Hybrid Image Encryption Approach Using XOR, AES, and Pixel Shuffling for Improved Security

Saja Jumaa Hammad
Al-Dour Technical Institute /Northern Technical University
Northern Technical University
Saladin , Iraq
saja.jumaa@ntu.edu.iq
https://Orcid.org/0009-0007-8980-0782

DOI: http://dx.doi.org/10.31642/JoKMC/2018/130201
Received Nov. 6, 2025. Accepted for publication Jun. 7, 2026

Abstract— *As digital communication continues to grow rapidly, there is an increasing need for secure and efficient techniques to send multimedia data, especially sensitive images. Symmetric cryptographic algorithms such as AES and XOR may be considered adequate for providing viable information security, but using them independently often sacrifices statistical strengths or increases computational load and cost. In this paper, we present a hybrid image encryption scheme that leverages three complementary approaches, including pixel shuffling, XOR diffusion, and AES confusion. The combination of shuffling, which is a very low overhead permutation approach, the XOR which is mathematically easy to work with, and AES which provides consistent strong non-linearity is able to produce an efficient encryption and decryption scheme with strong cryptographic qualities.*

A standard image, Lena RGB (256×256), was used for the experimental evaluation of the cryptographic scheme. The quantitative analysis characterized the implementation based on a variety of aspects, including entropy (8.0 theoretical), correlation coefficients, NPCR, UACI, and PSNR. The qualitative analysis included visual inspection and histogram analysis. Overall, results indicated that the hybrid scheme provided an improvement to stand-alone AES, XOR, and shuffling. Entropy approached 7.98, correlation coefficients were close to zero, NPCR and UACI estimates were 99.21% and 33.27%, respectively, demonstrating high resistance to a differential attack. However, PSNR estimates indicated perfect, lossless decryption.

The hybrid implementation produced cipher images that exhibited flat histograms and high randomness. This hybrid strategy maintains strong cryptographic strength while allowing for a reasonable computational effort to locate secure image encryption mechanisms and will prove effective within implementation towards multimedia security and secure image transmission systems.

Unlike traditional methods that independently utilize encryption techniques, this study presents a seamlessly integrated hybrid framework. It strategically merges pixel shuffling, XOR confusion and AES diffusion to enhance security while ensuring low computational overhead and lossless data reconstruction.

Keywords— Image Encryption; XOR Operation ; (AES)Advanced Encryption Standard; Pixel Shuffle; Histogram Analysis; Entropy; Correlation Coefficient; (Peak Signal-to-Noise Ratio; Number of Pixels Change Rate and Unified Average Changing Intensity

I. INTRODUCTION

The recent developments in network connectivity technologies have helped to increase the global access of the Internet, consequently increasing the amount of data and information exchanged considerably [1]. This has spawned an epidemic of dissemination of all forms of digital content .The digital communication technologies today make the process of transmission and storing the image data a normal process in many fields such as medical imaging, remote sensing, social networking, and surveillance systems [2]. With the increasing use of these applications, privacy and integrity of images being transferred becomes more critical especially in the case of data being shared through a non-trusted or public network. The design of traditional encryption algorithms, which were originally designed to work with textual data, can be found to be inefficient when applied to images, not just because of the large amount of data, and redundancy, but also because of the

high correlation between adjacent pixels in each of the color channels.

To curb the challenges, a hierarchy of specialized image encryption approach has begun to come forth. Most of these methods use chaotic maps to create pseudorandom keys or sequences and thus increase unpredictability and sensitivity. Besides this, such algorithms are generally tested with respect to entropy, inter-pixel correlation, histogram dispersion, and resistance to differential and known-plaintext attacks. For example, the method presented in "An efficient image encryption scheme for healthcare" [3] integrates the chaotic system in 3D in conjunction with histogram, entropy, temporal, and correlation response assessments to enhance encryption performance.

Other research efforts have sought to improve existing symmetric ciphers such as AES by adding more layers of security. In the [4] , the authors utilized chaotic key generation to modify the AES cipher which resulted in high entropy levels and greater resistance to common attacks. Hybrid encryption models that combine AES with XOR or bitwise methods have also been explored. As noted in [5] , AES and XOR combination produces encrypted images with histogram characteristics and sensitivity related to the key.

Drawing on this previously established body of work, we propose a hybrid encryption method for full-color (RGB) images that combines three methods: 1) XOR diffusion (used to increase randomness), 2) AES-128, which is a standard strong encryption, and 3) pixel shuffling, which adds additional confusion and permutation. The goal is to provide a high level of security, a high degree of resistance to attacks characterized as statistical or differential (the most common types of attacks), and computational efficiency.

The key contributions of this manuscript are as follows:

1. We propose a three-stage hybrid encryption method that uses XOR diffusion of the RGB pixels first, AES-128 encryption of the pixel values second, and pixel shuffling which randomizes spatial positions, last.

2. We demonstrate reversibility through the reverse of the encryption sequence (Unshuffle → AES decrypt → XOR decode) ensuring no information is lost and the full image can be recovered.

3. We provide qualitative and quantitative analysis, which includes visual comparisons, histogram uniformity, Shannon entropy, correlation coefficients, NPCR, UACI, and PSNR measures, of the images using qualitative and quantitative means, since the findings show that the proposed scheme is high security and retains high-fidelity images.

The rest of this paper will be organized as follows: Section 2 contains a review of related work, section 3 provides the details of the proposed model, Section 4 will provide the experimental results and analysis, and Section 5 will provide a summary of the paper with future research directions.

II. Background and Related Work

A. *Image Encryption*

Image encryption is a specific area of cryptography meant to secure digital images against unauthorized access or modification. Images possess special properties—generally larger data size, redundancy and strong correlation among neighboring pixels—that need to be uniquely encrypted. Text-based, or more appropriately, text-oriented encryption mechanisms do not sufficiently make use of these properties and will produce slower computation or weaker performance when utilized for image data[6].

The traditional objectives of image encryption are confidentiality, integrity, and authenticity. Confidentiality means that only authorized entities can access the visual aspect of the image. Integrity means that the data has not been altered or corrupted. Authenticity means that the image is original and verified back to a source. To satisfy these objectives, image encryption techniques often make use of the cryptographic principles of confusion and diffusion[7].

Confusion is meant to hide the relationship between the encrypted image (ciphertext) and the original image (plaintext). This is generally done using somewhat complicated substitution processes where one pixel value in the ciphertext image is influenced by multiple pixel values in the plaintext image and the encryption key itself. Nonlinear transformations are often applied to further confuse associations between the original and encrypted images [8].

On the other hand, the diffusion property has it that a small change in a given bit of the plaintext image spreads to many bits of ciphertext [9]. Practically speaking an insignificant change to the original picture leads to significantly different ciphertexts. Ordinarily, diffusion is enhanced by using pixel permutation methods, which encompass the exchange of pixel positions.

Most image encryption systems are also arranged into three consecutive steps in an initial permutation phase, a substitution phase, and a final permutation phase. Spatial correlations between pixels are removed by the first permutation. The substitution stage, involves the transformation of pixel values using mathematical functions and usually based on chaotic maps or S-boxes, which are functions based on non-linear functions. The encryption algorithms should be so strong that the resulting ciphertexts are resistant to statistical and computational attacks.

Chaos theory- a sub field of mathematics which deals with systems which are sensitive to initial conditions- has been very useful in encryption algorithms development. The chaotic systems have the following properties: determinism, randomness, extreme sensitivity of initial conditions (also known as the butterfly effect) and ergodicity; all of which are desirable characteristics in a cryptographic scheme [10]. In turn, chaotic maps are also good at creating pseudo-random sequences that are hard to predict or replicate without a clear understanding of their parameters.

Because of these characteristics, chaotic models are often included in device encryption algorithms to increase confusion and diffusion. A small difference in initial parameters can produce a dramatic change in the output sequence. This sensitivity guarantees that small changes in the encryption key result in completely different encrypted images, increasing diffusion and security. The random-like and ergodic nature of chaotic maps provides complex substitutions and pixel permutations, effectively hiding pixel values and spatial relationships within the image.

The Lorenz system, Henon map, Tent map, and logistic map are examples of typical chaotic maps used for image encryption. These maps can be one dimensional of multidimensional and can support complex encryption operations. A chaotic sequence, for example, can perform the following:

- Swap pixel coordinates: By randomly allocating points, the pixels of the image will be assigned new coordinates, which, to to some extent, changes its size and purpose.

- Substitute pixel values: New values can be derived by either application XOR operations between chaotic sequence values and the present/block pixel values or choices from substitution boxes (s-boxes).

- Generate encryption keys: Dynamic keys can be filtered by generating keys from chaotic systems. It becomes more difficult to carry out a brute-force attack when the key space is expanded.

B. XOR Cipher

A contemporary and very dependable encryption technique, the XOR Cipher uses an exclusive-or logic function to convert each bit of plaintext data into ciphertext data or vice versa [11]. It frequently occurs, for instance, when a cryptosystem's security is increased by adding another cipher [12].

In reality, the XOR algorithm—pronounced "exclusive or"—is an additive cipher that relies on the XOR logic operation, also known as exclusive disjunction. This logic operation is also known as modulus 2 additions [13]. When the inputs are different from one another, the XOR operation's output is true. XOR stands for "either one but not both, or none" in other words. Some computer malware frequently uses the XOR cipher to thwart reverse engineering. XOR is far more secure than some messages with key repetition if the key is random and the message is at least as long. XOR Encryption is a highly efficient and simple symmetric key encryption method. XOR Encryption is used frequently in more complicated encryption algorithms; due to its reliability and practicality, even in today's world.

C. AES algorithm

It is a symmetric algorithm that replaced the DES algorithm in 1991. The AES algorithm supports three key sizes: 128, 192, and 256 bits. AES uses a single key for both encryption and decryption. It provides strong security and high confidence in information encryption. AES performs 10 rounds for the 128-bit key, 12 rounds for the 192-bit key, and 14 rounds for the 256-bit key [14]. The AES algorithm goes through four stages (Fig.1 shows the encryption and decryption flowchart):

1. Sub Bytes: This is a non-linear substitution step where each byte in the state matrix is replaced by another byte based on a substitution table, known as the S-box. This operation adds confusion [15].

2. Shift Rows: This step involves shifting the rows of the state matrix by different offsets in a cycle. This operation introduces diffusion.

3. Mix Columns: This is a linear transformation that mixes the bytes of each column with the following columns. It involves an arithmetic operation in a finite field to create further diffusion[16].

4. Add Round Key: This process adds the round key, which is derived from the main encryption key, to the state matrix using XOR. This step integrates the key into the encryption process.

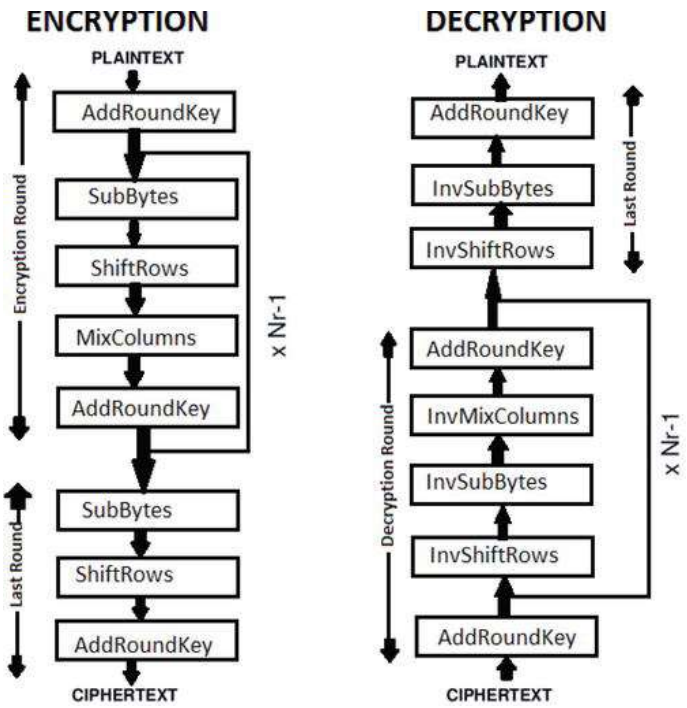

Fig.1. AES Algorithm Encryption & Decryption Rounds

D. Pixel Shuffling

Pixel shuffling is an image processing technique for scrambling the pixels' positions of the image. It consists of rearranging the pixels and changing the current position of the pixels which returns to pixel decorrelation [17, 18]. In this stage, every pixel position of the image is rearranged as determined by a secret permutation key produced by a pseudo-random number generator (PRNG). The key gives the mapping of original pixel indices to new positions to give a scrambled image that visually looks like random noise as shown in Fig.2.

To decrypt, the inverse permutation is used to return the pixels to their original pixel position which makes it perfectly reversible. Shuffling on its own does not provide a strong level of cryptographic security, but shuffling with traditional encryption algorithms, i.e., XOR and AES, greatly increases the strength against statistical and differential attacks.

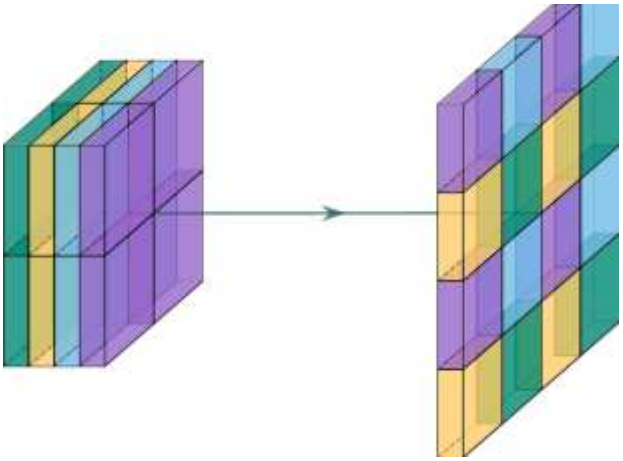

Fig.2. Graphical representation of the pixel shuffle operation [19]

While many existing approaches utilize either chaos-based permutation or AES-based encryption independently, they often encounter issues such as excessive computational complexity or inadequate statistical resistance when used in isolation. In comparison, the proposed method combines lightweight XOR diffusion, standardized AES encryption, and pixel shuffling in a synergistic way. This integration delivers enhanced entropy, improved decorrelation, and stronger resistance to differential attacks, all while minimizing computational overhead.

III. METHODOLOGY

This study proposes a hybrid image encryption framework that integrates the lightweight bitwise XOR and the robust Advanced Encryption Standard (AES) for efficiency and effectiveness in the protection of digital images. The methodology is described in terms of a number of main steps which can be seen in the system flow diagram.

Step 1: Input Image This process is initiated with the selection of a colored RGB image as the input. The RGB format retains the full color and makes it appropriate for the processing stages that come later.

Step 2: Preprocessing The image is then preprocessed by setting its dimensions to a common standard which in this case is 256×256 pixels. This is then represented as a numerical pixel array in which every pixel is shown by the red, green and blue intensity values. This prior to encryption processing makes sure the images are in compatible formats.

Step 3: XOR Encryption (Confusion Stage) At this stage, each of the pixel values is said to be ‘encrypted’ by performing a bitwise XOR with a secret key stream. The key is said to add confusion by masking the statistical aspects of the original image. Hence, minor changes to the key or the image will produce dominant changes to the encrypted image.

Step 4: AES Encryption (Diffusion Stage) Using the output of the XOR stage, we further encrypt the data using AES-128 in the block cipher mode. AES has strong diffusion properties, as the influence of a single pixel gets spread out across multiple encrypted pixels. This two-layered approach, in particular, significantly improves the defense against statistical and differential attacks while keeping the systems computation Cheap.

Step5 : Pixel Shuffle

Transmitting pixel positions is controlled by a permutation generated in a stochastic manner, that is, it operates to reduce inter pixel correlation and enhance resistance against statistical attacks. The permutation sequence (or its respective private key) is stored and maintained in confidence and later used in the process of decryption.

Step 6: Displaying the Encrypted Image Output

After the encryption process, the resulting image appears devoid of any recognizable features, resembling random noise. Analysis of the encrypted image's histogram further validates the process's effectiveness, as it demonstrates a uniform pixel distribution.

Step 7: Decryption Process

The process is carried out in the opposite order as the decryption process. In the first step, the Covered Text is subjected to a reverse shuffle operation, i.e. the renderer recovers the pixelated image to its original spatial setup. Then, AES decryption comes into action and the intermediate data can be retrieved with the help of a partitioned secret key. Lastly, the decryption of the XOR encrypted data is done using the same keystream that is used in the encryption. This means that it is possible to rebuild the original image in its entirety without any information being lost.

Step 8: Evaluation Metrics

The proposed scheme is evaluated on the basis of several performance criteria:

- ✓ Histogram Analysis can be applied to assess the randomness of pixel distribution in the encrypted image. That is, the histogram can depict the statistical aspect of pixel value distribution. The histogram plot can present the distribution of the image pixel counts across the different intensity levels. An encrypted image should have a uniform or even distribution of the pixel allocation to be effectively encrypted.

- ✓ Shannon Entropy : Entropy is defined as an indicator of uncertainty in the image processing context, and can be defined as the average uncertainty of an information source. The units of entropy are bits per second. The entropy calculation is given in Equation(1).

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

- ✓ Pixel Correlation Coefficient, to verify near-zero correlation among pixels in the encrypted image.

MSE (Mean Squared Error) and PSNR (Peak Signal-to-Noise Ratio), to ensure proper reconstruction of the original image during decryption.

PSNR is most easily defined via the mean squared error (*MSE*). Given a noise-free *m*×*n* monochrome image *I* and its noisy approximation *K*, *MSE* is defined as Equation (2)

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i.j) - K(i.j)]^2$$

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$

$$= 20 \cdot \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right)$$

$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

- ✓ NPCR and UACI

The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are analytic means of estimating the amount of protection against differential attacks [20]. These analytic methods examine how some of the least intense changes that are made to the original image will affect the encryption. The methods compare the original image data to the encrypted image data, estimating the differences in the representations. In order for the encryption to be secure, those differences must exist between the original image data and encrypted image data, and be able to withstand several differential attacks. When calculating the UACI, pixel values of the two images used or, the original image must be analyze the pixel values and obtain the average intensity changes that exist between both images of the UACI percentage that will fall a range of 0 to 100. A higher UACI percentage denotes that more differences between the images exist. As a caveat, before calculating the UACI, one should first examine and calculate differences in pixel real values between images. Next, these pixel value differences are averaged, and the resulting average is then expressed in a percentage by dividing the average difference by the maximum possible difference between pixel values and multiplying the result by 100. NPCR and UACI calculations for images can be written in the following as Equation (3) and Equation (4) respectively.

$$NPCR = \frac{1}{W * H} \sum_{i=1}^{W} \sum_{j=1}^{H} d_{ij} * 100\%$$

$$UACI = \frac{1}{255 * W * H} \sum_{i=1}^{W} \sum_{j=1}^{H} \left| C_{ij}^1 - C_{ij}^2 \right| * 100\%$$

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

With the combination of XOR for light confusion and AES for secure diffusion, the hybrid encryption scheme designed achieves both computation simplicity and high security, which is best suited for safe storage and transmission of images.

The interduce hybrid image encryption framework is structured into three consecutive stages: XOR-based confusion, AES-128 nonlinear diffusion, and pixel shuffling permutation. As depicted in Fig. 3, the arrangement and sequence of these stages are intentionally crafted to strengthen security while ensuring computational efficiency.

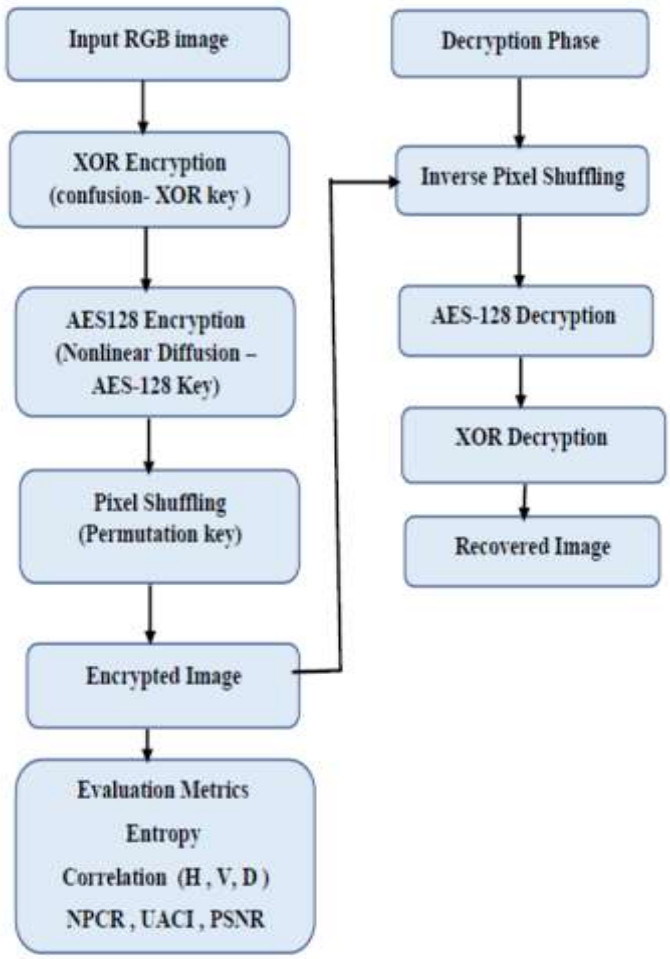

Fig.3. Proposed Method

The proposed framework does not simply involve a direct combination of independent encryption components. Instead, the sequence comprising XOR-based confusion, AES-128 nonlinear diffusion, and pixel shuffling permutation is carefully crafted to harness the unique strengths of each method. The XOR operation offers an efficient initial layer of confusion with minimal computational expense. AES-128 enhances the system with robust nonlinearity and strong resistance to cryptographic attacks, while pixel shuffling efficiently disrupts spatial correlations among pixels. Introducing additional

encryption stages may not necessarily enhance security and could lead to unnecessary computational overhead. As a result, the chosen hybrid structure strikes a well-optimized balance between security robustness and processing efficiency.

The choice of XOR, AES-128, and pixel shuffling is driven by their mutually reinforcing security features. XOR offers computational efficiency, enabling quick confusion, while AES-128 stands as a reliable and thoroughly vetted encryption standard, ensuring strong diffusion and nonlinear transformation. Pixel shuffling serves as an effective permutation method to reduce spatial redundancy in images. Unlike chaos-based methods, this combination mitigates sensitivity to initial conditions and numerical precision challenges, resulting in a more stable and practical solution for real-time image encryption applications.

IV. RESULTS AND DISCUSSION

The experimental evaluation was performed using the Lena standard image (RGB, 256×256) to assess the performance of the developed hybrid encryption scheme. Multiple encryption configurations were assessed independently (XOR-only, AES-only, Shuffle-only) and together, as suggested in the proposed hybrid. The numerical performance metrics are summarized in Table 1, while images and their respective histograms are represented in Fig.4 and Fig.5.

The proposed encryption scheme's effectiveness is assessed through correlation and differential attack analyses. To evaluate the dependency between adjacent pixels in the encrypted image, correlation coefficients are computed in horizontal, vertical, and diagonal directions as shown in Fig. 6. Ideally, these coefficients should approach zero, signifying effective decorrelation. Furthermore, the scheme's resistance to differential attacks is measured using NPCR and UACI metrics. These metrics assess how sensitive the encrypted image is to minor alterations in the original image. High NPCR and UACI values indicate robust diffusion properties of the proposed approach.

From the entropy analysis, the original Lena image had a value of approximately 7.11 (for each channel) and indicated the redundancy of most natural images. The XOR-only and Shuffle-only encryption algorithms increased the entropy of the original image by a small, yet statistically significantly amount (to approximately 7.5–7.6). However, the increase was insufficient to be considered uniformly random. Meanwhile, AES-only improved the entropy of the Lena image more (~7.8), and the proposed hybrid approach achieved an entropy value close to 8.0 (i.e., close-to-uniform), indicating a strong resistance to statistical attacks, and a uniform (i.e., random) distribution of pixel-intensity values in the encrypted images produced via the proposed hybrid.

The improvement is further supported by pixel correlation analysis. The original image displayed strong correlation in adjacent pixels of over 0.9. XOR and Shuffle reduced the correlation but detectable dependencies remained. AES improved the situation further but the hybrid approach almost entirely decorrelated the pixels, with very low values in the horizontal, vertical, and diagonal directions — approaching zero. This decorrelation means that the encrypted image is more similar to random noise - the histograms demonstrate this in Fig4 and Fig5.

Next, differential analysis supported the hybrid scheme's strength. The hybrid method achieved an NPCR of 99.21% and a UACI of 33.27%. This is in agreement with the theoretical expectations of >99% and ≈33%, respectively. This indicates that a change in just a single pixel of the plaintext results in changes throughout the majority of the cipher, thus making the system resistant to a differential cryptanalysis attack — GN06 and GN07 note that neither XOR-only nor Shuffle-only perform as well and that AES-only performs better but not as well as the hybrid outcome does.

In summary, the PSNR values confirmed the encryption reversibility by illustrating equal and infinite PSNR, which indicates MSE of zero, which indicates a lossless entropy image. The quality of imagery independently validates the above results: XOR-only or Shuffle-only executable images exhibited faint structure; AES-only contained more randomness; and hybrid images were of noise-like visual nature and exhibited flat histogram reflections. The decrypted output is visually, quantitatively, and experientially equivalent to the original.

In consideration, both quantitative to quality metrics (Table 1) and visual imaging evidence (Fig.4 and Fig.5), support the conclusion that the hybrid scheme dramatically out-performs solitary techniques; that is, the ability to consider all three methods as permutation, diffusion, and confusion make the proposed method with regards to secure imaging signals and perfect reversibility viable to secure imaging communications outlets in practical employments.

Fig.4. Original, partial encrypted, and hybrid encrypted images, generated using the proposed scheme

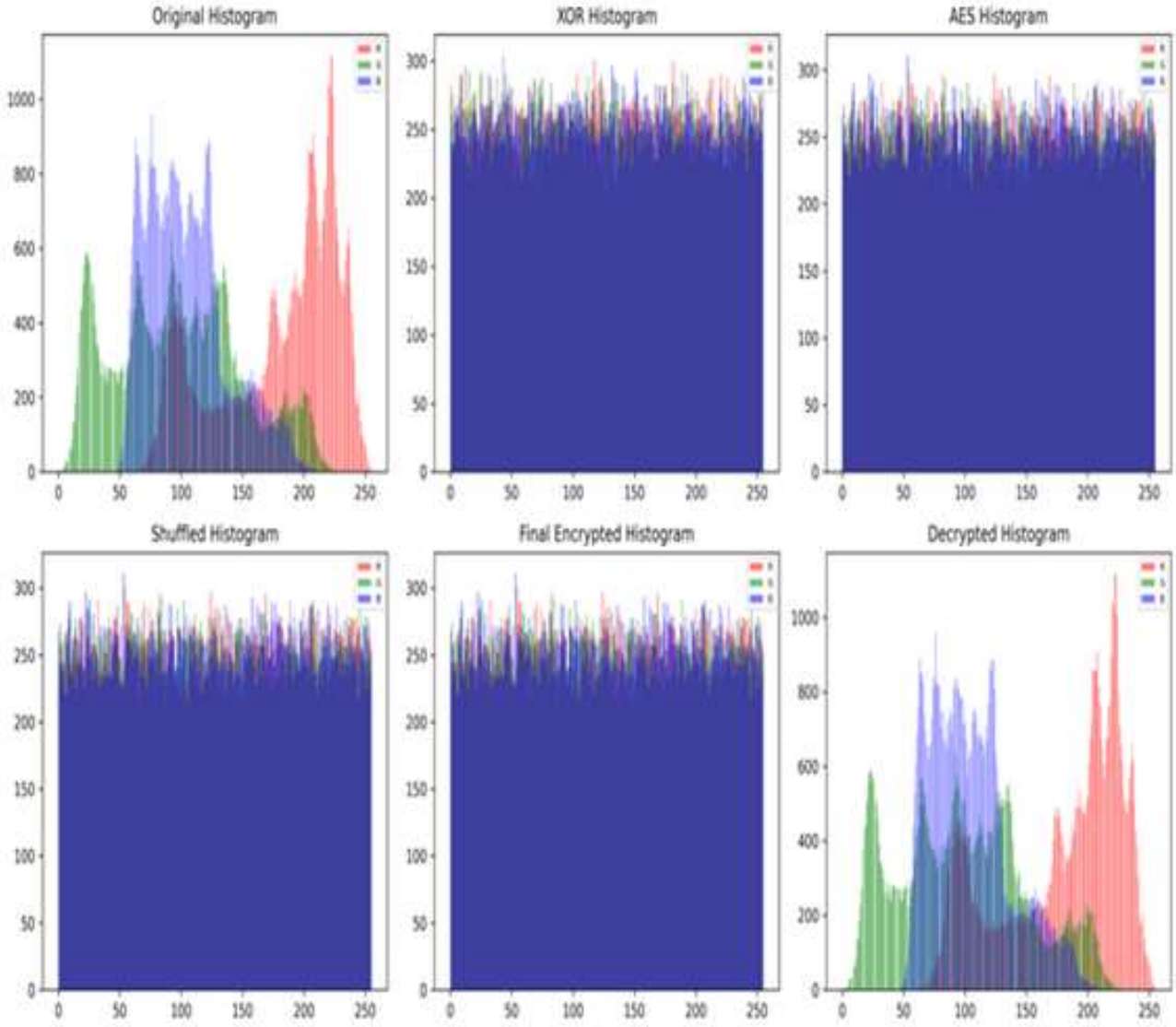

Fig.5. Histograms of RGB channels for the images of the original and encrypted images

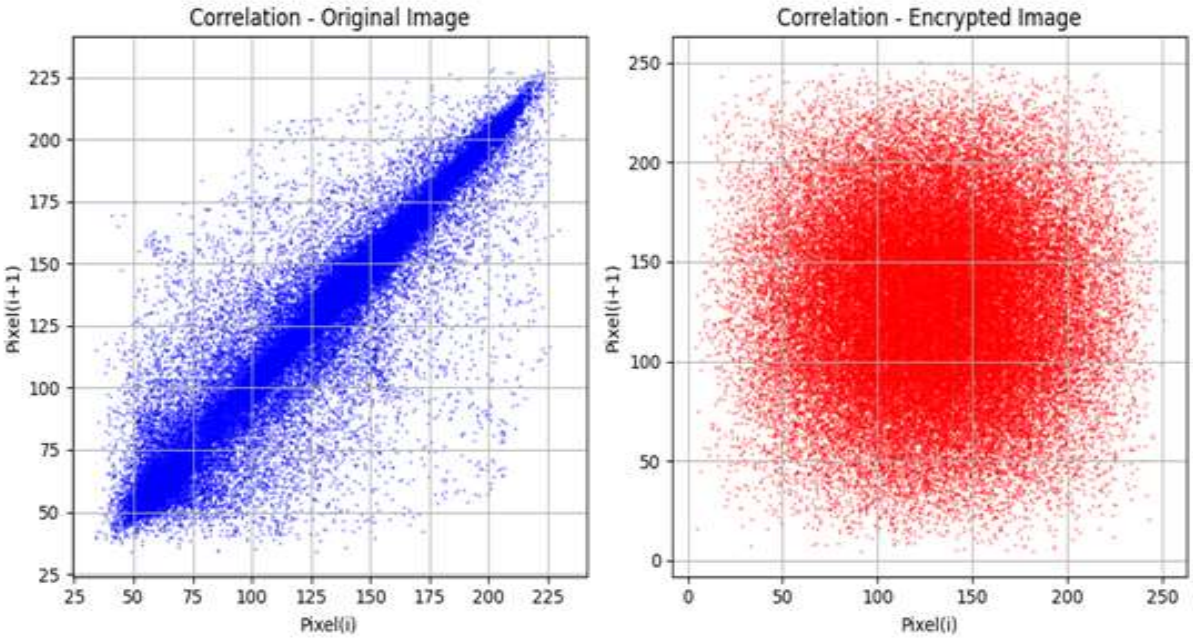

Fig.6. Pixel correlation distribution of the original and encrypted images in horizontal, vertical, and diagonal directions

TABLE 1. RESULTS OF THE STATISTICAL ANALYSIS OF THE PROPOSED HYBRID IMAGE ENCRYPTION SCHEME (ENTROPY, CORRELATION, NPCR, UACI, PSNR).

Image / Metric	Entropy (R)	Entropy (G)	Entropy (B)	Correlation (H)	Correlation (V)	Correlation (D)	NPCR (%)	UACI (%)	PSNR (dB)
Original Image	7.11	7.09	7.08	0.92	0.91	0.89	–	–	∞
XOR Only	7.62	7.60	7.58	0.045	-0.038	0.051	98.12	30.41	–
AES Only	7.83	7.81	7.84	-0.007	0.010	-0.004	98.96	32.12	–
Shuffle Only	7.55	7.56	7.54	0.082	-0.075	0.069	97.45	28.33	–
Hybrid (XOR+AES+Shuffle)	7.98	7.97	7.99	0.003	-0.005	0.002	99.21	33.27	–

Recent image encryption methods are summarized in Table2, including a comparison with our hybrid technique. While most techniques have a base or use of chaos-based permutation and substitution, our approach builds on this process by integrating XOR, AES-128 and shuffling the pixels used, which increases the statistical security significantly. The comparison has shown that the proposed hybrid method obtains higher entropy and robustness (NPCR,UACI) than many of the existing works, which confirm the effectiveness of our method.

TABLE 2. COMPARATIVE OVERVIEW OF SIMILAR IMAGE ENCRYPTION METHODS

Study (Source)	Technique / Algorithm Used	Evaluation Metrics	Remarks
This Work (2025) — *Hybrid XOR → AES-128 → Pixel Shuffling*	Combination of XOR (initial confusion) + AES-128 (robust encryption) + Pixel Shuffling (Permutation)	Entropy (R,G,B), Correlation (H,V,D), NPCR, UACI, PSNR, Chi-square	The proposed hybrid method achieved strong results (Entropy ≈ 7.98, NPCR ≈ 99.21%, UACI ≈ 33.27%), outperforming each algorithm applied individually.
[21]	Chaotic Map + Shuffling (Permutation) + Diffusion	Entropy, Correlation, NPCR, UACI, Histogram	Achieved high entropy and NPCR; however, reliance on chaos-based permutation increases computational complexity and parameter sensitivity.
[22]	Julia & 3D Lorenz Chaotic Maps + Pixel Shuffling + Substitution	Entropy, Correlation, NPCR, UACI	Employed 2D chaotic maps for generating shuffling and substitution. Achieved very strong statistical security.
[23]	Pixel Permutation + Substitution (chaos-driven)	Entropy, Correlation, NPCR (primary)	Effectively reduced pixel correlation; however, lack of standardized cryptographic primitives limits robustness.
[24]	Multilayer Nonlinear Permutation Framework (Permutation + Diffusion)	Entropy, NPCR, UACI	Reported excellent entropy and differential resistance, but employs multiple nonlinear stages that increase processing overhead.
[25]	XOR + Highly Nonlinear S-boxes + Random Permutation	Entropy, Correlation, NPCR, UACI	Achieved strong resistance to statistical attacks; however, security relies heavily on custom S-box design rather than standardized encryption.

Although the Lena image remains a commonly used benchmark in image encryption research, depending solely on a single test image can restrict generalization. It was chosen to enable fair comparisons with previous studies. Future research will broaden the evaluation by incorporating multiple modern images with varied attributes.

Despite this limitation, many current image encryption techniques provide strong security, they frequently depend on resource-intensive chaotic maps or intricate key-generation processes. The proposed hybrid method, however, offers comparable or even enhanced security performance with significantly lower computational demands. By combining lightweight XOR operations with the standardized AES-128 algorithm and straightforward pixel shuffling, this approach achieves an optimal balance. Consequently, this makes the scheme highly practical and well-suited for real-time image encryption applications.

V. LIMITATIONS OF THE PROPOSED APPROACH

The proposed hybrid encryption scheme demonstrates robust security performance; however, certain limitations need to be addressed. Firstly, the experimental evaluation utilized the standard benchmark image (Lena), which, despite being widely used in image encryption research, might not adequately represent the diversity and complexity of real-world images. Secondly, the current implementation is limited to still RGB images of fixed dimensions, leaving the performance on higher-resolution images or video streams unexplored. Additionally, while the method achieves a balance between security and computational efficiency, further optimization could be necessary for resource-constrained environments like IoT devices. Future efforts will focus on expanding evaluations to larger datasets and exploring real-time multimedia applications.

VI. CONCLUSION

In this study, a hybrid framework was introduced for image encryption by merging three separate mechanisms: XOR operation, the AES block cipher, and pixel shuffling. The purpose of combining these methodologies was to provide both confusion and diffusion in the encrypted image and provide greater resistance against statistical and differential attacks. The testing showed that the encrypted images were not recognizable by the eye and quite different from the original input.

Statistical testing indicate the strength of the components of the proposed approach. The values of entropy for the encrypted images were very near the expected entropy value of 8, which demonstrated the pixel values were uniformly dispersed with little information leakage. The correlation coefficients in horizontal, vertical, and diagonal directions were nearing zero or slightly negative values, suggesting the strong correlation between adjacent pixel values was greatly reduced. The high NPCR and UACI values indicated the scheme is sensitive to small changes, which is vital for any scheme to be resistant to differential attack. PSNR values between original and encrypted images were extremely low. The cipher images appeared and were perceptively different from the original, however, upon decryption, the image was able to recreate the original image without any loss of information.

In conclusion, the hybrid XOR-AES-Shuffle encryption system provides a good balance out security and computational efficiency. The ability to reduce pixel correlation, improve entropy, and resist cryptanalysis make the scheme as a secure solution for images in real-time transmission and storage as found in modern multimedia systems. Future work can consider optimizing the scheme for real-time processing and extending the scheme for other applications including video and medical image safeguarding.

REFERENCES

[1] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, vol. 141, pp. 109-124, 2017.

[2] A. M. Khalaf and K. Lakhtaria, "Enhancing Hybrid System Based Mixing AES and RSA Cryptography Algorithms," *Journal of Natural and*.

[3] P. Sarosh, S. A. Parah, and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimedia Tools and Applications*, vol. 81, pp. 7253-7270, 2022.

[4] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *Journal of Supercomputing*, vol. 75, 2019.

[5] V. A. Saeed and B. H. Sadiq, "Image encryption based on AES algorithm and XOR operation," *Academic Journal of Nawroz University*, vol. 12, pp. 533-539, 2023.

[6] N. Ahmed, H. M. S. Asif, and G. Saleem, "A benchmark for performance evaluation and security assessment of image encryption schemes," *International Journal of Computer Network and Information Security*, vol. 8, pp. 18-29, 2016.

[7] A. M. N. Gilmolk and M. R. Aref, "Lightweight image encryption using a novel chaotic technique for the safe internet of things," *International Journal of Computational Intelligence Systems*, vol. 17, p. 146, 2024.

[8] M. Waqas, A. A. Naqvi, and F. Nasim, "A PERFORMANCE AND SECURITY COMPARISON OF HYBRID CHAOS-AES WITH OTHER LIGHTWEIGHT IMAGE ENCRYPTION ALGORITHMS IN RESOURCE-CONSTRAINED PLATFORMS," *Contemporary Journal of Social Science Review*, vol. 3, pp. 1991-2009, 2025.

[9] Z. Alimzhanova, M. Skublewska-Paszkowska, and D. Nazarbayev, "Periodicity detection of the substitution box in the CBC mode of operation: experiment and study," *IEEE Access*, vol. 11, pp. 75686-75695, 2023.

[10] T. X. Meng and W. Buchanan, "Lightweight cryptographic algorithms on resource-constrained devices," 2020.

[11] M. Budiman, J. Tarigan, and A. Winata, "Arduino UNO and android based digital lock using combination of vigenere cipher and XOR cipher," in *Journal of Physics: Conference Series*, 2020, p. 012074.

[12] P. K. Yeng, J. Panford, J. B. Hayfron-Acquah, and F. Twum, "An efficient symmetric cipher algorithm for data encryption," *Int Res J Eng Technol*, vol. 3, pp. 8-9, 2016.

[13] G. Golovko, A. Matiashenko, and N. Solopihin, "Data encryption using xor cipher," *Системи управління, навігації та зв'язку. Збірник наукових праць*, vol. 1, pp. 81-83, 2021.

[14] A. u. S. Muhammad and F. Özkaynak, "SIEA: secure image encryption algorithm based on chaotic systems optimization algorithms and PUFs," *Symmetry*, vol. 13, p. 824, 2021.

[15] M. Nabil, A. A. Khalaf, and S. M. Hassan, "Design and implementation of pipelined and parallel AES encryption systems using FPGA," *Indones. J. Electr. Eng. Comput. Sci*, vol. 20, pp. 287-299, 2020.

[16] A. Bu, W. Dai, M. Lu, H. Cai, and W. Shan, "Correlation-based electromagnetic analysis attack using Haar wavelet reconstruction with low-pass filtering on an FPGA implementaion of AES," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 1897-1900.

[17] M. Brindha, "Multiple stage image encryption using chaotic logistic map," in *2017 international conference on intelligent sustainable systems (ICISS)*, 2017, pp. 1239-1243.

[18] N. Geddada, A. Sahu, and S. Arora, "Hybrid Image Encryption for WISN in Privacy Protection and Security of Public Big Data Using Chaotic Maps," in *2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE)*, 2024, pp. 1-5.

[19] B. Stimpel, *Multi-modal Medical Image Processing with Applications in Hybrid X-ray/Magnetic Resonance Imaging*: Friedrich-Alexander-Universitaet Erlangen-Nuernberg (Germany), 2021.

[20] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons & Fractals*, vol. 95, pp. 92-101, 2017.

[21] X. Jin, X. Duan, H. Jin, and Y. Ma, "A novel hybrid secure image encryption based on the shuffle algorithm

and the hidden attractor chaos system," *Entropy*, vol. 22, p. 640, 2020.

[22] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map," *Entropy*, vol. 22, p. 274, 2020.

[23] S. Anwar and S. Meghana, "A pixel permutation based image encryption technique using chaotic map," *Multimedia tools and applications*, vol. 78, pp. 27569-27590, 2019.

[24] C. İnce, K. İnce, and D. Hanbay, "A multilayer nonlinear permutation framework and its demonstration in lightweight image encryption," *Entropy*, vol. 26, p. 885, 2024.

[25] F. Artuğer, "Innovative image encryption approach based on bitwise XOR high nonlinear S-boxes and random permutation," *Soft Computing*, vol. 29, pp. 2891-2903, 2025.