Alqalam Journal of Medical and Applied Sciences. 2026;9(1):73-83
https://doi.org/10.54361/ajmas.269114

Original article

A Comparative Mathematical Analysis of Elliptic-Curve–Enhanced AES for Image Encryption Using Dynamic Keys and S-Boxes

Aisha Dhaw[1]*, Abdalftah Elbori[1], K El Hadad[2]

[1]*Faculty of Science, Azzaytuna University, Tarhuna, Libya*
[2]*Faculty of Engineering, Elmergib University, Garaboulli, Libya*
Corresponding email. *aishasalheen5@gmail.com*

Abstract
In this study, an enhanced version of the Advanced Encryption Standard (AES) is proposed by integrating Elliptic Curve Cryptography (ECC) to generate dynamic S-boxes and encryption keys. The proposed scheme aims to enhance security while preserving computational efficiency in image encryption. Three NIST- recommended elliptic curves—P-256, P-384, and P-521 are employed to investigate the impact of curve size and algebraic properties on encryption strength and randomness. Experimental results demonstrate that the ECC-enhanced AES scheme achieves strong overall performance, with all configurations enabling perfect image reconstruction without distortion. Entropy analysis confirms a high degree of randomness, particularly when using CTR mode and the AES–ECC (P-521) configuration. Security evaluation shows strong resistance to differential and statistical attacks, as evidenced by high NPCR and UACI values and near-zero correlation coefficients. The combination of CTR mode and ECC provides the most robust protection. Histogram and visual analyses further verify effective concealment of perceptual information, with CTR mode nearly eliminating spatial pixel correlations. Compared with standard AES, the proposed AES–ECC approach, especially with the AES–ECC (P-521) configuration, exhibits improved pixel distribution uniformity and reduced residual visual patterns. Memory usage remains constant across all configurations. Although integrating CTR mode and ECC increases computational overhead, memory usage remains constant across all configurations, and ECB mode with the AES–ECC (P-256) configuration for grayscale images achieves competitive encryption times, reflecting the efficiency of this setup compared to other variants, and visual obfuscation while maintaining acceptable computational efficiency and image quality.
Keywords. AES, ECC, Image Encryption, S-Box, NIST Curves, NPCR, UACI, Correlation.

Introduction

The security of digital images has become increasingly important due to the rapid expansion of multimedia applications, cloud storage services, and online communication platforms. The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm because of its robustness and computational efficiency [1,2]. However, the use of fixed keys and static substitution boxes (S-Boxes) in standard AES reduces its resistance to advanced cryptanalytic attacks, particularly linear and differential cryptanalysis [3,4]. Elliptic Curve Cryptography (ECC) provides strong mathematical structures capable of generating dynamic keys and nonlinear S-boxes based on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP) [5,6]. The integration of ECC into AES has therefore emerged as a promising approach for enhancing randomness and adaptability in the encryption process. Recent studies have focused on strengthening AES through dynamic S-box construction and hybrid encryption schemes. In particular, S-boxes generated from unconventional randomness sources, such as underwater acoustic signals and Knight's Tour sequences, have demonstrated high nonlinearity and strong statistical properties [7]. Additionally, surveys on chaos-based image encryption highlight a broader trend toward complex and flexible encryption architectures for securing digital images [8]. Hybrid encryption approaches integrating Elliptic Curve Cryptography (ECC) with AES have been widely studied to generate dynamic keys and key-dependent S-boxes, improving the avalanche effect and resistance to linear and differential attacks. AES–ECC frameworks have demonstrated enhanced security, authentication, and data integrity in cloud and wireless communication environments, outperforming standalone cryptographic schemes [9, 10].

Recent research has focused on designing stronger S-Boxes by refining affine transformations and increasing algebraic complexity, where enhancing the mathematical structure of the S-Box has been shown to increase nonlinearity and reduce SAC deviation [11]. Additionally, models have been developed to generate dynamic S-Boxes using Mordell elliptic curves over Galois fields, demonstrating strong performance in image encryption applications[12]. Recent studies have also emphasized the necessity of non-static S-Boxes to strengthen AES against brute-force and biclique attacks and to modernize its security frameworks[13].

Despite these developments, the evaluation of NIST-recommended elliptic curves (P-256, P-384, and P-521) for dynamic key and S-box generation in digital image encryption remains limited. This study addresses this gap by comparatively analyzing standard AES and ECC-enhanced AES variants using NIST curves, with performance assessed through security, randomness, and image quality metrics.

Received*: 07-11-2025 -* ***Accepted****: 05-01-2026 -* ***Published****: 11-01-2026*

Methods

The Advanced Encryption Standard (AES) is a 128-bit block cipher employing SubBytes, ShiftRows, MixColumns, and AddRoundKey operations, with round keys generated through RotWord, SubWord, and XOR with round constants [1, 2, 14, 20, 21]. In image encryption, the strong correlation between adjacent pixels may expose visual patterns, making enhanced key and S-Box randomness essential [19]. In this study, AES-128 is adopted as a baseline and applied to uint8 image matrices partitioned into 128-bit blocks using MATLAB, where the S-Box provides nonlinearity and resistance to linear and differential attacks [1, 2, 14]. Elliptic Curve Cryptography (ECC) is based on point operations over finite fields, where point multiplication enables secure public key generation and supports dynamic key and S-Box construction [14–17, 22]. This work employs the NIST-recommended curves P-256, P-384, and P-521, which provide increasing security levels at higher computational costs and are widely used in modern ECC-based cryptosystems [14, 18, 23]. A modified AES algorithm is proposed by integrating ECC into the key generation and S-Box construction processes while preserving the standard AES round structure. The selected NIST curves are used to examine the impact of elliptic curve parameters on substitution box behavior and round key generation. In the proposed scheme, the S-Box is generated using elliptic curve point multiplication rather than the conventional multiplicative inverse and affine transformation. A base point is multiplied by predefined or pseudo-random scalars to generate curve points, from which coordinate values are reduced modulo 256 to construct the S-Box. The AES master key is similarly derived from elliptic curve operations, while the standard AES key schedule is retained with the ECC-generated S-Box incorporated into the SubWord operation. An analytical comparative methodology is adopted to evaluate the proposed approach against standard AES in terms of computational efficiency, security strength, and image quality. Both algorithms are implemented in MATLAB using grayscale and color images of size 256×256 pixels. Performance evaluation is conducted using execution time, memory usage, correlation coefficient, NPCR, UACI, entropy, PSNR, MSE, and SSIM, with results reported numerically and graphically.

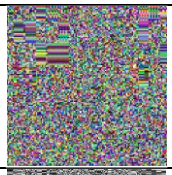
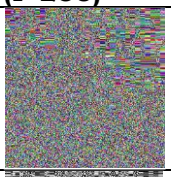
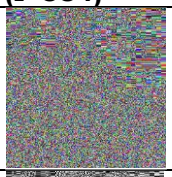
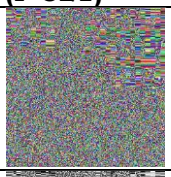
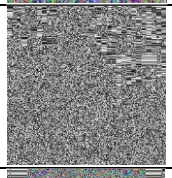
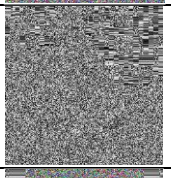
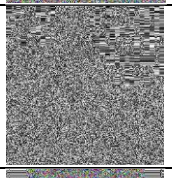
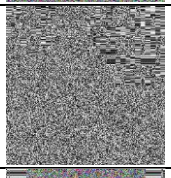
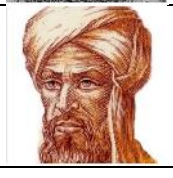
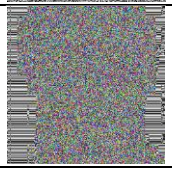
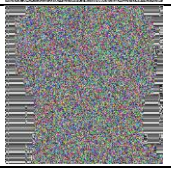
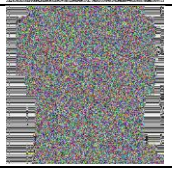
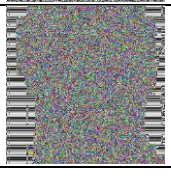
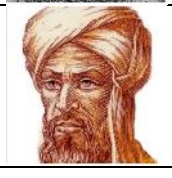
Results

This section presents the experimental results of the proposed encryption scheme, including visual analysis, statistical metrics, histograms, and S-box performance. Results are organized as follows: original and encrypted images, histogram analysis, quantitative metrics, supporting charts, S-box evaluation, and discussion of the findings.

Original and Encrypted Images

Table 1 shows a clear loss of overall perceptual meaning in most of the encrypted images, as the original image cannot be directly recognized, despite the presence of some residual random visual gradients. This effect is more pronounced in Img1-Makkah-Gray. It is also observed that the use of the modified versions based on elliptic curves slightly reduces the persistence of these visual gradients when compared to the standard AES algorithm, indicating a limited improvement in disrupting the spatial structures of the image. In contrast, Img2-Mathematician-Color and Img2-Mathematician-Gray exhibit the persistence of certain visual features from the original image within the encrypted outputs. This behavior can be attributed to the nature of personal images, which typically contain relatively homogeneous regions and repetitive structural patterns. Nevertheless, the integration of elliptic curves in key generation and non-linear structures contributes to a partial reduction in the visibility of these features, although it does not lead to their complete elimination under the current configuration. This observation highlights the necessity of complementing visual analysis with quantitative statistical metrics.

Table1.original and encrypted images using ECB mode.

Image	Original	AES-128	AES–ECC (P-256)	AES–ECC (P-384)	AES-ECC (P-521)	Decrypted
Img1-Makkah-Color						
Img1-Makkah-Gray						
Img2-Mathematician-Color						

Received*: 07-11-2025 -* ***Accepted****: 05-01-2026 -* ***Published****: 11-01-2026*

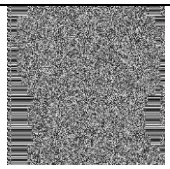
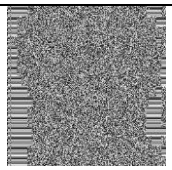
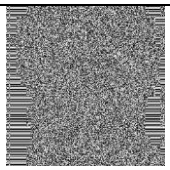
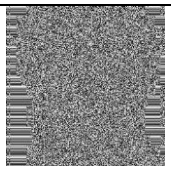
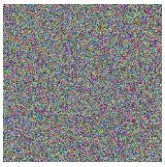
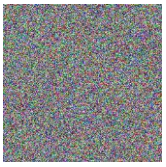
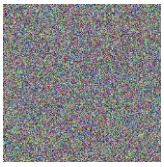
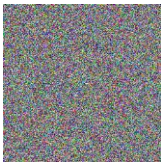
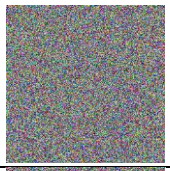
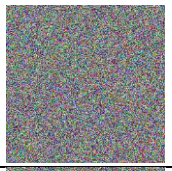
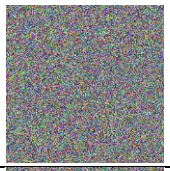
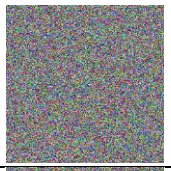
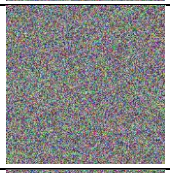
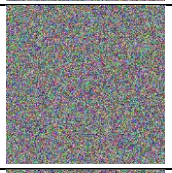
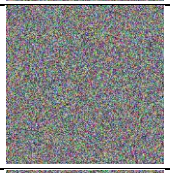
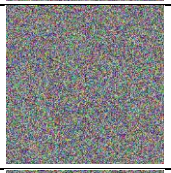
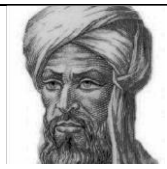
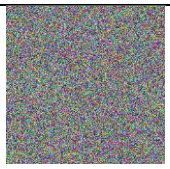
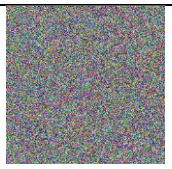
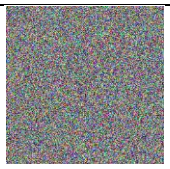
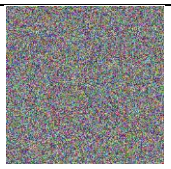
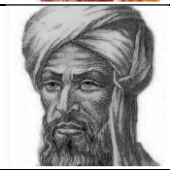
Img2-Mathematician-Gray						

Table 2 demonstrates that this mode leads to a near-complete elimination of any visual correlation between the original image and the encrypted image. All encrypted images appear as highly dispersed random noise, with no distinguishable visual features, regardless of whether the images are color or grayscale, and irrespective of the image content, whether personal images or landmark and natural scene images. This behavior reflects the strong capability of the CTR mode to effectively break the spatial correlation between pixels, making it more suitable for image encryption applications compared to the ECB mode. Furthermore, the results indicate that integrating elliptic curves into the algorithmic structure does not adversely affect this behavior; rather, it contributes to maintaining a fully secure encryption level, as the encrypted images consistently preserve a completely random appearance without the emergence of any perceptible patterns or visual structures.

Table2. original and encrypted images using CTR mode

Image	**Original**	**AES**	**AES–ECC (P-256)**	**AES–ECC (P-384)**	**AES-ECC (P-521)**	**Decrypted**
Img1-Makkah-Color						
Img1-Makkah-Gray						
Img2-Mathematician-Color						
Img2-Mathematician-Gray						

Histogram Analysis

To further evaluate the effectiveness of the proposed encryption schemes, a histogram analysis is conducted for both the original and encrypted images using the ECB and CTR modes. Histogram analysis is a widely used statistical tool to assess the distribution of pixel intensity values and to examine the ability of an encryption algorithm to eliminate statistical patterns inherent in the original image. A secure image encryption scheme is expected to produce encrypted images with uniform and flat histograms, indicating a high level of randomness and resistance to statistical attacks. The following tables present the histograms of the original images alongside their corresponding encrypted versions for both encryption modes.

Received*: 07-11-2025 -* ***Accepted****: 05-01-2026 -* ***Published****: 11-01-2026*

https://doi.org/10.54361/ajmas.269114

Figure 1. histogram of the original images

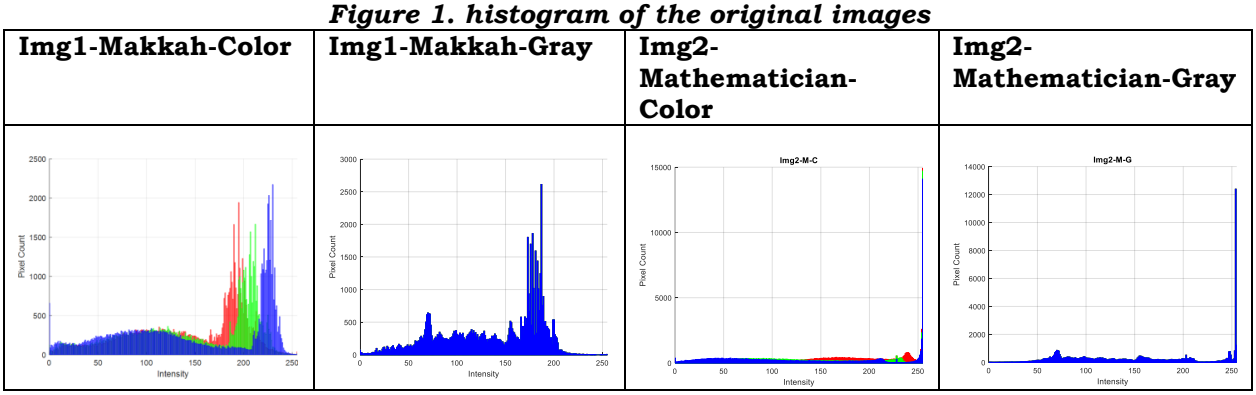


Figure 2. Histogram of the encryption images (ECB mode)

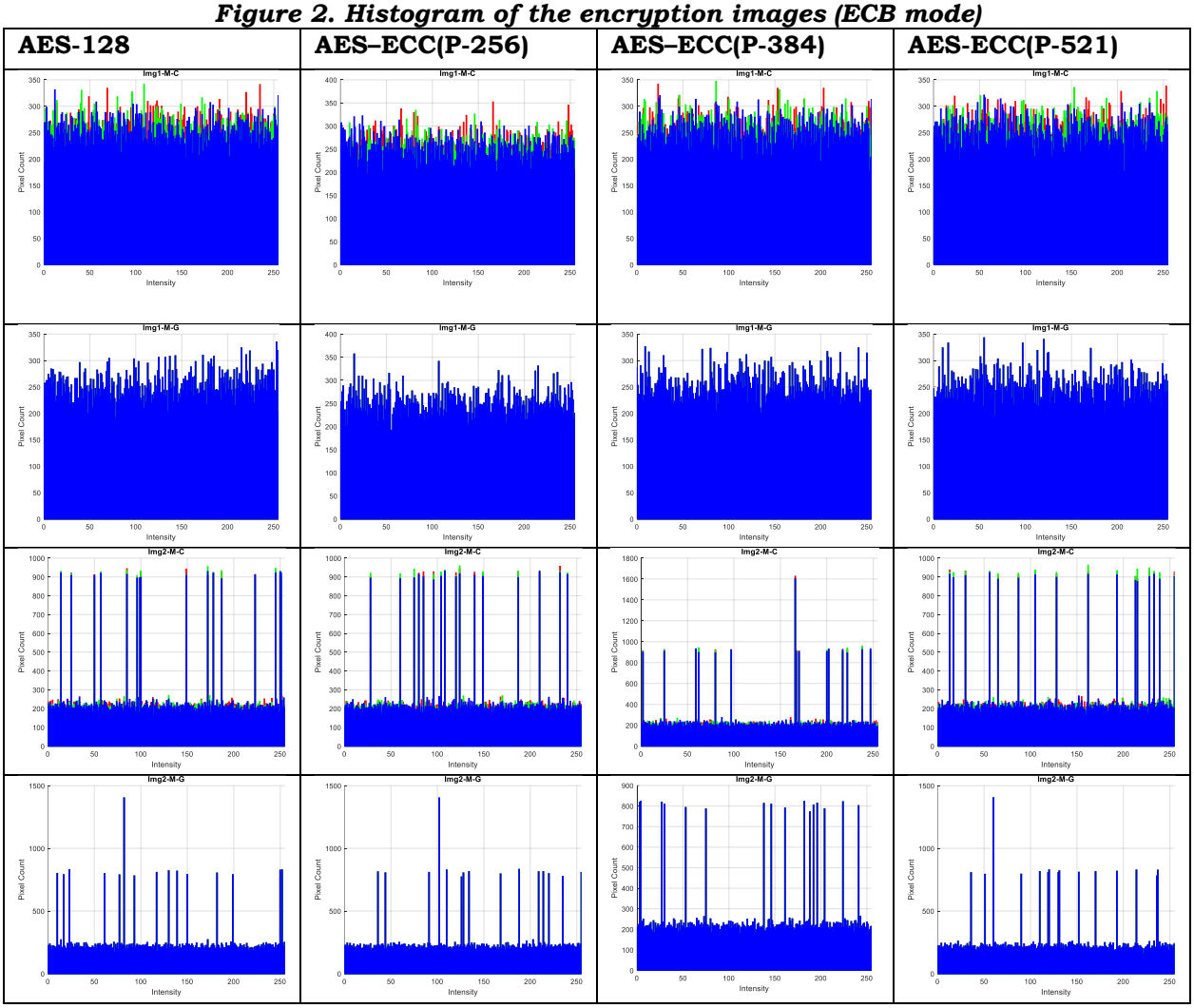


Figure 2 presents the unified histograms of the color channels for the images used in (Table 1), in the same order. For Img1-Makkah-Color and Img1-Makkah-Gray, the distribution appears nearly homogeneous across the full pixel value range (0–255), with the AES–ECC(P-521) algorithm achieving a slightly higher degree of homogeneity compared to the other algorithms, according to visual observation, although all algorithms exhibit a relatively homogeneous distribution. For Img2-Mathematician-Color, it was observed that AES–ECC(P-384) achieves the highest level of homogeneity in histogram distribution, while in Img2-Mathematician-Gray, both AES and AES–ECC(P-521) demonstrate the greatest degree of homogeneity.

These results indicate that the integration of elliptic curves contributes to improving the histogram distribution of the images, despite the limited effectiveness of this mode in encrypting the images. This reflects a slight improvement in the statistical distribution of pixel values when using elliptic curves, demonstrating the ability of these modifications to enhance randomness and reduce residual visual patterns.

Received: *07-11-2025* - ***Accepted***: *05-01-2026* - ***Published***: *11-01-2026*

https://doi.org/10.54361/ajmas.269114

Figure 3. histogram of the encryption images (CTR mode).

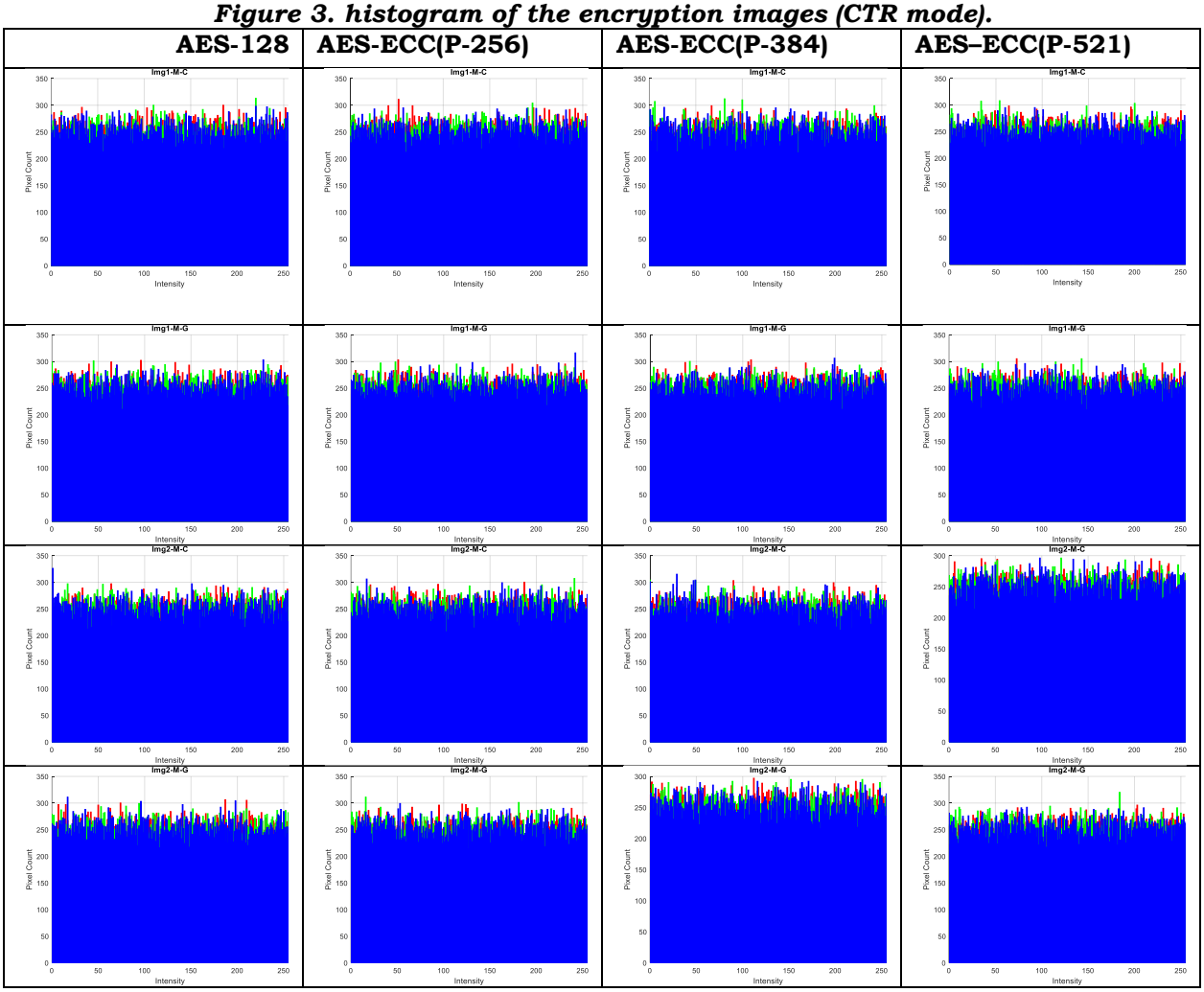


Figure 3 shows that all algorithms produce a nearly fully homogeneous histogram, reflecting the strength of this mode in image encryption. It is also observed that the integration of elliptic curves slightly improves the histogram, with Img1-Makkah-Color encrypted using AES–ECC(P-521) achieving the highest degree of homogeneity according to visual observation, while Img2-Mathematician-Color indicates that AES–ECC(P-256) is approximately the most effective. Furthermore, this mode demonstrates greater strength in encrypting grayscale images, as the histogram is represented across three channels instead of a single channel, as in the ECB mode, indicating a higher effectiveness in pixel value distribution. Finally, the incorporation of elliptic curves provides an additional enhancement to the histogram, particularly for AES–ECC(P-521), where the improvement is more pronounced in the ECB mode compared to the CTR mode.

Numerical Results and Supporting Figures

This section aims to present the numerical data and graphical representations that illustrate the performance of the encryption algorithms used in the study. The tables and graphs provide a comparison of the algorithms under both ECB and CTR modes, enabling the evaluation of randomness and encryption efficiency for each algorithm separately, while considering the impact of integrating elliptic curves. The tables and graphical representations also reflect the statistical and visual metrics for each algorithm, facilitating a clear understanding of the performance differences among the various models.

Received: *07-11-2025* - ***Accepted***: *05-01-2026* - ***Published***: *11-01-2026*

Table 3. Performance metrics for AES-128 and ECC-AES using P-256, P-384, and P-521 under ECB and CTR mode.

Algorithms	Security			Computational Efficiency		Image Quality			
	NPCR	UACI	Correlation	Total Execution Time	Memory Usage	PSNR	MSE	SSIM	Entropy
Img1-Makkah-Color									
AES-128+ECB	99.64%	30.44%	0.0042	282.98s	192.00KB	Inf dB	0.0000	1.0000	7.9936
AES-128+CTR	99.61%	30.55%	0.0008	317.77s	192.00KB	Inf dB	0.0000	1.0000	7.9970
AES–ECC(P-256)+ECB	99.61%	30.64%	0.0032	286.85s	192.00KB	Inf dB	0.0000	1.0000	7.9927
AES–ECC(P-256)+CTR	99.59%	30.76%	0.0023-	381.40s	192.00KB	Inf dB	0.0000	1.0000	7.9969
AES–ECC(P-384)+ECB	99.62%	30.71%	0.0033-	286.20s	192.00KB	Inf dB	0.0000	1.0000	7.9927
AES–ECC(P-384)+CTR	99.61%	30.56%	0.0002-	321.46s	192.00KB	Inf dB	0.0000	1.0000	7.9975
AES–ECC(P-521)+ECB	99.62%	30.30%	0.0160	287.16s	192.00KB	Inf dB	0.0000	1.0000	7.9928
AES–ECC(P-521)+CTR	99.59%	30.59%	0.0011	333.52s	192.00KB	Inf dB	0.0000	1.0000	7.9968
Img1-Makkah-Gray									
AES-128+ECB	99.59%	28.98%	0.0151	274.00s	192.00KB	Inf dB	0.0000	1.0000	7.9933
AES-128+CTR	99.61%	29.08%	0.0029	387.05s	192.00KB	Inf dB	0.0000	1.0000	7.9971
AES–ECC(P-256)+ECB	99.57%	29.30%	0.0024-	257.65s	192.00KB	Inf dB	0.0000	1.0000	7.9924
AES–ECC(P-256)+CTR	99.59%	29.41%	0.0021-	415.35s	192.00KB	Inf dB	0.0000	1.0000	7.9972
AES–ECC(P-384)+ECB	99.61%	29.18%	0.0019-	272.96s	192.00KB	Inf dB	0.0000	1.0000	7.9931
AES–ECC(P-384)+CTR	99.61%	29.17%	0.0015-	400.76s	192.00KB	Inf dB	0.0000	1.0000	7.9969
AES–ECC(P-521)+ECB	99.62%	29.19%	0.0010-	270.72s	192.00KB	Inf dB	0.0000	1.0000	7.9929
AES–ECC(P-521)+CTR	99.59%	29.24%	0.0037-	413.54s	192.00KB	Inf dB	0.0000	1.0000	7.9973
Img2-Mathematician-Color									
AES-128+ECB	99.67%	37.34%	0.0207	285.33s	192.00KB	Inf dB	0.0000	1.0000	7.7962
AES-128+CTR	99.61%	37.62%	0.0017-	323.86s	192.00KB	Inf dB	0.0000	1.0000	7.9974
AES–ECC(P-256)+ECB	99.69%	37.72%	0.0008	277.00s	192.00KB	Inf dB	0.0000	1.0000	7.7955
AES–ECC(P-256)+CTR	99.59%	37.98%	0.0017	345.72s	192.00KB	Inf dB	0.0000	1.0000	7.9973
AES–ECC(P-384)+ECB	99.69%	36.68%	0.0481	276.15s	192.00KB	Inf dB	0.0000	1.0000	7.7824
AES–ECC(P-384)+CTR	99.61%	37.80%	0.0048	304.13s	192.00KB	Inf dB	0.0000	1.0000	7.9973
AES–ECC(P-521)+ECB	98.59%	36.74%	0.0363	278.28s	192.00KB	Inf dB	0.0000	1.0000	7.7970
AES–ECC(P-521)+CTR	99.59%	37.84%	0.0053	314.22s	192.00KB	Inf dB	0.0000	1.0000	7.9976
Img2-Mathematician-Gray									
AES-128+ECB	99.65%	35.57%	0.0358-	274.32s	192.00KB	Inf dB	0.0000	1.0000	7.8396
AES-128+CTR	99.61%	34.68%	0.0003	311.77s	192.00KB	Inf dB	0.0000	1.0000	7.9972
AES–ECC(P-256)+ECB	99.71%	33.70%	0.0496	257.89s	192.00KB	Inf dB	0.0000	1.0000	7.8402
AES–ECC(P-256)+CTR	99.59%	34.89%	0.0027-	315.94s	192.00KB	Inf dB	0.0000	1.0000	7.9974

Received*: 07-11-2025 -* ***Accepted****: 05-01-2026 -* ***Published****: 11-01-2026*

AES–ECC(P-384)+ECB	99.69%	34.61%	0.0039	277.33s	192.00KB	Inf dB	0.0000	1.0000	7.8508
AES–ECC(P-384)+CTR	99.61%	34.86%	0.0041-	308.01s	192.00KB	Inf dB	0.0000	1.0000	7.9969
AES–ECC(P-521)+ECB	99.61%	34.42%	0.0136	267.62s	192.00KB	Inf dB	0.0000	1.0000	7.8376
AES–ECC(P-521)+CTR	99.59%	34.74%	0.0007-	305.54s	192.00KB	Inf dB	0.0000	1.0000	7.9976

Following the presentation of the numerical data in Table 3, the subsequent section introduces illustrative graphs that visually depict the performance of the algorithms. These graphs support the comparative analysis under ECB and CTR modes, as well as the integration of elliptic curves, providing a clearer understanding of the performance differences among the various algorithms.

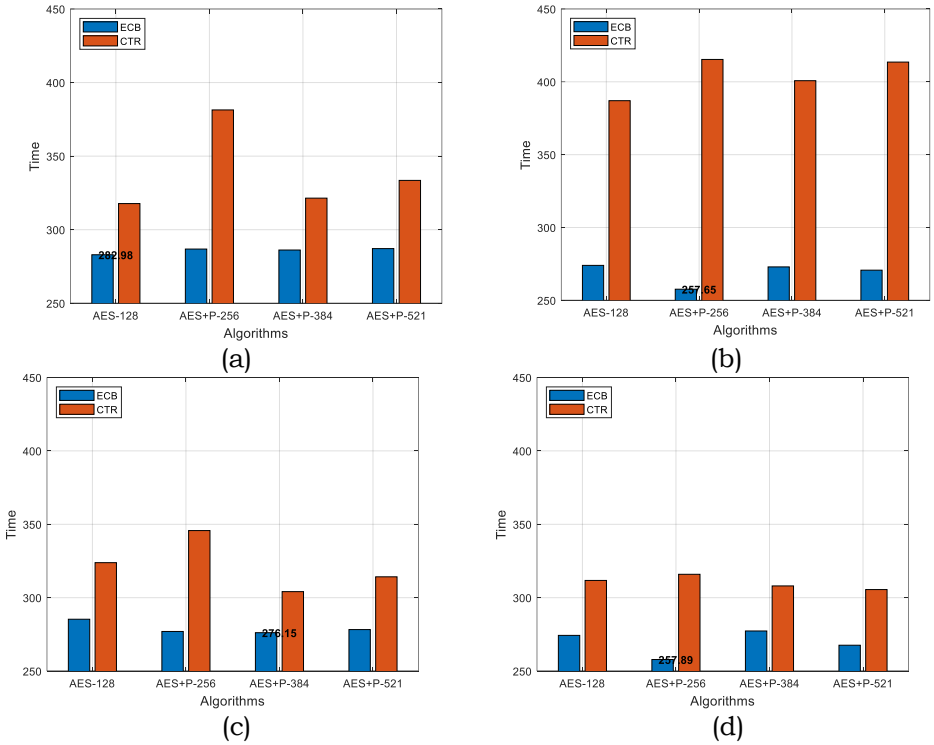


Figure* 4*. Execution and encryption time analysis: (a) Img1 – Makkah (Color), (b) Img1 – Makkah (Gray), (c) Img2 – Mathematician (Color) (d) Img2 – Mathematician (Gray).

Figures 4(a–d)) show that CTR-mode encryption (red bars) requires longer execution times than ECB across all algorithms, reflecting the extra processing for counter-based encryption and keystream generation. In ECB mode (Figure 4(a)), standard AES shows the lowest encryption time. Figures 4(b)–4(d) indicate that integrating ECC into AES reduces encryption time for certain images; notably, AES–ECC (P-256) achieves the shortest time for grayscale images, outperforming standard AES and other ECC variants. Although CTR mode incurs higher computational overhead, ECC-based key generation can improve efficiency in specific scenarios without compromising security. Following this, entropy values are analyzed to assess randomness in encrypted images and their resistance to statistical attacks.

Received*: 07-11-2025 -* ***Accepted****: 05-01-2026 -* ***Published****: 11-01-2026*

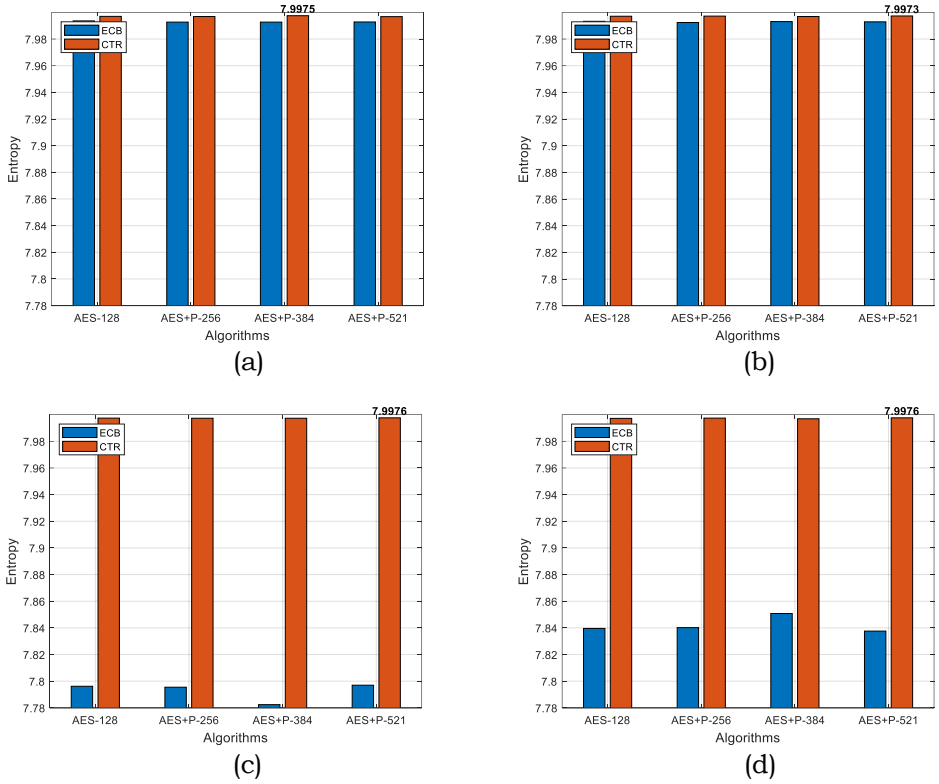


Figure 5. Entropy analysis: (a) Img1 – Makkah (Color), (b) Img1 – Makkah (Gray), (c) Img2 – Mathematician (Color), and (d) Img2 – Mathematician (Gray).

Figures 5(a–d) show that CTR mode achieves higher entropy than ECB, indicating stronger statistical randomness and suppression of repetitive patterns. While both modes exhibit high entropy across all algorithms, integrating ECC into AES provides a slight additional improvement, and this effect is most pronounced with the AES–ECC (P-521) configuration, reaching an entropy of 7.9976 (Figure 5(d)), suggesting that increased complexity in key generation and S-box construction positively, though modestly, impacts encrypted image quality.

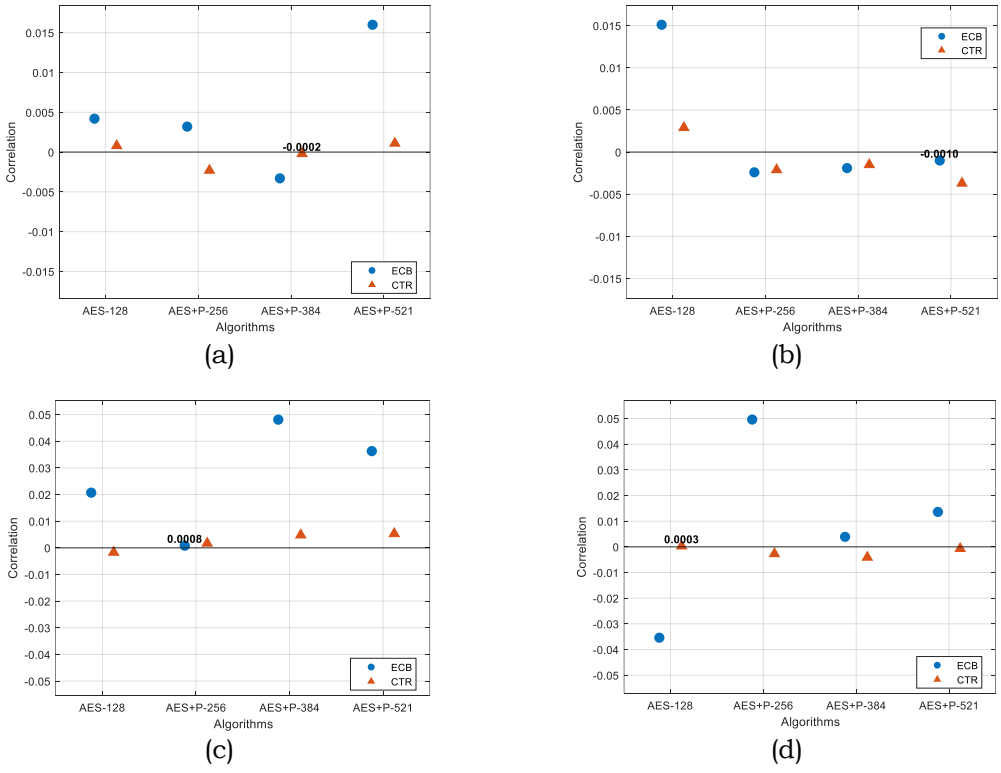


Figure 6. Correlation Analysis: (a) Img1 – Makkah (Color), (b) Img1 – Makkah (Gray), (c) Img2 – Mathematician (Color), and (d) Img2 – Mathematician (Gray).

Received: *07-11-2025* - ***Accepted***: *05-01-2026* - ***Published***: *11-01-2026*

The results show that the CTR mode achieves lower correlation coefficients than ECB, indicating a stronger reduction of statistical dependency in encrypted images. Integrating ECC further reduces correlation in most cases. For example, (Figure 6(a)) shows that the AES–ECC (P-384) configuration attains the lowest correlation of −0.0002, closest to zero, while (Figure 6(d)) shows that standard AES reaches 0.0003, with other images exhibiting higher values. These results indicate that input image characteristics, along with encryption mode and algorithm structure, influence performance.

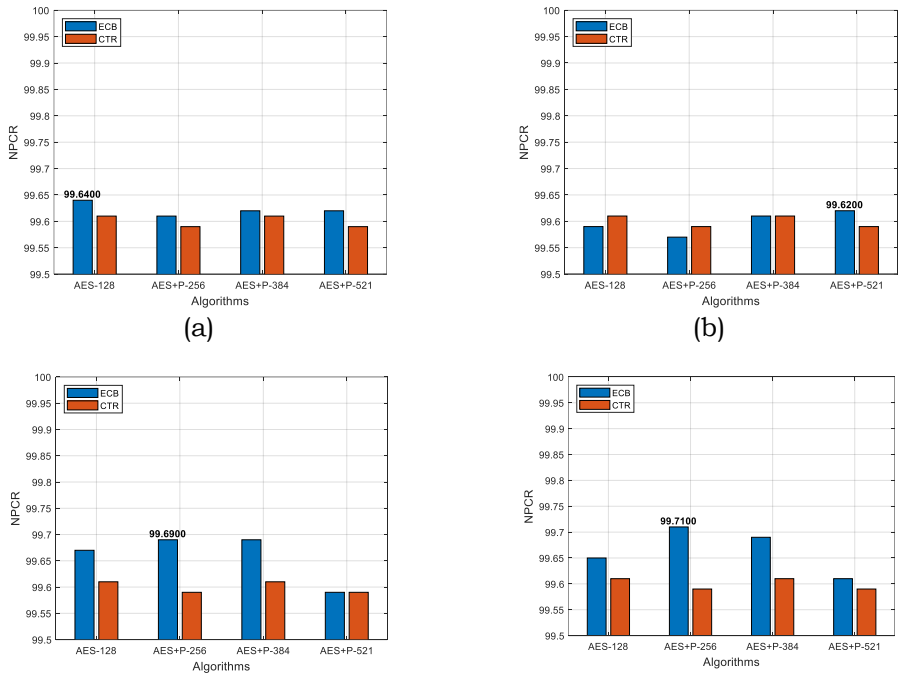


Figure 7. NPCR Analysis: (a) Img1 – Makkah (Color), (b) Img1 – Makkah (Gray), (c) Img2 – Mathematician (Color), and (d) Img2 – Mathematician (Gray)

The results presented in the previous figures show that the CTR mode achieves relatively stable values across all images, whereas the ECB mode exhibits higher NPCR percentages in most of the tested images. It is also observed that the AES–ECC (P-256) configuration reaches an NPCR value of 99.71%, achieving the highest NPCR as illustrated in (Figure 7(d)). This indicates that incorporating elliptic curves increases the sensitivity of the algorithm to small changes in the original image, meaning that any minor modification in the plaintext results in a larger impact on the encrypted image, although this improvement remains relatively limited.

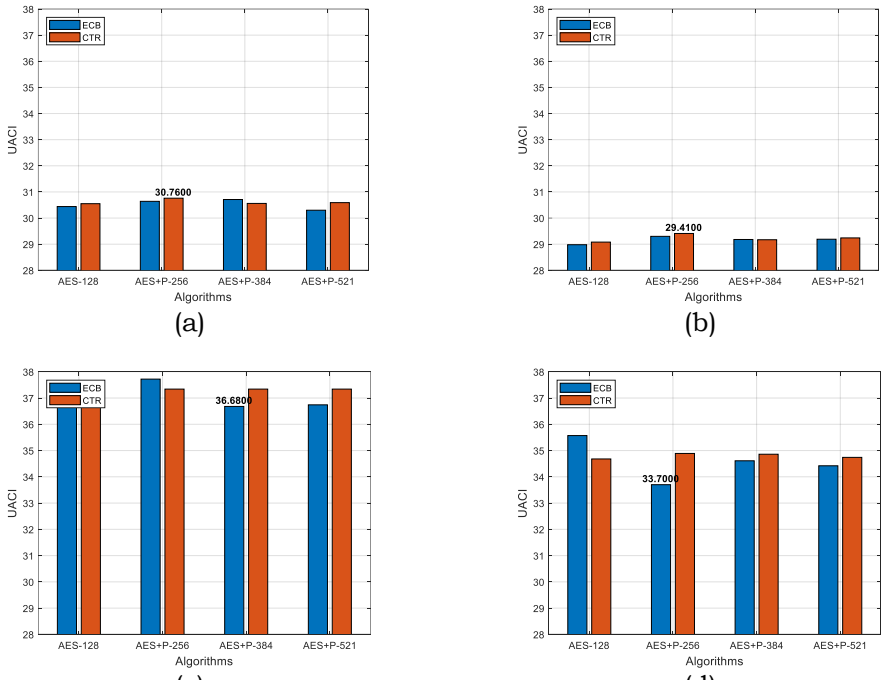


Figure 8. UACI Analysis: (a) Img1 – Makkah (Color), (b) Img1 – Makkah (Gray), (c) Img2 – Mathematician (Color), and (d) Img2 – Mathematician (Gray)

Received: *07-11-2025* - ***Accepted***: *05-01-2026* - ***Published***: *11-01-2026*

Most experiments show that the ECB mode achieves values close to the optimal 33.33%. Integrating the AES–ECC (P-256) configuration further improves the value to 33.70% (Figure 8(d)). Image type also affects results; for example, Img2-Mathematician-Color achieved high percentages across algorithms, whereas Img1-Makkah-Gray (Figure 8(b)) showed lower UACI values, likely due to inherent image characteristics.

Discussion

These results summarize the evaluations of image quality, security, and computational efficiency, highlighting accurate image reconstruction, robustness against differential and statistical attacks, and practical feasibility in terms of memory usage and execution time. Overall, they illustrate how algorithmic modifications and encryption modes influence performance.

Image Quality Metrics

All algorithms achieved identical reconstruction quality, with MSE = 0 and PSNR = ∞, indicating perfect recovery of the original image after decryption. SSIM values of 1.0000 across all experiments further confirm that neither AES nor the hybrid ECC-AES introduced any degradation or distortion.

Entropy values ranged between 7.7824 and 7.9976, reflecting a high degree of randomness in the encrypted images, with a clear advantage for the CTR mode over the ECB mode, as shown in Figures 5(a-b). The integration of elliptic curve cryptography led to a slight improvement in entropy values, which became more evident when the AES–ECC (P-521) configuration was employed, achieving the highest entropy value of 7.9976 (Figure 5(d)). This indicates a limited but positive impact of the added mathematical complexity on the quality of the encrypted images.

Security Metrics

The Number of Pixels Change Rate (NPCR) values range from 99.57% to 99.71%, demonstrating strong resistance to differential attacks, while the Unified Average Changing Intensity (UACI) values lie between 28.98% and 37.98%, close to the theoretical ideal of 33% for encrypted images. Correlation coefficients remain near zero (−0.0358 to 0.0496), with negative values reflecting random variation rather than true inverse correlation, indicating negligible statistical dependency between original and encrypted images.

Overall, the CTR mode outperforms ECB in reducing correlation and enhancing NPCR and UACI values, particularly when combined with elliptic curves. The AES–ECC (P-384) configuration achieves the lowest correlation (−0.0002, Figure 6(a)), whereas the original AES attains 0.0003. The AES–ECC (P-256) configuration yields the highest NPCR (99.71%, Figure 7(d)) and brings UACI closer to the optimal (33.70%, Figure 8(d)), indicating increased sensitivity to small plaintext changes.

These results also highlight that the type of image affects performance. For example, Img2-Mathematician-Color shows higher UACI across algorithms, while Img1-Makkah-Gray exhibits lower values (Figure 8(b)), reflecting inherent image characteristics. Overall, integrating elliptic curve cryptography enhances the algorithm's resistance to differential and statistical attacks, with CTR + ECC combinations providing the most secure configuration.

Computational Efficiency

Memory usage remains constant at 192 KB across all methods, indicating that integrating elliptic curve cryptography (ECC) does not affect memory requirements. It is observed that using the CTR mode requires longer execution time compared to ECB across all algorithms. This is due to the additional operations involved in CTR, such as keystream generation and counter processing for each data block, which increase the computational overhead compared to the simpler ECB mode, where each block is processed independently. ECC-based methods generally incur higher execution times because of scalar point multiplication. However, in certain cases, such as grayscale images, the AES–ECC (P-256) configuration achieves shorter encryption times compared to other ECC variants, indicating that the type of image can influence computational efficiency. Overall, the results suggest that while integrating ECC enhances security, using the CTR mode introduces additional computational cost, which is expected due to the extra processing complexity.

Conclusion

The integration of ECC into AES significantly enhances image encryption performance. All configurations achieved lossless reconstruction, confirming the preservation of image integrity. Security analysis demonstrates robust resistance to differential and statistical attacks, with CTR mode combined with ECC delivering higher randomness, elevated NPCR and UACI values, and near-zero correlation. Memory usage remained constant, while execution time increased marginally due to ECC computations and CTR operations. Overall, ECC-enhanced AES in CTR mode provides an optimal balance of security, randomness, and computational efficiency, establishing it as a reliable solution for secure image encryption. Future research should further investigate encryption and decryption times across varying image sizes to evaluate

Received*: 07-11-2025 -* ***Accepted****: 05-01-2026 -* ***Published****: 11-01-2026*

scalability and conduct comparative analyses with chaos-based encryption schemes to systematically assess security robustness, processing efficiency, and suitability across diverse image encryption scenarios.

Conflicts of Interest.
The author declares no conflict of interest.

References

1. Stallings W. Cryptography and network security. 4th ed. Pearson Education India; 2006.
2. Daemen J, Rijmen V. The design of Rijndael. Vol. 2. Springer; 2002.
3. Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. J CRYPTOL. 1991;4(1):3-72.
4. Matsui M. Linear cryptanalysis method for DES cipher. In: Workshop on the Theory and Application of of Cryptographic Techniques. Springer; 1993.
5. Miller VS. Use of elliptic curves in cryptography. In: Conference on the theory and application of cryptographic techniques. Springer; 1985.
6. Koblitz N. Elliptic curve cryptosystems. Math Comput. 1987;48(177):203-209.
7. Khan MF, Ali A, Javed K, Naqvi RA, ur Rehman S. Block cipher's substitution box generation based on natural randomness in underwater acoustics and knight's tour chain. Comput Intell Neurosci. 2022;2022:8338508.
8. Zolfaghari B, Koshiba T. Chaotic image encryption: state-of-the-art, ecosystem, and future roadmap. Appl Syst Innov. 2022;5(3):57.
9. Rehman S, Alamer A, Alharbi A, Baig M, Ali A. Hybrid AES-ECC model for the security of data over cloud storage. Electronics. 2021;10(21):2673.
10. Subedar Z, Araballi A. Hybrid cryptography: Performance analysis of various cryptographic combinations for secure communication. Int J Math Sci Comput. 2020;6(4):35-41.
11. Cui J, Huang L, Zhong H, Chang C, Yang W. An improved AES S-box and its performance analysis. Int J Innov Comput Inf Control. 2011;7(5):2291-2302.
12. Alali AS, Almutairi ZM, Khan MF, Maqsood T, Alotaibi A. Dynamic S-box construction using mordell elliptic curves over galois field and its applications in image encryption. Mathematics. 2024;12(4):587.
13. Nissar G, Garg DK, Khan BUI. Implementation of security enhancement in AES by inducting dynamicity in AES s-box. Int J Innov Technol Explor Eng. 2019;8(10):1-9.
14. Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of Applied Cryptography. CRC Press; 1996.
15. Koblitz N. A course in number theory and cryptography. Vol. 114. Springer Science & Business Media; 1994.
16. Miller VS. Use of elliptic curves in cryptography. In: Advances in Cryptography CRYPTO'85 (Lecture Notes in Computer Science, vol 218). Springer-Verlag; 1986.
17. Hankerson D, Vanstone S, Menezes A. Guide to elliptic curve cryptography. Springer; 2004.
18. National Institute of Standards and Technology (US). Digital Signature Standard (DSS). FIPS PUB. 2000:186-192.
19. Afreen R, Mehrotra SC. A review on elliptic curve cryptography for embedded systems. arXiv:1107.3631 [Preprint]. 2011.
20. Paar C, Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer; 2009.
21. Ferguson N, Schneier B, Kohno T. Cryptography engineering: design principles and practical applications. John Wiley & Sons; 2011.
22. Silverman JH. The arithmetic of elliptic curves. Vol. 106. Springer; 2009.
23. Qu M. SEC 2: Recommended elliptic curve domain parameters. Mississauga, ON, Canada: Certicom Research; 1999. Tech. Rep. SEC2-Ver-0.6.

Received*: 07-11-2025 -* ***Accepted****: 05-01-2026 -* ***Published****: 11-01-2026*