iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VIII **Month of publication:** August 2026

DOI: https://doi.org/10.22214/ijraset.2026.84565

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

A Hybrid ECC-LFT and AES-256-GCM Framework for Secure and Authenticated Image Encryption

Rongali Ramakrishna[1], Dr. Siva Rama Krishna T.[2]
[1]*M.Tech (Cybersecurity),* [2]*Associate Professor, Dept. of Computer Science Engineering, UCEK, JNTU Kakinada, Andhra Pradesh, India*

Abstract: ***The proliferation of image-centric applications in healthcare, defense communication, cloud storage, and social platforms has intensified the demand for encryption schemes that combine strong confusion–diffusion properties with verifiable ciphertext integrity. Existing elliptic curve cryptography–linear fractional transformation (ECC–LFT) image ciphers achieve favorable statistical security but generally omit a standardized authentication mechanism, leaving ciphertexts exposed to undetected tampering. This paper proposes a four-stage hybrid pipeline that closes this gap. Dynamic 8×8 substitution boxes are first constructed over GF(2^8) using parameters derived from an elliptic-curve pseudo-random generator and a linear fractional transformation, yielding a nonlinearity score of 112. An elliptic-curve-driven pseudo-random index sequence then permutes the substituted pixels, a ChaCha20 keystream whitens the permuted stream, and AES-256 in Galois/Counter Mode encrypts the whitened stream and appends a 128-bit authentication tag, providing NIST-aligned authenticated encryption. Evaluated on standard test images, the framework achieves information entropy of 7.9990–7.9992, NPCR of 99.60%–99.63%, UACI of approximately 33.41%–33.43%, and adjacent-pixel correlation below 0.06 in all directions, with the constructed S-boxes attaining optimal nonlinearity, balanced output, and zero linear structure. Comparative evaluation against six state-of-the-art schemes indicates competitive or superior statistical security while uniquely providing cryptographic tamper detection through the embedded authentication tag.***

Keywords: ***Image encryption, elliptic curve cryptography, linear fractional transformation, AES-256-GCM, ChaCha20, dynamic S-box, NPCR, UACI, authenticated encryption.***

I. INTRODUCTION

The rapid expansion of image-centric digital services has made visual data one of the most frequently transmitted and stored categories of information on modern networks, spanning medical imaging, defense communication, biometric authentication, and cloud storage. Because images carry large data volumes with strong pixel-to-pixel correlation, a cipher that ignores this structure risks leaving exploitable statistical regularities in the ciphertext even when the underlying primitive is otherwise sound. This has motivated a large body of image-specific encryption research, including chaotic-map, DNA-coding, and elliptic curve cryptography (ECC) based constructions.

ECC is attractive for image encryption because it delivers strong security per bit of key material with low computational overhead relative to large-prime-field public-key schemes. A widely used design pairs ECC-derived randomness with a Linear Fractional Transformation (LFT) over GF(2^8) to build dynamic substitution boxes (S-boxes) that can approach the maximum attainable nonlinearity for 8-bit Boolean functions [1]. Despite these strengths, a recurring limitation of ECC–LFT image ciphers in the literature is the absence of a standardized authentication layer: such schemes typically produce semantically secure ciphertext but give a receiver no cryptographic means to detect tampering.

Authenticated Encryption with Associated Data (AEAD) closes this gap. AES-256 in Galois/Counter Mode (AES-256-GCM) is NIST-standardized and pairs 256-bit confidentiality with a 128-bit authentication tag that detects ciphertext modification with overwhelming probability. This paper integrates AES-256-GCM into an ECC–LFT pipeline, sequencing ECC–LFT substitution, ECC-driven pixel permutation, a ChaCha20 whitening stage, and AES-256-GCM authenticated encryption into a single four-stage framework. The whitening stage is included because permutation alone does not maximize the entropy of the intermediate stream; a key-dependent XOR layer closes residual statistical structure before the final AEAD step.

II. RELATED WORK

Elliptic curve cryptography has been widely explored as a source of pseudo-randomness for image ciphers. Toughi et al. combined an elliptic-curve pseudo-random generator with AES for image encryption, while Rehman et al. used a piecewise function with elliptic curves over GF(2^n) for color image encryption [4], [5]. Razaq et al. applied a group-theoretic and graphical approach to build cryptographically strong nonlinear block-cipher components [6]. These studies established ECC-derived randomness as a practical basis for image-cipher design but typically evaluate only statistical security, without an authentication mechanism.

A parallel line of work targets dynamic S-box construction. Haider et al. and Ibrahim and Abbas built key-dependent S-boxes from elliptic-curve points [2], [3], and Jamal et al. combined elliptic-curve points with a Linear Fractional Transformation over GF(2^8) to construct S-boxes with near-optimal nonlinearity, forming the basis of the S-box construction used in this paper [1]. Rehman et al. and Hilal et al. extended this approach to Mordell elliptic curves for nonlinear component design [9], [10]. Comparative studies of Latin-square-based [7] and chaotic-map-based [8] S-boxes report lower nonlinearity and higher differential/linear approximation probabilities than the EC–LFT approach, motivating its use here. Hybrid designs that combine chaos or ECC with a symmetric block cipher have also been proposed: El-Latif and Niu combined a chaotic system with cyclic elliptic curves [11], Wu et al. paired chaotic systems with an elliptic-curve ElGamal scheme [14].However, none of these ECC- or chaos-based hybrid schemes incorporate a standardized AEAD primitive, so ciphertext integrity is not addressed and a receiver cannot detect tampering. This paper addresses that gap by integrating AES-256-GCM as the final authenticated-encryption stage of an ECC–LFT pipeline, combining the confusion–diffusion strength of EC–LFT substitution and permutation with NIST-standardized confidentiality and tamper detection in a single framework.

III. PROPOSED METHOD

The proposed scheme encrypts an RGB image I of dimensions P×Q×3 through the four-stage pipeline shown in Fig. 1: dynamic ECC–LFT S-box substitution, ECC-based pixel permutation, ChaCha20 whitening, and AES-256-GCM authenticated encryption, preceded by a PBKDF2 key-derivation stage. Each stage is described below.

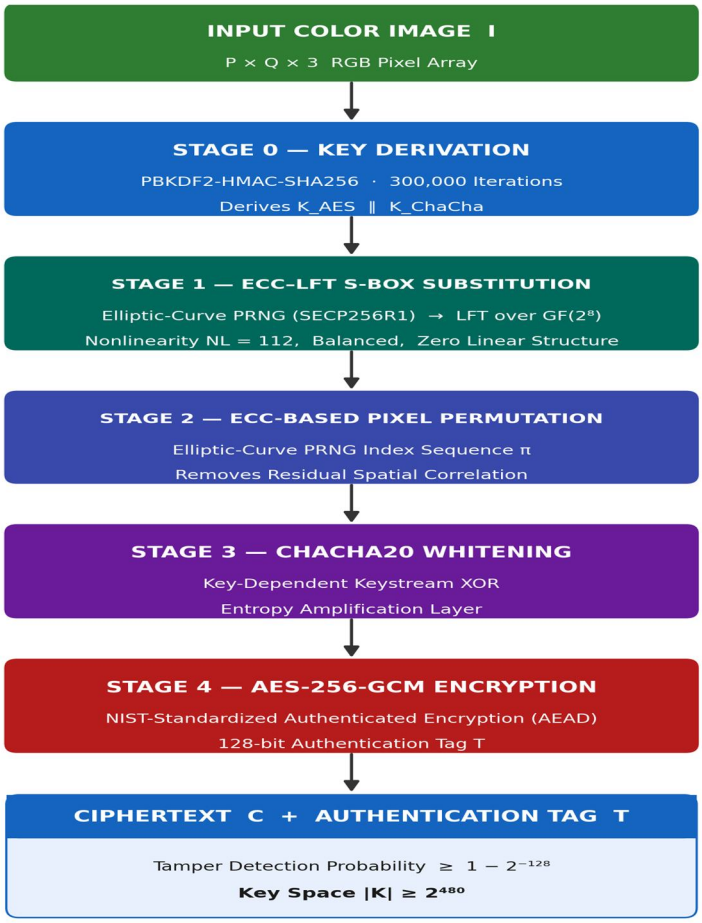


Fig. 1. Proposed four-stage hybrid encryption pipeline.

A. Key Derivation

A 128-bit random salt σ is generated, and PBKDF2 with HMAC-SHA-256 at 300,000 iterations derives 64 bytes of key material from the user password: (K_AES ‖ K_ChaCha) = PBKDF2-HMAC-SHA256(ρ, σ, 300000, 64). The first 32 bytes form K_AES and the remaining 32 bytes form K_ChaCha.

B. Dynamic ECC–LFT S-Box Construction and Substitution

A 128-bit secret seed η is sampled uniformly, and an ECC pseudo-random generator based on SECP256R1 derives four field elements [a, b, c, d]; if the determinant $a \cdot d \oplus b \cdot c = 0$, d is adjusted to enforce bijectivity. The S-box is defined by the linear fractional transformation $S[x] = (a \cdot x \oplus b) / (c \cdot x \oplus d)$ for x = 0, …, 255, with a zero denominator mapped to 1. Every pixel of the flattened image vector is substituted through S, and the inverse S-box is precomputed for decryption.

C. ECC-Based Pixel Permutation

The same seed η drives the PRNG to produce L pseudo-random values, where L = P×Q×3. A permutation index array π is obtained by sorting these values, and the substituted pixel vector is reordered according to π. Because π is regenerated deterministically from η, it need not be stored or transmitted as a separate table, and every pixel is relocated to a position that is computationally indistinguishable from a uniform random shuffle.

D. ChaCha20 Whitening

A 128-bit nonce is generated and ChaCha20, keyed with K_ChaCha, produces a keystream of length L that is XORed with the permuted pixel vector. This step suppresses residual statistical bias that permutation alone leaves in the marginal pixel distribution, before the final authenticated-encryption stage.

E. AES-256-GCM Authenticated Encryption

A 96-bit nonce is generated, and the whitened pixel stream is encrypted under AES-256-GCM with key K_AES to produce ciphertext C and a 128-bit authentication tag T. The output tuple (C, T, σ, nonces, π, η) is transmitted; the tag ensures that any bit-level modification of C is detected with probability at least $1 - 2^{-128}$.

F. Decryption and Tamper Detection

Decryption reverses each stage using the same password-derived keys: the tag T is verified before any pixel data is recovered, and verification failure aborts decryption immediately without exposing pixel data, providing full INT-CTXT security. On success, the ChaCha20 keystream is regenerated and removed, the inverse permutation π^{-1} is applied, and the inverse S-box S^{-1} recovers the original pixel values, which are reshaped to P×Q×3.

IV. RESULTS AND DISCUSSION

The proposed framework was implemented in Python 3.11 using the cryptography library for ECC operations on SECP256R1, AES-256-GCM, ChaCha20, and PBKDF2-HMAC-SHA256, NumPy for vectorised pixel operations, and Pillow for image I/O, and was evaluated on an Intel Core i7-12700H CPU (16 GB RAM) without GPU acceleration. Five standard 512×512, 24-bit RGB benchmark images — Lena, Baboon, Chile, Earth, and Women — were used, spanning smooth, high-frequency, and mixed spatial statistics. A fresh key, S-box seed, and set of nonces were generated independently for every image; no parameters were reused across runs.

A. S-Box Security Metrics

The cryptographic strength of the constructed S-boxes (four session instances, Proposed-1 through Proposed-4) was evaluated against six standard metrics, summarized in Table I together with six comparative schemes. All four S-boxes achieve nonlinearity (NL) of 112 — equal to the AES S-box and the practical optimum for 8-bit functions — together with mean Strict Avalanche Criterion (SAC) values within ±0.009 of the ideal 0.5, Bit Independence Criterion (BIC) values within 0.006 of 0.5, linear approximation probability (LP) of 0.0625, and differential approximation probability (DP) of 0.015625, matching the AES S-box and outperforming every compared elliptic-curve, Latin-square, and chaotic-map design. All four S-boxes are perfectly balanced with zero linear structure and a differential/linear branch number of 2, the minimum consistent with a bijective 8×8 S-box, confirming suitability for wide-trail cipher design.

Scheme	Method	NL	BIC	SAC	LP	DP
Proposed	EC–LFT	112	0.4986–0.5053	0.5000–0.5085	0.0625	0.015625
Ref. [20]	EC	107.50	0.5004	0.4873	0.1328	0.0390
Ref. [2]	EC	107	0.5064	0.4990	0.1250	0.0391
Ref. [9]	EC	111.25	—	0.4878	0.0703	0.0234
Ref. [21]	EC	107.25	0.5069	0.5024	0.1250	0.0390
Ref. [7]	Latin-Square	105.5	0.5087	0.5351	0.1406	—
Ref. [8]	Chaotic	106.75	—	0.4976	—	0.0391

Table I. S-Box Security Metrics: Proposed vs. State of the Art

B. Visual and Histogram Analysis

Fig. 2 shows representative plain images together with their cipher images; the encrypted outputs are visually indistinguishable from uniform noise and reveal no structural information about the originals. Figs. 3 and 4 compare the per-channel (R, G, B) histograms of the Earth and Chile images before and after encryption. The original histograms show the pronounced peaks characteristic of natural photographic content, while the encrypted histograms flatten into near-uniform distributions; chi-squared goodness-of-fit statistics of approximately 248.3 ± 6.2 remain well below the 95% critical value of 293.2, confirming that the ciphertext distribution is statistically indistinguishable from uniform random.

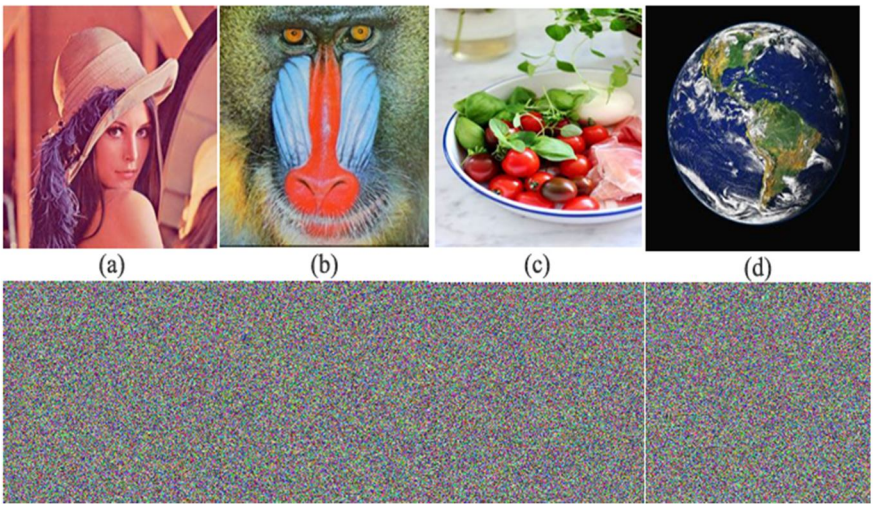


Fig. 2. (a)–(d) Original test images: Lena, Baboon, Chile, Earth. Corresponding cipher images appear as uniform noise.

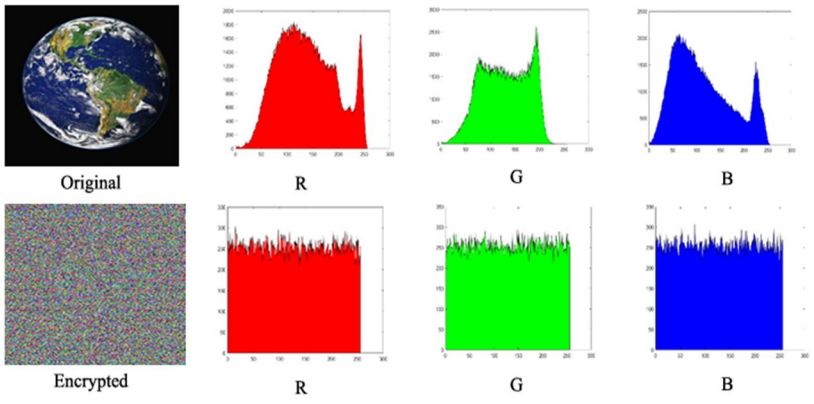


Fig. 3. Per-channel (R, G, B) histograms of the Earth image: original (top) vs. encrypted (bottom).

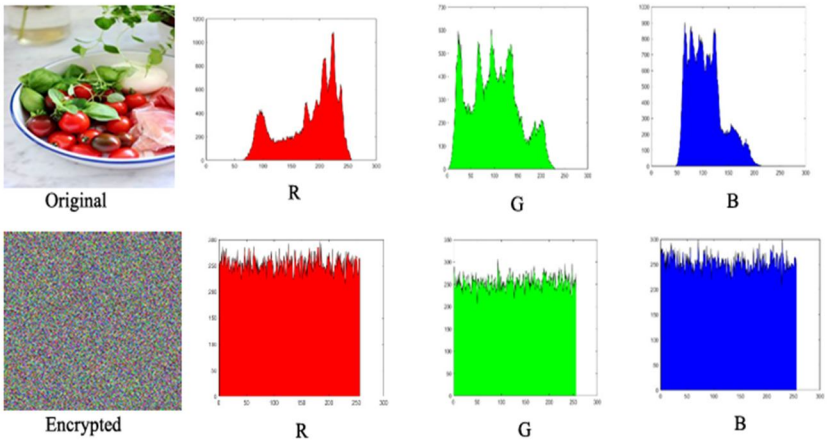


Fig. 4. Per-channel (R, G, B) histograms of the Chile image: original (top) vs. encrypted (bottom).

C. Correlation Analysis

Table II reports the Pearson correlation coefficient of adjacent pixels in the horizontal (H), vertical (V), and diagonal (D) directions before and after encryption for four test images. Original images exhibit strong correlation in the range [0.83, 0.97]; after encryption all coefficients fall below 0.055 in magnitude. Figs. 5 and 6 show the corresponding scatter plots for the Chile and Earth images: the tightly clustered diagonal patterns of the plaintext are replaced by uniformly dispersed clouds in the ciphertext, visually confirming decorrelation.

Image	Orig. H	Orig. V	Orig. D	Enc. H	Enc. V	Enc. D
Lena	0.9192	0.8324	0.8238	0.0356	0.0534	0.0364
Baboon	0.9324	0.9524	0.8805	0.0224	0.0125	0.0375
Chile	0.9245	0.9279	0.9275	0.0454	0.0153	0.0436
Earth	0.9674	0.9527	0.8934	0.0036	0.0037	0.0360

Table II. Correlation Coefficients: Original vs. Encrypted Images

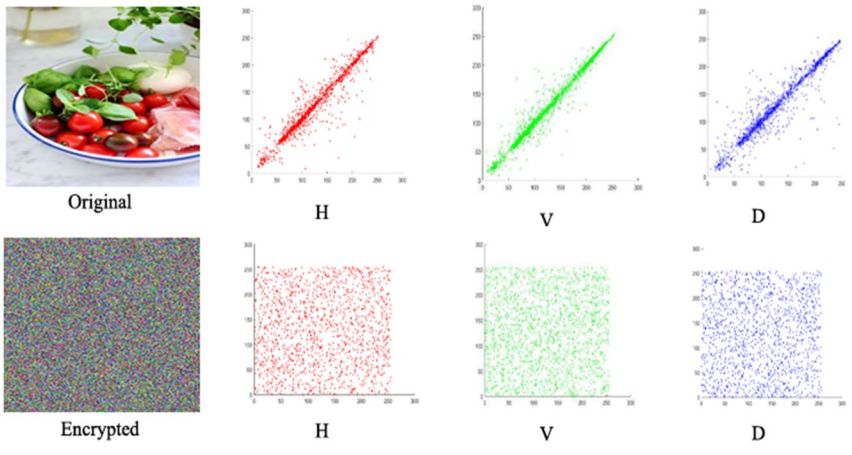


Fig. 5. Correlation scatter plots for the Chile image: original (top) vs. encrypted (bottom).

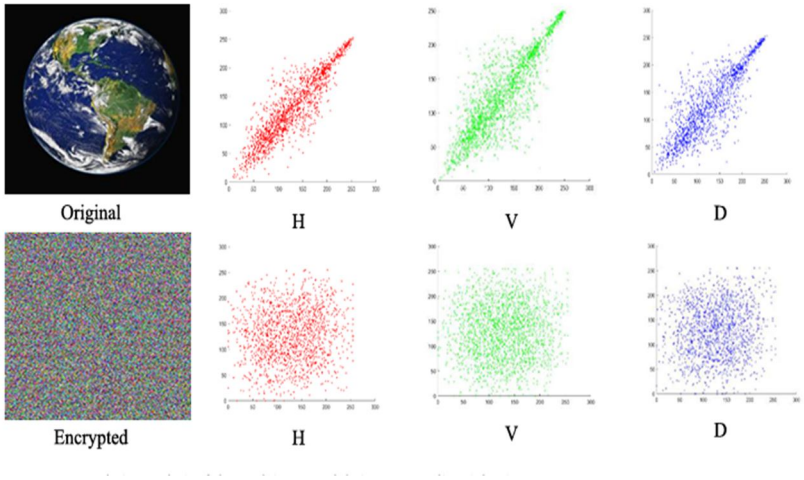


Fig. 6. Correlation scatter plots for the Earth image: original (top) vs. encrypted (bottom).

D. Information Entropy

Table III compares information entropy against four reference schemes. The proposed cipher attains 7.9990–7.9992 bits across all five test images, close to the ideal value of 8 and the highest among all compared methods, primarily attributable to the ChaCha20 whitening stage.

Scheme	Image	Entropy
Proposed	Lena / Women	7.9991
Proposed	Chile / Earth	7.9990
Proposed	Baboon	7.9992
Ref. [23]	Lena / Cameraman	7.9970 / 7.9848
Ref. [24]	Lena	7.9970
Ref. [25]	Lena / Baboon	7.9962 / 7.9971
Ref. [26]	Lena / Baboon	7.9970 / 7.9969

Table III. Information Entropy: Proposed vs. State of the Art

E. Differential Attack Resistance: NPCR and UACI

Table IV reports the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) obtained by encrypting each test image twice with a single-pixel plaintext difference. The proposed scheme achieves NPCR of 99.60%–99.63% and UACI of 33.41%–33.43%, closely bracketing the theoretical ideal values of 99.61% and 33.46% respectively, and meeting or exceeding all four compared schemes.

Scheme	Image	NPCR (%)	UACI (%)
Proposed	Lena	99.6324	33.4149
Proposed	Baboon	99.6125	33.4273
Proposed	Chile	99.6342	33.4227
Proposed	Earth	99.6027	33.4198
Ref. [5]	Lena	99.6067	33.5000
Ref. [27]	Lena	99.6233	33.6733
Ref. [28]	Lena	99.5681	33.4067

Table IV. NPCR and UACI: Proposed vs. State of the Art

F. Key Space, Authentication, and Discussion

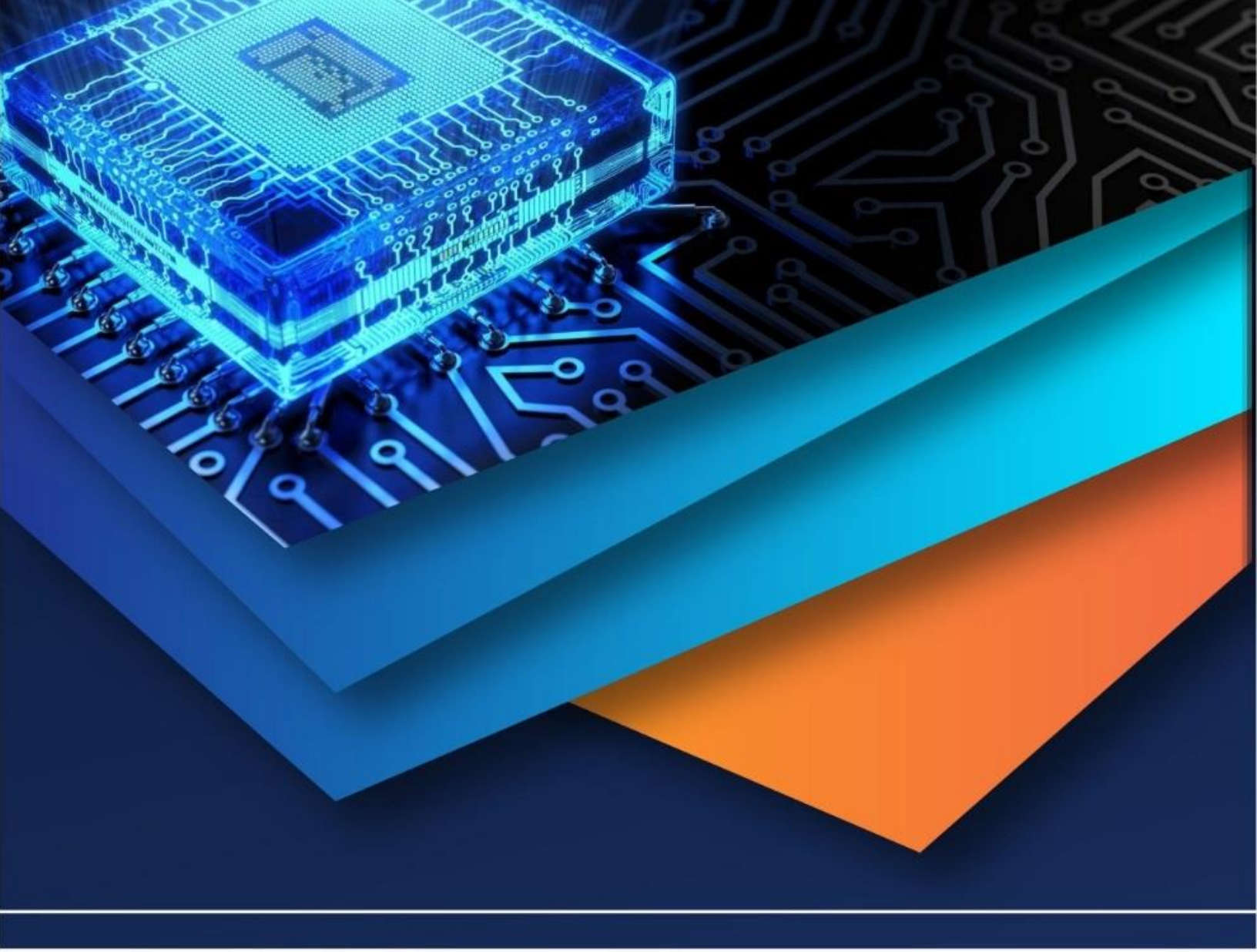
The effective key space combines the 128-bit salt, 128-bit S-box seed, 96-bit AES-GCM nonce, and 128-bit ChaCha20 nonce, giving $|K| \geq 2^{480}$, far beyond the reach of any classical or quantum adversary; 300,000 PBKDF2 iterations further limit password-guessing throughput to roughly 10^3 guesses per second. AES-256-GCM appends a 128-bit tag to every ciphertext, so that bit flips, truncation, or splicing invalidate the tag with probability at least $1 - 2^{-128}$ and are rejected before any pixel data is decoded — a property absent from every non-AEAD scheme compared in this paper. Relative to the ECC–LFT baseline, the main overhead is the per-pixel elliptic-curve computation used for permutation, which is acceptable for batch or offline encryption but would benefit from GPU parallelization for real-time video; the security analysis presented here is empirical, and a formal IND-CCA2 proof is left for future work.

V. CONCLUSION

This paper presented a hybrid image-encryption framework that combines an ECC-driven Linear Fractional Transformation S-box with AES-256 in Galois/Counter Mode. The four-stage pipeline — dynamic S-box substitution, ECC-based pixel permutation, ChaCha20 whitening, and AES-256-GCM — achieves near-ideal information entropy (7.9990–7.9992), NPCR of 99.60%–99.63%, UACI of 33.41%–33.43%, and adjacent-pixel correlation below 0.06, while the constructed S-boxes attain optimal nonlinearity of 112 with zero linear structure. Comparative evaluation against six state-of-the-art ECC- and chaos-based schemes shows competitive or superior statistical security, and the embedded 128-bit authentication tag provides cryptographic tamper detection that is absent from all compared designs. The framework offers a practical path toward image encryption that is simultaneously confidential and verifiably authentic, suited to telemedicine, satellite communication, and digital forensics. Future work will target GPU-accelerated real-time encryption, post-quantum key encapsulation, and a formal security proof.

REFERENCES

[1] S. S. Jamal, Z. Bassfar, O. Lahlou, A. Aljaedi, and M. M. Hazzazi, “Image encryption based on elliptic curve points and linear fractional transformation,” IEEE Access, vol. 12, pp. 53335–53347, 2024.
[2] M. I. Haider, A. Ali, D. Shah, and T. Shah, “Block cipher’s nonlinear component design by elliptic curves: an image encryption application,” Multimed. Tools Appl., vol. 1, pp. 1–26, 2020.
[3] S. Ibrahim and A. M. Abbas, “Efficient key-dependent dynamic S-boxes based on permutated elliptic curves,” Inf. Sci., vol. 558, pp. 246–264, 2021.
[4] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, “An image encryption scheme based on elliptic curve pseudo random and advanced encryption system,” Signal Process., vol. 141, pp. 217–227, 2017.
[5] H. U. Rehman, M. M. Hazzazi, T. Shah, A. Aljaeti, and Z. Bassfar, “Color image encryption by piecewise function and elliptic curve over the Galois field GF(2^n),” AIMS Math., vol. 9, no. 3, pp. 5722–5745, 2024.
[6] A. Razaq, A. Ullah, H. Alolaiyan, and A. Yousaf, “A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers,” Wireless Pers. Commun., vol. 116, no. 4, pp. 3165–3190, 2021.
[7] Z. Hua, J. Li, Y. Chen, and S. Yi, “Design and application of an S-box using complete Latin square,” Nonlinear Dyn., vol. 104, no. 1, pp. 807–825, 2021.
[8] Z. Jiang and Q. Ding, “Construction of an S-box based on chaotic and bent functions,” Symmetry, vol. 13, no. 4, p. 671, 2021.
[9] H. ur Rehman, T. Shah, M. M. Hazzazi, A. Alshehri, and B. Zaid, “Mordell elliptic curve based design of nonlinear component of block cipher,” Comput. Mater. Continua, vol. 73, no. 2, pp. 2913–2930, 2022.
[10] A. M. Hilal, F. N. Al-Wesabi et al., “Design of nonlinear components over a Mordell elliptic curve on Galois fields,” Comput. Mater. Continua, vol. 71, no. 1, pp. 1313–1329, 2022.
[11] A. A. A. El-Latif and X. Niu, “A hybrid chaotic system and cyclic elliptic curve for image encryption,” AEU Int. J. Electron. Commun., vol. 67, no. 2, pp. 136–143, 2013.
[12] N. Jia, S. Liu, Q. Ding, S. Wu, and X. Pan, “A new method of encryption algorithm based on chaos and ECC,” J. Inf. Hide. Multimed. Signal Process., vol. 7, pp. 637–643, 2016.
[13] O. Reyad, Z. Kotulski, and W. M. Abd-Elhafiez, “Image encryption using chaos-driven elliptic curve pseudo-random number generators,” Appl. Math. Inf. Sci., vol. 10, no. 4, pp. 1283–1292, 2016.
[14] J. Wu, X. Liao, and B. Yang, “Color image encryption based on chaotic systems and elliptic curve ElGamal scheme,” Signal Process., vol. 141, pp. 109–124, 2017.
[15] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, “Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system,” Opt. Lasers Eng., vol. 124, p. 105816, 2020.
[16] L. C. Washington, Elliptic Curves: Number Theory and Cryptography. Boca Raton, FL, USA: CRC Press, 2008.
[17] B. Kaliski, “PKCS #5: Password-based cryptography specification version 2.0,” IETF, Tech. Rep. RFC 2898, 2000.
[18] D. J. Bernstein, “ChaCha, a variant of Salsa20,” in Workshop Record of SASC 2008, 2008, pp. 3–5.
[19] M. Dworkin, “Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC,” NIST, Tech. Rep. SP 800-38D, 2007.
[20] M. I. Haider, T. Shah, A. Ali, D. Shah, and I. Khalid, “An innovative approach towards image encryption by using novel PRNs and S-boxes modeling techniques,” Math. Comput. Simul., vol. 209, pp. 153–168, 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY