Number of Pixels Change Rate (NPCR) measures the percentage of pixel values that differ between both the two images. The (UACI) quantifies intensity of the average difference between corresponding pixels, Mean Squared Error (MSE) computes the average squared difference between two images, Peak Signal-to-Noise Ratio (PSNR) is a metric that is used for measuring the ratio between the maximum power case of the signal and the noise power affecting its representation, typically expressed in decibels (dB). It is commonly used to assess the quality or fidelity of reconstructed or processed data, such as images or audio. The Structure Similarity Index Measuring (SSIM) helps the structural resemblance between two images; the Information Entropy measures the randomness of pixel distribution; higher entropy values (close to 8 for 8-bit images) demonstrate stronger security and better resistance to statistical attacks. Finally, the Correlation Coefficient evaluates the linear relationship between adjacent pixels. Table 1 shows the values of these metrics for the comparison of the original image with the image result from level one encryption of the proposed method. Level two encryption aims to make the encryption method stronger and more robustness as show in table 2, there is a significant change in metrics which indicates increased efficiency of the encryption process. In order to provide a realistic evaluation of the proposed method, a comparison is derived for both the referenced image and the final image resulting from the second level of the encryption process. The values for the metrics reveal significant changes and significant differences between the original and encrypted images, as shown in Table 3.

It is well known that when a digital image is encrypted, the goal is to make the resulting encoded image is different from the referenced image. This conceals the image's features, preventing unauthorized individuals from viewing it and understanding its content. By observing the metrics used to demonstrate the effectiveness of the proposed method, we note that the values in Table 1 indicate a significant difference between the two images.

Table 1 Performance evaluation of level 1 encryption

Images / Metrics	Image1	Image2	Image3	Image4	Avg.
NPCR	96.3327	97.1103	96.6659	96.1228	**96.5579**
UACI	31.3251	31.7622	31.0117	32.2329	**31.5829**
MSE	69.7623	69.9984	69.0012	70.1183	**69.7200**
PSNR	2.9945	2.9679	2.9742	2.9672	**2.96972**
SSIM	0.3258	0.2844	0.3751	0.3921	**0.3443**
Entropy	5.9528	5.3673	6.0341	6.2056	**5.8899**
Correlation	0.4729	0.3983	0.4229	0.4116	**0.4264**

Table 2 Performance evaluation between level1 and level 2 encryption

Images / Metrics	Image1	Image2	Image3	Image4	Avg.
NPCR	69.2823	69.2911	68.8301	69.1245	**69.1320**
UACI	22.9016	22.5821	22.1725	23.0176	**22.7080**
MSE	20.9229	21.0011	21.9881	21.2229	**21.2837**
PSNR	13.5662	14.0117	14.9111	14.0914	**14.1451**
SSIM	0.7798	0.8991	0.8130	0.7191	**0.8027**
Entropy	7.6679	7.7734	7.1497	7.0803	**7.4178**
Correlation	0.1874	0.1022	0.1899	0.1437	**0.1555**

 ISSN:2302-8149
e-ISSN:2540-9719

Table 3 Performance evaluation of the proposed encryption method

Images / Metrics	Image1	Image2	Image3	Image4	Avg.
NPCR	98.3297	99.0985	98.8004	99.0227	**98.8128**
UACI	32.9016	32.5821	32.1725	32.0176	**32.4184**
MSE	88.1093	86.1283	88.9224	88.1017	**87.8154**
PSNR	1.3566	1.4011	1.4911	1.4091	**1.4144**
SSIM	0.2755	0.1995	0.2100	0.2964	**0.2453**
Entropy	7.9611	7.8784	7.7437	7.2891	**7.7180**
Correlation	0.0392	0.0087	0.0129	0.0681	**0.0322**

In Table 2, the difference between the two encrypted images (the resulting image from Level 1 and the resulting image from Level 2) is minimal. This is because the encryption process at Level 2 is complementary to the encryption process at Level 1, as the input image to Level 2 is an encrypted image. By observing the results in Table 3, which represents the final evaluation of the proposed encryption method, we note that all metric values indicate the efficiency of the encryption process and the significant difference between the original image and the resulting encrypted image, making it highly secure and effective. It achieves excellent diffusion, noise, and randomness, which are the essential factors for resisting statistical and differential attacks.

5 Conclusion

Xor operation used as the main process for the proposed image encryption method, we used the xor in different stages and inputs. The selected 8- rows threshold for divided image to blocks give perfect permutation between rows and high confusion and diffusion. By observing the results of the criteria values in the tables, we notice a significant change in the image data between the original image and the image resulting from first-level encryption. This percentage increased after second-level encryption. The proposed method is characterized by its ease of application, as it relies on the XOR operation, by changing the positions of the XOR results and placing them in different areas of the resulting image lines continuously during the encryption process, rather than relying on a fixed method, led to increased randomness, confusion, and diffusion thus increasing the efficiency of the proposed encryption method.

Acknowledgement

The authors would appreciate the support provided by the Computer Science Department/ College of Computer Science and Mathematics/ University of Mosul during the steps of this work.

References

[1] M. A. Khan, A. Rehman, A. A. Alnowiser, and S. Alqahtani, "*A Comprehensive Survey on Image Encryption: Taxonomy, challenges, and future directions*," Chaos, Solitons & Fractals, Vol. 177, p. 114370, Jan. 2024. [Online]. Available: https://doi.org/10.1016/j.chaos.2023.114370.

[2] E. A. Jameel and S. A. Fadhel, "*Digital Image Encryption Techniques: Article Review*," Technium, Vol. 4, No. 2, pp. 24–35, 2022. [Online]. Available: https://www.techniumscience.com.

[3] A. A. Alghamdi and R. Munir, "*Image Encryption Algorithms: A Survey of Design and Evaluation Metrics*," Journal of Cybersecurity and Privacy, Vol. 4, No. 1, p. 7, 2024. [Online]. Available: https://doi.org/10.3390/jcp4010007.

[4] S. Alshahrani and M. K. Khan, "*Survey on Image Encryption Techniques using Chaotic Maps*," International Journal of Information Security, Vol. 21, pp. 745–777, 2022. DOI: 10.1007/s10207-022-00588-5.

 ISSN:2302-8149
e-ISSN:2540-9719

[5] M. M. Eltoukhy, F. S. Alsubaei, Y. M. Elnabawy, and K. M. Hosny, "*Multiple Image Encryption Techniques: Strategies, Challenges and Potential Future Directions*," Alexandria Engineering Journal, Vol. 125, pp. 367–387, Apr. 2025. DOI: 10.1016/j.aej.2025.04.006.
[6] M. Dhakal and S. Shakya, "*Enhancing Image Data Security: DNA Cryptography and XOR-based Feistel Encryption*," Journal of Innovative Image Processing, Vol. 7, No. 1, pp. 1–27, 2025.
[7] M. Essaid, I. Akharraz, A. Saaidi, and A. Mouhib, "*A New Image Encryption Scheme based on Confusion-Diffusion using an Enhanced Skew Tent Map*," Procedia Computer Science, Vol. 127, pp. 539–548, 2018. DOI: 10.1016/j.procs.2018.01.153
[8] A. Afifi, "*A Chaotic Confusion-Diffusion Image Encryption based on Henon Map*," International Journal of Network Security & Applications (IJNSA), Vol. 11, No. 4, pp. 1–13, 2019. DOI: 10.5121/ijnsa.2019.11401.
[9] T. Li, B. Du, and X. Liang, *"Image Encryption Algorithm based on Logistic and Two-Dimensional Lorenz*," IEEE Access, Vol. 8, pp. 13792–13805, 2020. DOI: 10.1109/ACCESS.2020.2966320.
[10] L. Yao, C. Yuan, S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, "*An Asymmetric Color Image Encryption Method by using Deduced Gyrator Transform*," Multimedia Tools and Applications, Vol. 79, pp. 31101–31118, 2020. DOI: 10.1007/s11042-020-08916-5.
[11] Y. He, Y. Q. Zhang, X. He, et al., "*A New Image Encryption Algorithm based on the OF-LSTMS and Chaotic Sequences*," Scientific Reports, Vol. 11, p. 6398, 2021. DOI: 10.1038/s41598-021-85377-1.
[12] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "*New Image Encryption Algorithm using Hyperchaotic System and Fibonacci Q-matrix*," Electronics, Vol. 10, No. 9, p. 1066, 2021. doi: 10.3390/electronics10091066.
[13] S. Bai, L. Zhou, M. Yan, X. Ji, and X. Tao, "*Image Cryptosystem for Visually Meaningful Encryption based on Fractal Graph Generating*," IETE Technical Review, Vol. 38, No. 1, pp. 130–141, 2021. DOI: 10.1080/02564602.2019.1611559.
[14] Q. Qin, Z. Liang, S. Liu, X. Wang and C. Zhou, "*A Dual-Domain Image Encryption Algorithm based on Hyperchaos and Dynamic Wavelet Decomposition*," IEEE Access, Vol. 10, pp. 122726-122744, 2022, Doi: 10.1109/ACCESS.2022.3212145.
[15] S. F. Yousif, A. J. Abboud, and R. S. Alhumaima, "*A New Image Encryption based on Bit Replacing, Chaos and DNA Coding Techniques*," Multimedia Tools and Applications, Vol. 81, pp. 27453–27493, 2022. DOI: 10.1007/s11042-022-12762-x.
[16] S. Sun, "*A New Image Encryption Scheme based on 6D Hyperchaotic System and Random Signal Insertion*," IEEE Access, Vol. 11, pp. 66009–66016, 2023. DOI: 10.1109/ACCESS.2023.3290915.
[17] S. Inam, S. Kanwal, R. Firdous, K. Zakria and F. Hajjej, "*A New Method of Image Encryption using Advanced Encryption Standard (AES) for Network Security*," Physica Scripta, Vol. 98, No. 12, p. 126005, 2023, DOI: 10.1088/1402-4896/acd3cc.
[18] Y. Zhou and E. Zhu, "*A New Image Encryption based on Hybrid Heterogeneous Time-Delay Chaotic Systems*," AIMS Mathematics, Vol. 9, No. 3, pp. 5582–5608, 2024, DOI: 10.3934/math.2024270.