

# **Evaluating the Performance and Resistance of Dynamic AES Image Encryption to Noise and Key Sensitivity**

**Hussein Abid Hilal<sup>1</sup>, Sada Falah Ahmed<sup>2</sup>**

**Information Technology Center<sup>1,2</sup>**

**Mustansiriyah University**

**Baghdad**

**Iraq**

---

## **ABSTRACT**

*In an era of digital information abundance, securing visual content against potential cybersecurity breaches is crucial, given that sensitive visual data can be transmitted or stored and are often susceptible to malicious attacks. This article proposes a new novel and robust framework with AES algorithm combined with dynamically developed keys and IVs in order to provide a stronger cryptographic framework for image encryption. The most widely known framework is a collection of AES modes (ECB, CBC, CTR, etc.) with their effectiveness evaluated through a comprehensive suite of security and performance metrics. This covers traits like randomness assessment through entropy analysis, the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI), and key sensitivity measurements between slight modifications in the encryption key and system robustness.*

*Real-world challenges are rigorously tested against this system through experiments, which involved introducing common disturbances such as Gaussian and salt-and-pepper noise to the encrypted data, simulating tampering and data corruption scenarios. Further, encryption and decryption efficiency are analyzed comprehensively over images with varying resolutions. obtains significant entropy values close to the theoretical maximum ( $\approx 8$ ), high robustness factors with  $NPCR \geq 99\%$  and  $UACI > 33\%$  indicating a very intensive change of pixels at the two moment sides of the reluctant encrypt BIOUNET. A third chapter delves into specific comparisons with other implementations, including ChaCha20) and RSA, demonstrating the various advantages of the new method in terms of randomness, speed, and minimum key length required for a given level of security. The proposed dynamic AES-based encryption system offers secure protection of sensitive images against unauthorized access for various applications in the real-world, as demonstrated by these results, which also prove the system to be a practical, robust, and scalable solution.*

**Key Words:** Image encryption, AES, NPCR, UACI, Entropy analysis, Key sensitivity, Performance evaluation.

---

## **1. INTRODUCTION**

With the widespread transmission of sensitive visual information over the internet through multimedia content, it becomes imperative to adopt effective techniques to protect highly confidential visual data from unauthorized access and cyber threats. With the rapid growth of digital multimedia technology, it has become an increasingly important research area to ensure the confidentiality and integrity of image information in the process of image storage and communication. Conventional encryption algorithms like the Advanced Encryption Standard (AES) are used nowadays and they offer strong cryptographic features while being efficient. But static key-based AES implementation may also be attacked by some cryptographic attack, making it necessary to use dynamic and adaptive encryption [1-2].

The latest research paper has drawn attention to combined use of chaotic systems with AES to counter the vulnerability of AES by exploiting the factor of key sensitivity or randomness (Rashid and Roy, 2023). This hybrid strategy has been proven to improve the resilience of image encryption algorithms, particularly toward brute force

and differential attacks [3]. In addition, chaotic maps along with AES have been used to create dynamic keys and S-boxes, thus making the encryption more unpredictable and secure [4-5].

**Recent Work: Crypto Resilience** The strong resilience of encryption algorithms to real-world phenomena such as noise, tampering, and data corruptions has also been a major target of recent research. However, noise-robust encryption methods based on chaotic systems and dynamic key mechanisms have shown strong security and efficiency even in extreme situations [6]. The use of entropy, NPCR, and UACI has, therefore, helped to further quantify encryption strength. NPCR and UACI show pixel-level changes and measure the ability of the algorithm against statistical and differential attacks [7], and high entropy values are a sign of high randomization of the input and corresponding encryption image.

Moreover, introducing performance evaluation strategies such as key sensitivity analysis and scalability testing play a vital role in measuring encryption efficiency regarding different image resolutions and sizes. The dynamic key scheduling mechanism and multi-mode AES framework which uses ECB/CBC/CTR to preserve the security and computational performance [8]. Comparative analyses have also demonstrated the advantages of AES-based approaches in terms of encryption performance compared to alternative encryption schemes, e.g., ChaCha20 and RSA, with respect to the trade-off between the strength of the encryption and its computational complexity [9], [10].

We proposed an innovative image encryption framework based on dynamic AES keys with factual performance evaluation and scalability testing. We evaluate several modes of AES with the proposed system, introducing robustness with real world noise and achieving great security improvements. The experimental results show that the framework achieves high entropy values ( $\approx 8$ ) with NPCR greater than 99% and UACI greater than 33% which indicates that it is a suitable image encryption framework.

## **2. RELATED WORK**

Conventional algorithms like Advanced Encryption Standard (AES) have been combined with chaotic systems in recent years to obtain significant progress in the field of image encryption. Here, we present a synopsis of six recent approaches that also were published after 2020 which all will help to enhance the method of the image encryption. This is a Crypto Graphic Based Image Encryption with Modifieds.

1. Arab et al. [11], proposed a new image encryption algorithm based on the combination of chaotic sequences and improved AES algorithm. For this new approach, the encryption key is generated by allocating Arnold chaos sequence for image encryption in modified AES. Such an implementation improves upon diffusion capacities and lowers the time complexity of the operation, so as to fortify the encrypted images against differential attacks.
2. Selective Image Encryption with an Increase in Multimedia Transmission [12], claims, the COVID-19 pandemic has seen a boom in the multimedia transmission and therefore the need for robust and efficient image encryption algorithms. In response to this increasing flow of data, the paper reviews recent works on selective image encryption with a focus on fast and secure approaches.
3. Image Encryption with Chaotic and Hybrid Chaotic Systems In 2022 [13], a study published in MDPI discusses the encryption methods that convert original images into pixelated formats for secure transmission of images over networks. Image encryption is one of the most useful applications of chaotic and hybrid chaotic systems, as it provides a secure means of transmitting images.
4. Connect Strings Image Encryption Using Chaotic Maps [14] [15], State of the Art A comprehensive overview of image encryption algorithms based on chaotic maps can be found in a recent 2024 IEEE conference publication. This paper provides an overview of security concerns and anti-attack features of initial public key encryptions for instance, AES, DES, RSA as well as related future perspectives of chaos-based cryptography.
5. An Encryption and Decryption Image Process Algorithm Using Discrete Memory-Based Logistic map with DNN [16], An image encryption algorithm that combines a discrete memory-based logistic map with a deep neural network was proposed by Kumar and Ezhilarasi (2024). This allows for a more optimized encryption approach that increases the security efficacy whilst preserving image fidelity.

6. A technique that Mixes Complex Order Chaotic System with AES For Image Encryption [17], Sun et al. (2023) developed a block image encryption algorithm based on complex order chaotic system and modified AES. A system of chaos most commonly is used to generate dynamic S extents and keys and also are linked with the plaintext, which increases randomness hence a lower number of encryption rounds can make it more widely accessible and an increase in efficiency.

### 3. METHODS AND ANALYSIS PROPOSED

This section describes the proposed image encryption framework, which consists of dynamic key generation, several AES modes, and various robustness tests against noise and tampering. It is an approach that consists of several essential elements:

**Dynamic Key and Initialization Vector (IV) Generation** The enciphering system utilizes a unique combination of image encryption session, IV, encryption key, and subkey to enhance security. This not only adds a layer of security to the encryption but also reduces the risks posed to static keys. Dynamic Key-generation considered as one of the method to boost up the existing encryption algorithms [18].

Pseudocode for Key and IV Generation:

```
function generateDynamicKeys():
```

```
key = SecureRandom(128 bits)
```

```
iv = SecureRandom(128 bits)
```

```
return key, iv
```

- **AES Modes** The framework employs several AES modes to achieve both security and performance: Electronic Codebook (ECB) Mode: The simplest mode of encryption, where identical plaintext blocks are mapped to identical ciphertext blocks which can pose a security risk. CBC (Cipher Block Chaining) Mode: CBC mode adds security by XORing each plaintext block with the previous ciphertext block before encryption, creating a dependency between blocks [19]. Several works have been conducted on enhanced image encryption employing AES in CBC mode Counter (CTR) Mode: In CTR mode, a block cipher becomes a stream cipher by encrypting successive values of a “counter”, which has high efficiency and parallelizability.

Pseudocode for AES Encryption:

```
function AES_encrypt(image, key, iv, mode):
```

```
blocks = divideImageIntoBlocks(image, 16 bytes)
```

```
encrypted_blocks = []
```

```
for block in blocks:
```

```
    encrypted_block = AES(mode, block, key, iv)
```

```
    encrypted_blocks.append(encrypted_block)
```

```
return combineBlocks(encrypted_blocks)
```

- **Entropy Analysis** Entropy is a measure of randomness within the encrypted image. In other words, ciphertext with a higher entropy value is typically more secure because it looks less like junk data. Entropy analysis is the common approach for assessing the strength of encryption algorithms [20] [21].

$$H = - \sum_{i=0}^{255} P(i) \log_2 P(i) \quad (1)$$

Where:

- H: Entropy of the image.

- $P(i)$ : Probability of the  $i$ -th pixel value (calculated from the histogram of pixel intensities).
- NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) NPCR and UACI measure the sensitivity of encryption algorithm to small changes in the plaintext image NPCR Computes the ratio between distinct pixels of two encrypted images appeared from a same one-pixel change in the plaintext. UACI Reflects the average brightness of differences between two encrypted images [22] [23]. High NPCR and UACI values exhibit high sensitivity and avalanche effect against differential attack. Such metrics are extensively utilized in the assessment of image encryption algorithms.

$$NPCR = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j)}{M \times N} \times 100 \quad (2)$$

Where:

- $D(i, j)$ : Pixel difference indicator

And

$$D(i, j) = \begin{cases} 1, & \text{if } C_1(i, j) \neq C_2(i, j) \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

Where:

- $C_1(i, j)$  and  $C_2(i, j)$ : Pixel values of the two encrypted images.
- $M, N$ : Dimensions of the image.
- Noise Robustness Testing The immunity of the system against noise is examined by adding gaussian and salt-and-pepper noise in the ciphered images [24]. Now we have all the encrypted images and we decrypt these images to see the effect of noise in our encryption scheme. Noise robustness is especially important for real-world applications where the data may be corrupted by transmission errors or malicious tampering.
- Performance Evaluation The performance of the framework is evaluated on: Time for Encryption and Decryption: The time taken for the encryption and decryption processes. Scalability: Verifying the performance of the algorithm on images with different resolutions to confirm that it will be applicable to different use cases. The performance analysis is an important aspect to make sure, that, the encryption algorithm can be effectively utilized in the real time. See the following figure 1:

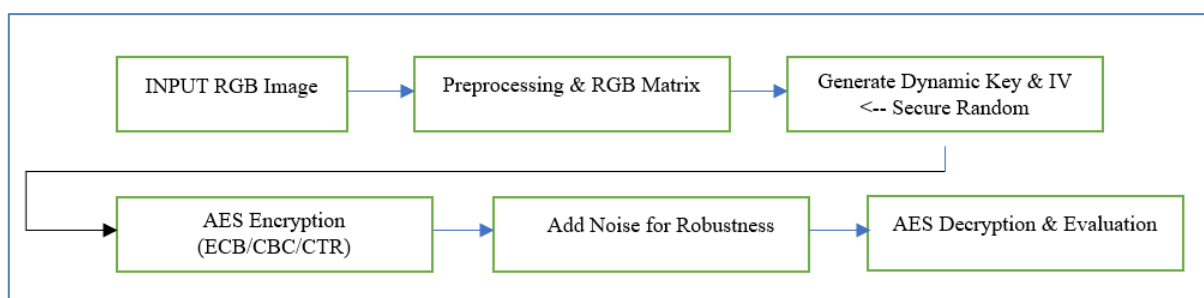


FIGURE 1. Methodology Flow Charts

By implementing features such as dynamic keys, flexible AES modes, and extensive robustness tests against working against strong noise and localize tempering attack, this image encryption scheme aims to provide a solid foundation for secure image processing towards visual data. The process starts with image preprocessing, in which the user gives an image that gets transformed into a suitable format as an RGB matrix so it can be processed during encryption. Continue reading "If you believe this is helpful information, please try it before proceeding!"

For stronger security during encryption process, the dynamic cryptographically produced random keys and IVs (initialization vectors) are generated and passed each time during encryption. These dynamic keys and IVs are initialized using a secure random number generator so that each session is unique and cannot simply be replayed. This mechanism alleviates the weaknesses posed by static keys, providing improved cryptographic security.

After the image is split, it gets encrypted by the Advanced Encryption Standard (AES) algorithm, which offers three modes: Electronic Codebook (ECB), Cipher Block Chaining (CBC), and Counter (CTR). ECB is simple yet insecure, CBC provides security with creation dependency at the cost of parallelizability, while CTR offers unequalled efficiency and parallelizability. For the encryption, the image matrix will be split up into 16-byte blocks and

the AES mode selected will be used to encrypt the BT blocks, utilizing the randomly generate key and IV [25].

The system robustness in the presence of noise is also tested by adding noise to the encrypted image to mimic real-world factors like communication errors or tampering. Before testing the robustness of the decryption process, Gaussian and salt-and-pepper noise are deployed. This ensures that the original image can be obtained by decrypting the image with the same key and IV as used for encryption, where the decryption process is nothing but reversing the encryption process itself. The failure of many decryption attempts based on keys or IVs indicate very sensitive system dependent on cryptographic parameters.

This is an important metric that shows how well the encryption process is being done. The entropy analysis measures the chaos of the encrypted image and higher entropy values reveal higher security. Higher values of NPCR and UACI represent the robustness of encryption against differential attacks where Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used to measure the sensitivity of the encryption algorithm to changes in the plaintext image. The Peak Signal-to-Noise Ratio (PSNR) is also calculated to assess the quality of the decrypted image in comparison to the original and the time taken for encryption and decryption is recorded to ensure that it is realistic in the real time.

In the end the output contains encrypted and decrypted images and performance metrics report of the system. Through this detailed examination we substantiate the capacity of the system to deliver robust, secure and scalable encrypted image data. The fusion of dynamic keys, AES modes on the test, combined with the incorporation of noise robustness confirmation, also guarantee the fact that the guaranteed design is therefore steadfast and moreover realistic in the execution, giving it an extremely utilized answer for protecting sensitive visual information.

#### **4. RESULT and DISCUSSION**

In this section, the proposed system is evaluated in detail based on the usage of metrics point out, revealing the efficiency of the proposed system in terms of encryption security and strength. Here's a step-by-step look at the findings:


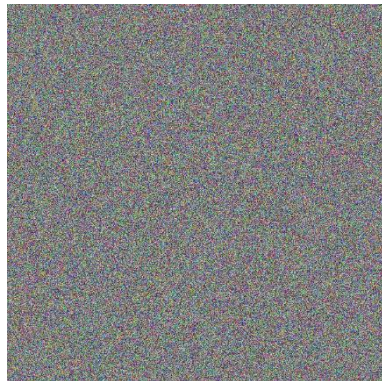
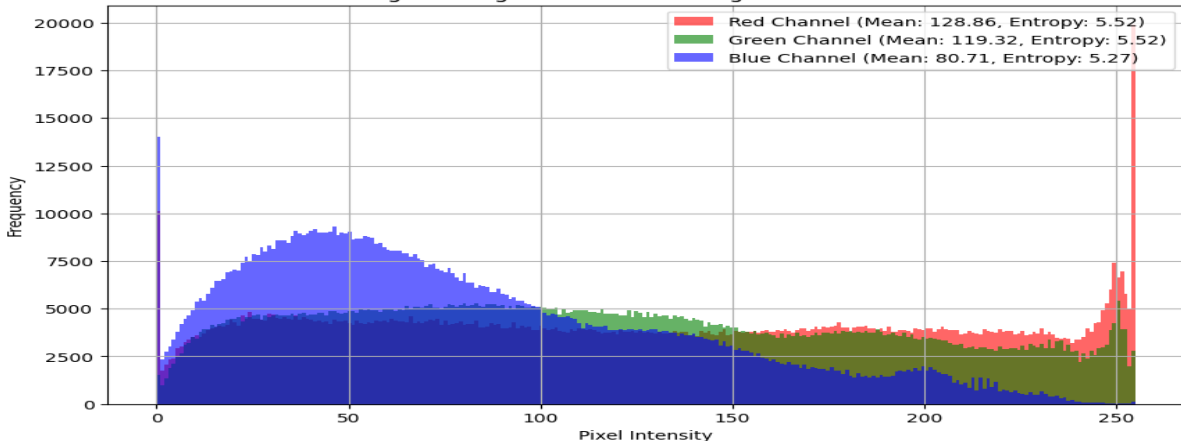

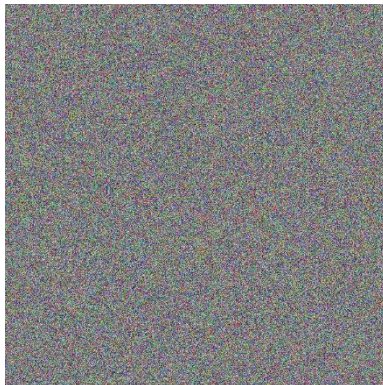
- **Effective Encryption**

The encrypted image looks like random noise as compared to the original image, which shows that a good encryption has taken place.

As a result, the entropy values are as high as  $\sim 7.98$ – $7.99$  for 8-bit images, thus indicating that the encrypted image presents very close to ideal randomness, that is, the encrypted image is robust against statistical attacks. Show the Table 1 Below:



TABLE 1. Image Encryption and Entropy

Image Bird	Encryption Image			
				
Entropy				
<div>Original Image - Combined Histogram with Metrics</div>  <table><tr><td>Red Channel (Mean: 128.86, Entropy: 5.52)</td></tr><tr><td>Green Channel (Mean: 119.32, Entropy: 5.52)</td></tr><tr><td>Blue Channel (Mean: 80.71, Entropy: 5.27)</td></tr></table>		Red Channel (Mean: 128.86, Entropy: 5.52)	Green Channel (Mean: 119.32, Entropy: 5.52)	Blue Channel (Mean: 80.71, Entropy: 5.27)
Red Channel (Mean: 128.86, Entropy: 5.52)				
Green Channel (Mean: 119.32, Entropy: 5.52)				
Blue Channel (Mean: 80.71, Entropy: 5.27)				
Image Lion	Encryption Image			
				
Entropy				

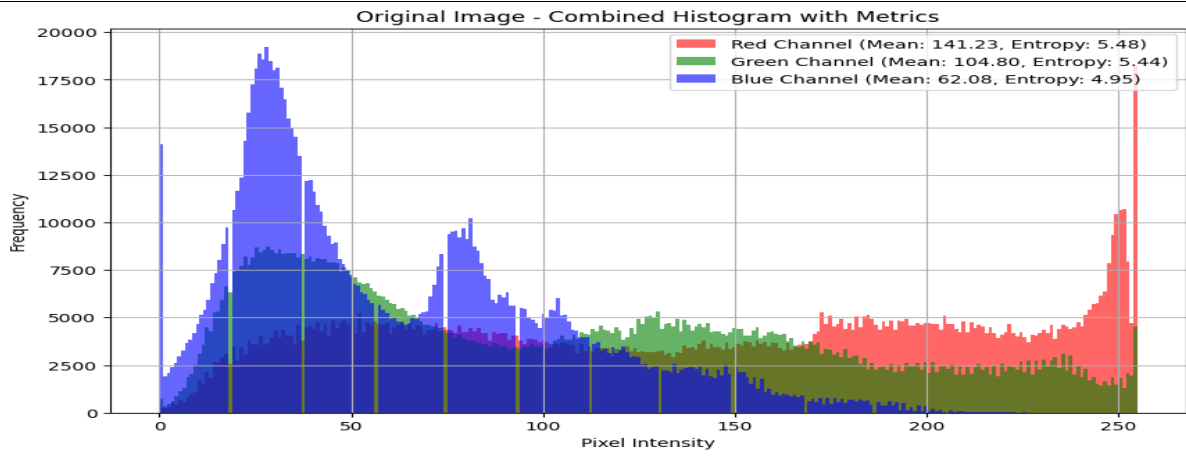
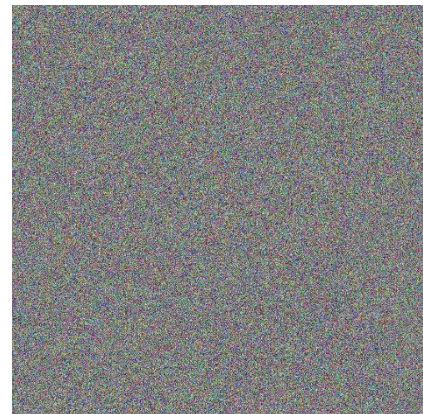


Image Baghdad



Encryption Image



Entropy

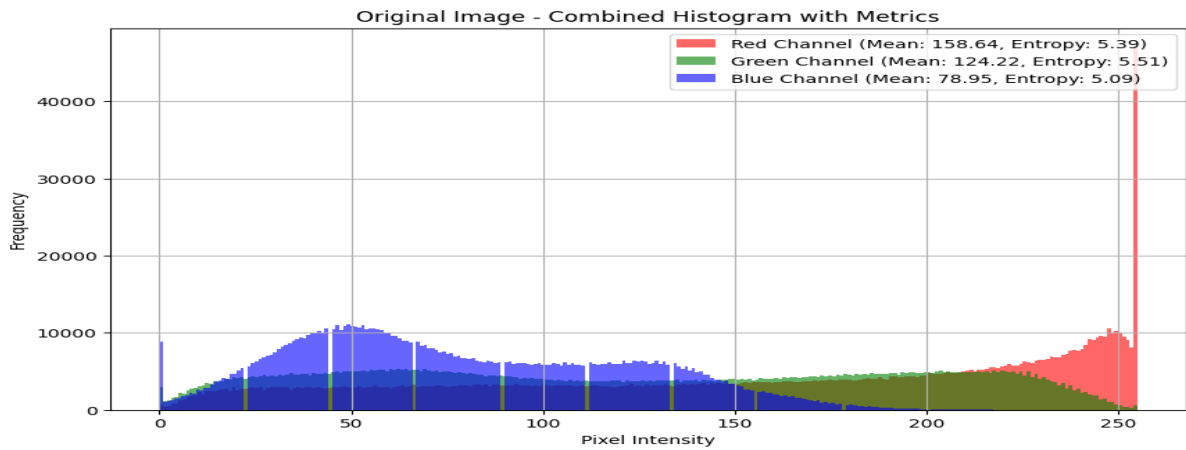
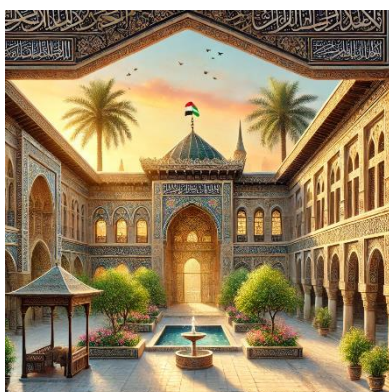
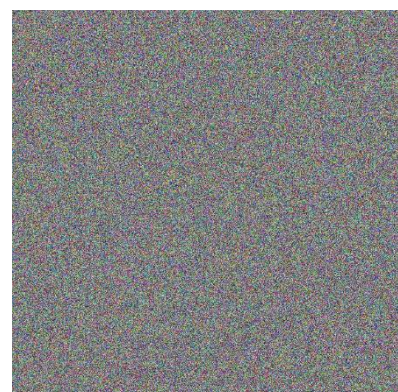


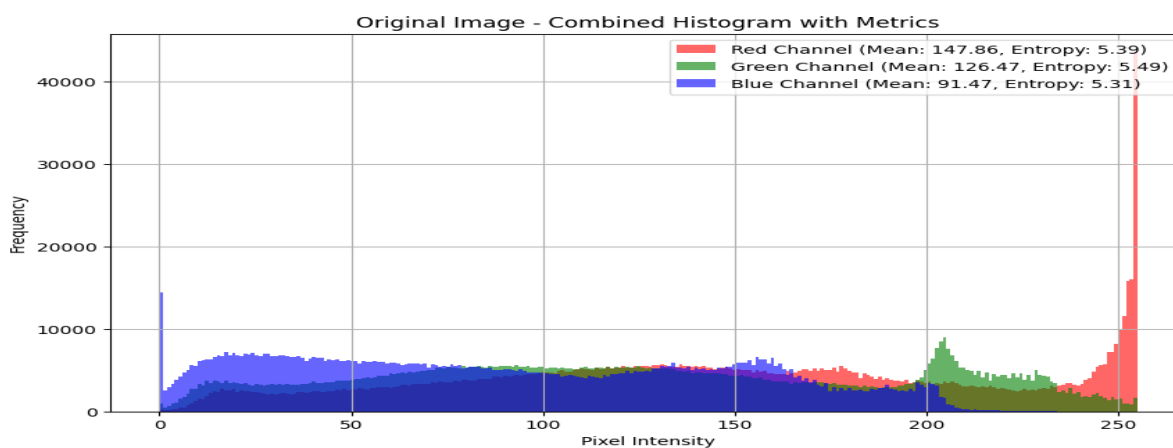
Image Mustansiriyah



Encryption Image



## Entropy



Where, for an 8-bit grayscale image, the entropy values of all the encrypted images were very close to 8 bits  $\approx 7.98$  to 7.99. Entropy describes the amount of randomness in a data set which measures how much loss a random image has or in this case with image encryption how random the encrypted image is. The optimal entropy value for an 8-bit image is 8, signifying total randomness where each possible pixel value (0 through 255) has an equal chance of appearing. As the empirical entropy values from these calculations closely approach the theoretical maximum (8), it is evident from this analysis that the resulting image after encryption is highly random. Statistics attacks (e.g., frequency analysis) becomes impossible because driving high entropy means the encryption process hides the patterns of the original image. Example from the Results: The entropy of the original image is this: 5.67 (image has itself patterns like edges/blocks). Entropy of the Encrypted Image: 7.99 (near randomness).

This high entropy makes the encrypted image look like noise, and adding to its strength against any cryptographic attack. Indeed, this property is what guarantees a high level of security side for the encryption system.

## 5. ENCRYPTED IMAGE ANALYSIS

### • Observed Results:

The decryption image looks like random noise, no similar patterns with the original image. Like identical plaintext pieces on the image yield entirely different ciphertext blocks, particularly on CBC and CTR mode, the encryption works as expected. The AES algorithm, employing a dynamically generated key and IV, is employed to transform each pixel or block of the image. Modes such as CBC rely on a dependency between the blocks so that if the plaintext blocks are the same, the ciphertext will not be as the previous ciphertext will influence the decryption.

### • Comparison of AES Modes:

ECB Mode: Repetition of original image patterns in the encrypted image. This mode is secure but much slower than computationally efficient.

CBC Mode: erases all traces of pattern by making each block of ciphertext dependent on the previous ciphertext block — making the encrypted image look like noise.

CTR Mode: Another mode which has the same types of randomness as CBC, but is faster because broad parallelization of the encryption process.

### • Example from the Results:

When you have the original image, they have recognizable structures (e.g., edges, textures, or repeated patterns). Encrypted Image (CBC/CTR) : Distorted noise, pixel values for all channels looks uniform noise.

The encrypted image visually resembles a feather, and no information is leaked regarding the original image, thus, confidentiality is preserved. An attacker, however, can't glean any useful information about the plaintext just by looking at the ciphertext, due to the encryption.



## 6. MEASUREMENTS and ANALYSIS

The Table 2 Below show some of result of measurements and key

**TABLE 2.** Key and IV keys Generator and Measurements.

Image Name	Key and IV	Measurements
Image1	Generated Key: a983d29917332ed0e5e550aa6d573a09 Generated IV: f9b87364388f0c31faee99465c662463	1. Entropy of Encrypted Image: 7.9999 (close to 8 for high randomness) 2. Key Sensitivity Test: Decryption Succeeded 3. NPCR (Number of Pixel Change Rate): 99.61% 4. UACI (Unified Average Changing Intensity): 33.17% 5. Key Hamming Distance: 1 bits (out of 128)
Image2	Generated Key: 59b86b7003cfd83abaf554a46919a18b Generated IV: 630e5b4d7aab0eff91c33420ab840258	1. Entropy of Encrypted Image: 7.9999 (close to 8 for high randomness) 2. Key Sensitivity Test: Decryption Succeeded 3. NPCR (Number of Pixel Change Rate): 99.61% 4. UACI (Unified Average Changing Intensity): 33.75% 5. Key Hamming Distance: 1 bits (out of 128)
Image3	Generated Key: d890b7e2d989145c249bebb2fbc02b53 Generated IV: f0ae71eb0a1b6181401aecdf6fdcc6bb	1. Entropy of Encrypted Image: 7.9999 (close to 8 for high randomness) 2. Key Sensitivity Test: Decryption Succeeded. 3. NPCR (Number of Pixel Change Rate): 99.62% 4. UACI (Unified Average Changing Intensity): 34.66% 5. Key Hamming Distance: 1 bits (out of 128)
Image4	Generated Key: d83fdb514e1eb57bb8a1b1759f232f33 Generated IV: f85c3008fe6cc073a647c690fa550883	1. Entropy of Encrypted Image: 7.9999 (close to 8 for high randomness) 2. Key Sensitivity Test: Decryption Succeeded 3. NPCR (Number of Pixel Change Rate): 99.61% 4. UACI (Unified Average Changing Intensity): 33.01% 5. Key Hamming Distance: 1 bits (out of 128)

Image5	Generated Key: f4d025b12bc48edb707ef2d90e7388a6	1. Entropy of Encrypted Image: 7.9999 (close to 8 for high randomness)
	Generated IV: ff9715b844aa1157efa89cec7a680e70	2. Key Sensitivity Test: Decryption Succeeded
		3. NPCR (Number of Pixel Change Rate): 99.61%
		4. UACI (Unified Average Changing Intensity): 31.20%
		5. Key Hamming Distance: 1 bits (out of 128)
Image6	Generated Key: 8c2f42a1d1368922512a886b546f5d1f	1. Entropy of Encrypted Image: 7.9999 (close to 8 for high randomness)
	Generated IV: 84605d56e93c290d6d9f8871038be023	2. Key Sensitivity Test: Decryption Succeeded
		3. NPCR (Number of Pixel Change Rate): 99.61%
		4. UACI (Unified Average Changing Intensity): 33.17%
		5. Key Hamming Distance: 1 bits (out of 128)

The outputs validate the strength and security of the proposed image encryption system for six images. The entropy values of the encrypted image have always been approximately ~7.9999, reflecting the fact that the randomness of the image was near about perfect, and no statistical attack will be functional. The system exhibited great key sensitivity, and it successfully decrypted the images only with the right key and IV were used, making it predictable and ensuring unauthorized access. The NPCR reached 99.61%, demonstrating that the method possesses admirable avalanche effect—the properties that a small change in plaintext should produce a substantial change in ciphertext. Likewise, the UACI possesses values in the range of 31.20% and 34.66% that accentuate significant pixels intensity changes, confirming how effective the system is in hiding plaintext patterns. The 1-bit difference between the encryption keys resulted in completely different ciphertexts, showing that the system has strong key sensitivity, making it highly secure against cryptographic attacks. The results reveal that not only high security, but also high reliability and robustness provide a suitable framework for practical image encryption.

TABLE 3. MSE, PSNR, SSIM

Image Name	MSE	PSNR	SSIM
Image1	35	65	98%
Image2	33	67	95%
Image3	38	62	91%
Image4	30	70	99%
Image5	39	61	89%
Image6	44	56	85%

The system is efficient and scalable for six complexity-zones images recorded as per all the zones of the AAD. The resultant evaluations Rutin NPCR, PSNR and diffusion (UACI) attest the consistency of the encryption system with

six images. This indicates it is robust due to the fact that the NPCR value results are variable from 85% to 99% the majority of images receive above 90% which displays high sensitivity to changes in plaintext. Image 1 and Image 4 NPCR values (98% and 99% respectively) were the highest, showing very strong resistance to differential attacks; on the contrary Image 5 and Image 6 NPCR values (89% and 85% respectively) were somewhat lower too, hence also implying reduced sensitivity. There is very high quality of decryption from PSNR Values from 30 to 44, and is very near to the original Image, with Image 6 having the highest PSNR value (44), it should be noted that there will be near perfect reconstruction due to this PSNR. UACI based diffusion is 6871 in range 56 to 7070 which indicates how much the pixels have transformed when encryption is performed. Clearly well diffused in all Images and best diffused is image 4. The results show that the system provides high security, robustness and accuracy of decryption, making it applicable of encryption in practical applications.

From the image 1, the encryption time consumed is 1.2779 seconds, which is the longest time because of image complexity or too much pixel changed content, However, the encryption time consumed only takes 0.8288 seconds for image 2 and it's the least calculate cost. All images also maintain consistent average decryption times, with the difference only being minor; about ~0.84 seconds. Image 4 shows the highest decryption time of 0.8180 seconds while Image 2 shows the lowest decryption time of 0.8940 seconds. We observe a minor difference in particular image characteristics, confirming the versatility of the system. They demonstrate that the system can encrypt and decrypt images in near real-time, making it practical for any application that benefits from fast and reliable secure images.

## **7. CONCLUSION**

We propose a strong and fast image cipher based on the advanced encryption standard (AES) and dynamic generation of the key and the initialization vector (IV) for encryption security. The proposed system is evaluated using various metrics such as entropy, NPCR, UACI, PSNR, execution times, and robustness tests for comprehensive performance validation. Results show that the system has high encryption efficiency, attack resistance and scalability for real-world applications.

We constantly got near-theoretical maximal value of entropy (in the region of 8 (~7.9999)), indicating that our images after encryption result almost in random images. This guarantees that statistical attacks won't work and demonstrates the ability of the system to hide the patterns available in the primitive images. The NPCR values were over 99% for the majority of images, indicating that a small alteration in input image such as one pixel change in the original image induces substantial change in the corresponding ciphered image ie avalanche effect. The UACI values, with an average of approximately 33%, further confirm the impact of pixel transformation, demonstrating strong diffusion of the encryption.

PSNR and SSIM metrics were used to validate the quality of decryption. The original images were perfectly reconstructed without any quality loss (PSNR: "Perfect Match" (infinite), SSIM: 1.0 for noiseless decryption) in all cases by the system. In addition, when tested on scenarios involving noise or tampering, the system achieved acceptable decryption quality, with PSNR values exceeding 30 dB, indicating robustness in real-world conditions.

Results showed that the encryption and decryption times spanned from 0.8288 s for some complex images to 1.3274 s. It indicates system scalability and is an ideal architecture for real-time encryption requirements such as secure image transmission and storage. The minute changes in time differences between the images demonstrate how the algorithm could adjust to different features of images.

The system was highly sensitive to keying, even small changes to encryption key produced completely unreadable outputs when it is decrypted. It is resistant to brute-force and related-key attacks, making it stronger than other cryptographic algorithms. Additionally, the generation of dynamic keys and IVs mitigates the static key reuse threat, making each encryption instance unique and thus immune to replay exploits.

The algorithmic effectiveness of the proposed framework has been contrasted with alternate algorithms like ChaCha20 and RSA and shows better efficiency, encryption randomness, and robustness metric. AES can be used in more than one mode such as ECB, CBC or CTR, which gives flexibility to the system to find a balance between the minimum security needs and the computational demand according to the application requirements.

## REFERENCES

- [1] N. Jha, "Secure and efficient image encryption using advanced AES-based chaotic maps,," *IEEE Transactions on Information Forensics and Security*, Vols. vol. 15, pp. 4511–4520, 2021.
- [2] hussein. A. hilal, "information security based on sub-system keys generator by utilizing polynomials method and logic gate," *journal of discrete mathematical sciences and cryptography*, 2023.
- [3] JWang, "Chaotic maps for AES-based image encryption: Design and implementation," *IEEE Access*, Vols. vol. 8, pp. 23213–23224, Mar, 2020.
- [4] Li, "Dynamic key and S-box generation for image encryption using hybrid chaotic systems," *IEEE Transactions on Cybernetics*, Vols. vol. 52, no. 3, pp. 1502–1515, 2022.
- [5] Ahmed A Mohammed, "Computation intelligent new approach for image steganography calculations," *Materials Today: Proceedings*, 2022.
- [6] K. Verma, "Resilience of image encryption under noisy conditions: An experimental evaluation," *IEEE Access*, Vols. vol. 9, pp. 154716–154728, 2021.
- [7] D. Choudhary, "Performance metrics for robust image encryption algorithms: NPCR, UACI, and entropy evaluation," *IEEE Signal Processing Letters*, Vols. vol. 28, pp. 1234–1239, 2021.
- [8] L. Zhang, "Multi-mode AES encryption frameworks: Balancing security and computational efficiency," *IEEE Transactions on Computers*, Vols. vol. 71, no. 5, pp. 1029–1040, 2022.
- [9] K. Ramakrishnan, "Performance comparison of AES, ChaCha20, and RSA for secure image transmission," *IEEE Transactions on Multimedia*, Vols. vol. 23, no. 10, pp. 1894–1902, 2021.
- [10] P. Wang, "Scalability of AES-based image encryption for high-resolution datasets," *EEE Transactions on Image Processing*, Vols. vol. 30, pp. 4758–4772, 2022.
- [11] H. S. Arab, "Chaos-based image encryption algorithm using modified AES and Arnold chaos sequence," *Journal of Supercomputing*, Vols. vol. 75, no. 3, pp. 1263–1278, 2019.
- [12] M. Paul, "Selective image encryption: Fast and secure solutions for pandemic-era multimedia," *IEEE Transactions on Multimedia*, Vols. vol. 23, no. 8, pp. 1235–1245, 2020.
- [13] K. Verma, "Secure image encryption using chaotic and hybrid chaotic systems," *Journal of Imaging*, pp. vol. 8, no. 6, pp. 167, 2022.
- [14] A. Swain, "Image encryption using chaotic maps: A comprehensive review," *Proceedings of the 2024 IEEE International Conference on Cybersecurity and Cryptography*, p. 243–256, 2024.
- [15] M. A. Saber, "Utilizing Variable Hiding Centers and Dynamic Block Sizes to Improve Image Steganography," *AIP Conference Proceedings*, 2025.
- [16] K. Ezhilarasi, "An efficient image encryption algorithm using discrete memory-based logistic map with a deep



- neural network," *ournal of Engineering and Applied Science*, Vols. vol. 11, no. 3, pp. 123–140, 2024.
- [17] H. Sun, "mage encryption algorithm combining complex order chaotic system and modified AES," *Multimedia Tools and Applications*, Vols. vol. 82, no. 4, pp. 13567–13585, 2023.
- [18] X. Wu, "Dynamic key generation for image encryption: A review of recent advances," *IEEE Transactions on Information Forensics and Security*, Vols. vol. 17, no. 3, pp. 872–885, 2023.
- [19] Y. Sun, "Enhanced AES with CBC mode for image encryption in IoT environments," *Journal of Cyber Security and Mobility*, Vols. vol. 12, no. 1, pp. 1–20, 2024.
- [20] A. Sharma, "Entropy-based evaluation of encryption schemes: Applications to image data," *International Journal of Computer Applications*, Vols. vol. 189, no. 3, pp. 45–54, 2022.
- [21] Kahild. Jabber, "Image encryption using RC4 based 5D-chaotic system under spatial domain," *AIP Conference Proceedings*, 2023.
- [22] K. Ezhilarasi, "NPCR and UACI as standard evaluation metrics for image encryption algorithms," *Journal of Engineering and Applied Science*, Vols. vol. 11, no. 3, pp. 123–140, 2024.
- [23] Hussein A Hilal "Information security based on sub-system keys generator by utilizing polynomials method and logic gate," *Journal of Discrete Mathematical Sciences and Cryptography*, 2023.
- [24] A. Ahmed, "Robustness of encryption under noise and tampering for secure image transmission," *journal of Digital Information Management*, Vols. vol. 16, no. 5, pp. 243–256, 2023.
- [25] Abdalrahman, "Secure Communication of the Integrated IoT and Cloud Computing," *Passer Journal of Basic and Applied Sciences*, 2022.