ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug864

Advanced Image Encryption: Utilizing SHA-256 Empowered ECC and LFT Approach for Enhancing Image Security

Surekha Samsani[1]; Deepti Asi[2]

[1]Assistant Professor, Department of CSE, UCEK(A) JNTU Kakinada, Andhra Pradesh
[2]Student, Master of Computer Applications, UCEK(A) JNTU Kakinada, Andhra Pradesh

Publication Date: 2025/08/29

Abstract: The proliferation of picture use across several sectors is directly attributable to the exponential growth of digital technology. Confidential data transfer over networks is becoming commonplace. Images privacy so becomes extremely important, and they must be shielded from any illegal user access. In order to provide a highly secure and resilient method of picture encryption, this study introduces a hybrid approach that combines SHA-256 with ECC and LFT. An ECC private key is derived from a SHA-256 hash of the image filename, which seeds pseudo-random generators for all cryptographic elements. The image undergoes LFT-based transformation for nonlinearity, followed by S-box substitution and XOR-based diffusion using ECC-derived values. Essential metadata is stored for accurate decryption and integrity verification. Security is evaluated through metrics like Information Entropy, Correlation Coefficient assessment, PSNR, UACI and NPCR and SAC,BIC confirming that the method significantly strengthens Encryption Against different Attacks.

Keywords: *Image Encryption, Secure Hash Algorithm (SHA), Elliptic Curve (EC), Linear Fractional Transformation (LFT), Substitution Box (S-Box).*

How to Cite: Surekha Samsani; Deepti Asi (2025), Advanced Image Encryption: Utilizing SHA-256 Empowered ECC and LFT Approach for Enhancing Image Security. *International Journal of Innovative Science and Research Technology*, 10(8), 1530-1538. https://doi.org/10.38124/ijisrt/25aug864

I. INTRODUCTION

Today, data and information communication are seen as valuable assets for both individuals and organizations in the current digital age [9]. They are an integral part of technology life in general. With the rise of cloud computing, the need to ensure the confidentiality of digital photographs sent to authorized recipients has grown in importance [1]. Countless industries rely on images for anything from internet communication and multimedia systems to medical imaging, financial transactions, and military communication. The need for safe picture transmission is growing at an unprecedented rate due to the proliferation of online communication and the ever-increasing volume of sensitive information being sent over the web. The fast expansion of smartphone use, social media, and cloud computing has recently increased the need of adequately protecting users' photos during storage and transmission [5]. Data encryption is the cornerstone of information security. An approach to security known as "image encryption" transforms clearly identifiable pictures into ones that are obscured by noise [18]. Conventional block ciphers like DES, IDEA, and AES aren't great choices for encrypting images because of their unique storage structure and inherent redundancy [20]. Even though this method encrypts data quickly, it relies on an algorithm that isn't up to the standards of today's encryption systems[11].

II. RELATED WORK

Recent efforts have aimed to improve the security of cryptographic systems. An innovative picture encryption method that uses ECs over a binary extension field (BEF) and therefore minimizes computing effort was suggested by H.U.Rehman et al. [2].Ibrahim et al.[6] proposed Using permuted elliptic curves (ECs) to create key-based changing S-boxes helps reduce computing costs. A. H. Zahid et al. [19] proposed an image encryption process that uses a newly designed S- box based on a modular approach involving transformation, modular inverse, and permutation. Lu Qing, Zhu Chong, and Deng Xiang. An effective and safe approach for encrypting images using chaotic S- Boxes was suggested by Z. E. Dawahdeh et al. in [10].[15] suggested an improved method of picture encryption that is both more secure and more resistant to hacking: ECCHC, which combines Elliptic Curve Cryptosystem with Hill Cipher. Other approaches include image encryption schemes utilizing PRNG and AES modules [17]. This paper proposes the concept of Elliptic Curve Cryptography was a method uses elliptic curves, which are mathematical curves useful for secure encryption. One of

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug864

the successful public key encryption methods is elliptic curve cryptography (ECC), which was suggested independently by Miller (1985) and Koblitz (1987) [15]. ECC uses less memory and power than other techniques like RSA while yet maintaining a small key size [15].

Finite fields are usually used in EC-based methods in order to reach the target level of security [1]. In this paper, a hybrid method that is based upon elliptic curves over a finite field will be presented. Elliptic curve (EC) cryptography is the light weight, high performance, and safe manner to implement the computer cryptographic procedures [2]. The ECC can provide the reduction of cryptographic algorithms which makes it efficient and safe. This work is based on a secure key generation and integrity validation on the basis of SHA-256. It guarantees uniqueness, repeatability, and tamper- resistance of encryption, which makes the whole image encryption-decryption pipeline stronger and secure. Linear Fractional Transformations (LFTs) are a kind of bijective transformations that are famous in terms of providing the great non-linearity and complexity in the process of encryption and consequently, by performing pixel scrambling, increasing the security of the system.

Lastly, non-linearity via S-box substitution, and diffusion via XOR that is highly secure. The secured image and data of the metadata are stored securely or transferred.

III. PRELIMINARIES

In this section, the basic idea of ECs, SHA-256, Linear Fractional Transformation (LFT) as important ingredients of the proposed scheme is discussed.

➢ *Elliptic Curve*

Elliptic curves are mathematical structures, which are described by equation of

$$y^2=x^3+ax+b \quad (1)$$

In which a and b are fixed values. The curves in question are definitely not known as the elliptic curves. They are called such, because they are defined by cubic equations, as in computing the circumference of an ellipse. In our application we may restrict ourselves to equation. This is referred to as the general form of the elliptic curves and the curve meets the requirement so as to be non-singular.

$$4a^3+27b^2\neq 0 \quad (2)$$

This makes the curve smooth enough, such that it can be applied to define group operations, which in mathematical terms is the actual foundation of the Elliptic Curve Cryptography (ECC).

➢ *Secure Hashing Algorithm-256*

Secure Hash Algorithm (SHA), also known as Secure Hash Standard (SHS) is a one-way hash which reduces messages of any variable length into a fixed- length summary, which was developed by the National Institute of Standards and Technology (NIST) to compute various digest lengths. The SHA-256 is the second generation a very secure one way hash functional that is meant to ensure that it is difficult to retrieve the original message having the hash value. It guarantees the security strength of messages in cryptography and resolving a SHA-256 hash value entails 2256 efforts. The algorithm works in more than 64 rounds under non- linear functions, cyclic rotations and round constants.

➢ *Linear Fractional Transformation (lft)*

An Mobius transformation is a mathematical expression called the Linear Fractional Transformation (LFT):

$$T(x) = \frac{a \,.\, x + b}{c \,.\, x + d} \quad (3)$$

In the case of a, b, c, d as constants with a value of Denominator c.x+d not equal to 0. This transformation may be characterized on either the real or the complex numbers and finds extensive investigation in complex analysis, geometry and applied mathematics. LFT are injective (one-to-one and onto) mappings of the extended complex plane or, equivalently inverses exist: a mapping will have an inverse inverse: an LFT mapping is to have a unique preimage, its inverse, for any given output. This inevitability is essential where an encryption system is transformations, where a perfect reconstruction of the original information is possible.

➢ *Substitution Box(S-Box)*

The Substitution box (S-box) is a fixed or key-specific look up table used to replace an input (frequently a byte or pixel value) with a different value. Development of robust and multifunctional S-boxes is a significant element in the design of significant cryptography systems because they are an important part in delivering nonlinear modification of measuring the performance of a well-organized crypto algorithm [1].

Their basic unit is the Substitution box (S-box) which appears in most symmetric-key block ciphers. The capability to produce speedy dynamic S-box is the most optimistic criteria to come up with efficient cryptosystems and contributes significantly in the non- linear transformations applied in evaluation of well- devised crypto-algorithms [3].

➢ *XOR Operation*

The exclusive or (abbreviated XOR) is a basic binary axiom, which has strong good applications inmany encryption techniques because of its easiness and real utility. XOR is a binary operator that consumes two bits and produces one output. 1 in the case they are different, or 0 in the case they are equal.

XOR is applicable in the process of encryption referred to as combining the plaintext information with a key. This is reversible and hence the XOR operation can be repeated with the same key to access the initial data in the ciphertext.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug864

IV. PROPOSED ENCRYPTION SCHEME

Images are very important visual information in a large variety, including military, business, medical, entertainment, etc. where defined security during transmission is necessary, at least. To guard against any unauthorized access or modification, protection of this sensitive data is needed. Multiple mathematical algorithms and styles of encryption are often used to ensure confidentiality, integrity or safety of images. These cryptographic methods assist in standardizing the security operations which ensures that the images can be secured at all times during storage and communication. Particularly, the proposed approach would entail the encryption of an image I of size p x q x 3 with p as the number of rows and q as the number of columns and 3 represents RGB color elements. The degree of distortion the image experiences indicates how successful the encryption method is. The encryption protocol has a number of steps.

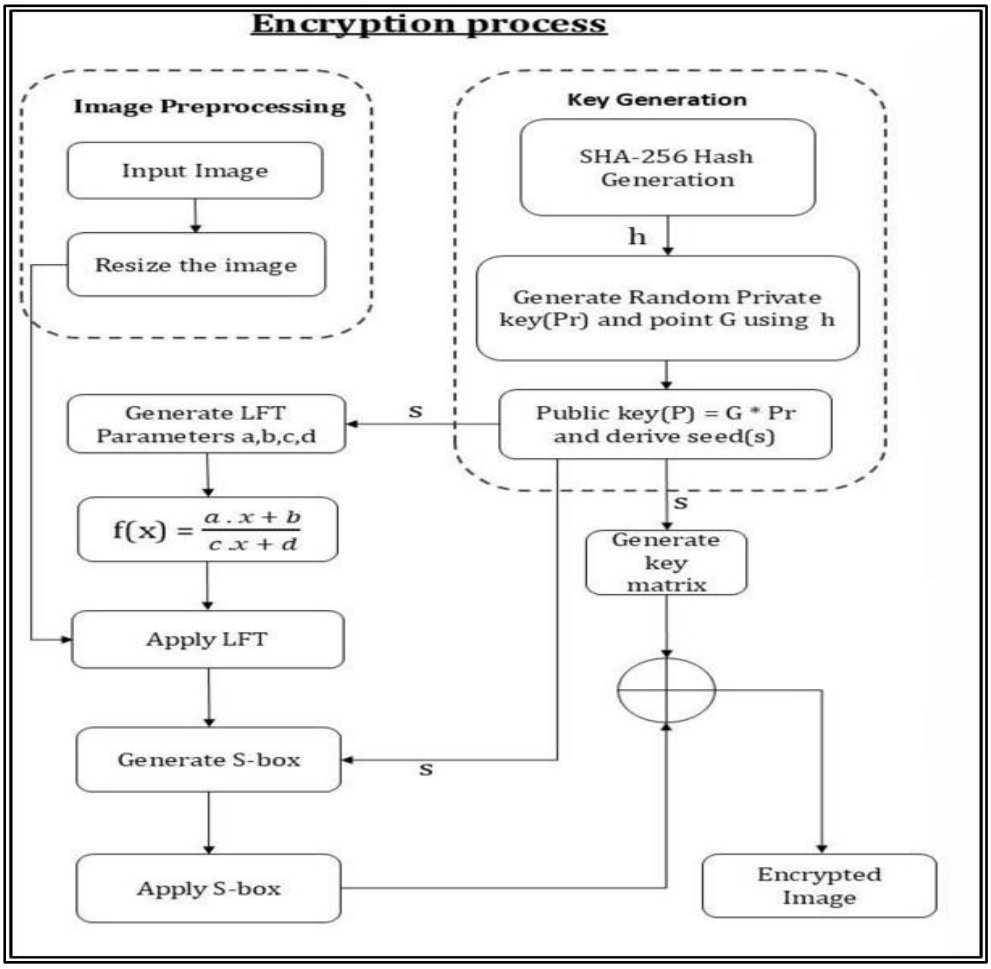

Fig 1 Encryption Process of Proposed System

- The encryption algorithm procedure starts with input picture loading into the memory and standard size checking of the picture to process it together to guarantee uniformity.
- SHA-256 hash is generated based on the image file name which is securely used as the basis of key generation.
- One comes up with a private key that employs elliptic curve cryptography (ECC) and generates the associated public key. The x-value of the public key provides a random input to make it dependent of the key.
- A reversible non-linear mathematical transformation is also performed on the image applying random parameters of the Linear Fractional Transform (LFT).
- A public key seed is used to build an S-Box that confuses pixel values and a key matrix that would be used in the XOR step in the future is also produced.
- The image is subjected to the Linear Fractional Transformation, and the pixel values are changed in a complicated and unpredictable manner.
- The generated S-Box in turn is used in a substitution process to further improve security and withstand statistical analysis.
- The substituted image is then bitwise XORed with the key matrix in order to introduce diffusion so that small alterations to the input cause substantial differences in the output text of the encryption.
- The image is written in the encrypted form and formatted as PNG, whereas the most relevant encryption metadata is saved in a NumPy file that facilitates the process of decryption.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug864

V. PROPOSED DECRYPTED SCHEME

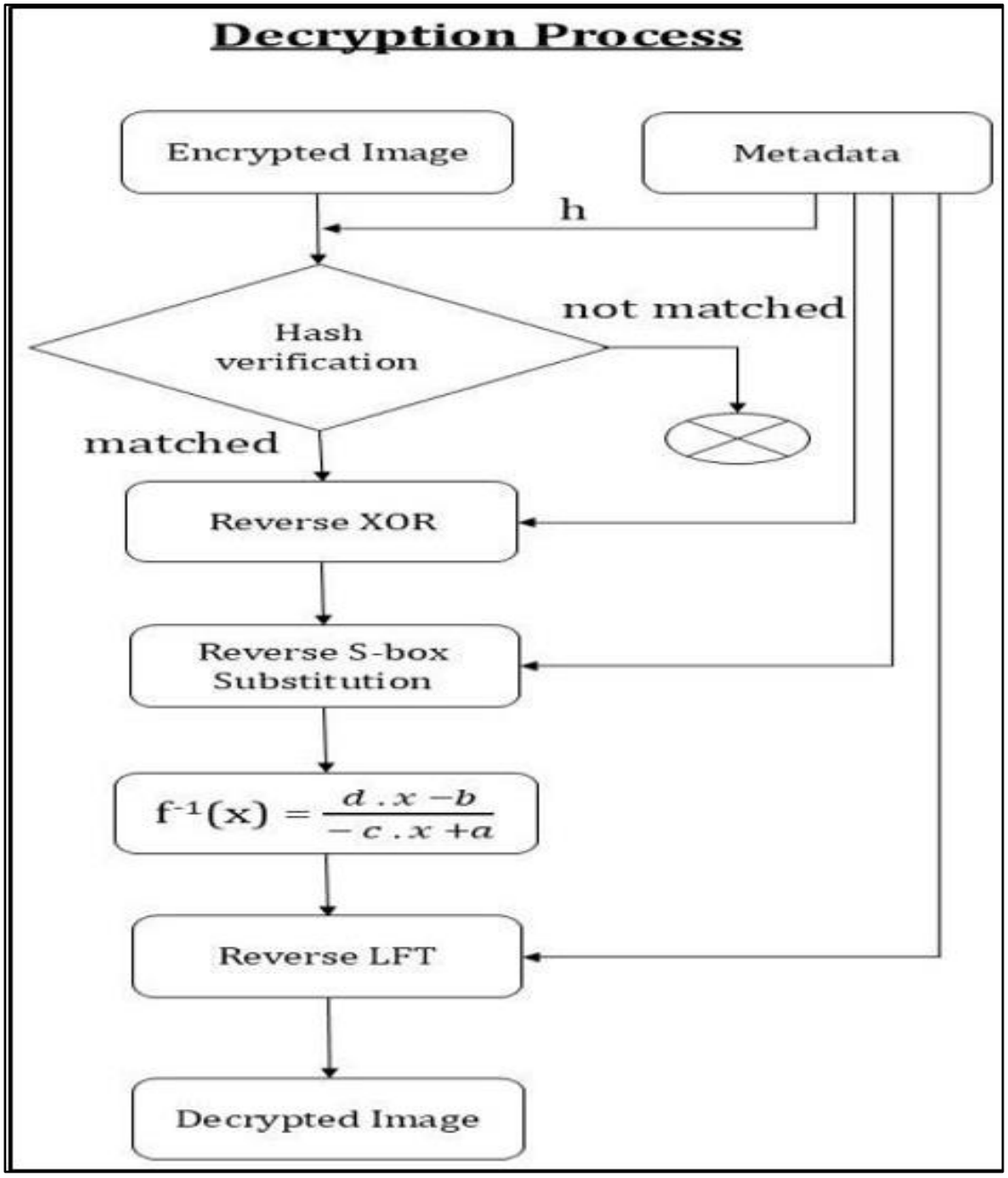

Fig 2 Decryption Process of Proposed System

- The image file that is encrypted and the metadata file are loaded. The encoded picture is processed into RGB numpy array to be further manipulated.
- The program verifies the existence of the encrypted files of the image and metadata and their validity in their formats. It also checks the validity of the files with comparison of the stored SHA-256-hash with the new one calculated to ensure that the files were not distorted.
- The required decryption parameters, such as the LFT values, S-Box, key matrix, and the stored transformed float matrix, are extracted from the metadata file.
- The diffusion effect generated during the encryption process is reversed by applying a bitwise XOR operation between the encrypted picture and the key matrix.
- The inverse of the original S-Box is applied to the result of the XOR operation to undo the substitution step and recover the pixel values closer to their original state.
- Using the saved LFT parameters, the system performs the reverse Linear Fractional Transform to mathematically restore the image structure to its original form.
- The decrypted floating-point pixel values are scaled back to the standard 8-bit integer format (0-255) to obtain a properly formatted image.
- The fully decrypted image is saved in PNG format in the working directory, with the filename modified to include the suffix '_decrypted' to distinguish it from the original and encrypted files.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug864

VI. PERFORMANCE ANALYSIS OF S- BOXES

The S-boxes designed in the process of cryptography were tested, by employing the available and renowned parameters like Strict Avalanche Criterion (SAC) and Bit Independence Criterion (BIC). These findings make it feasible to access the S-box's
efficacy. Below are the performance indices of the S-boxes that were produced.

➢ *Strict Avalanche Criterion (SAC)*

The output bits' response to an impending change in the input bits is examined using the strict avalanche criterion (SAC) [1]. The SAC is said to be satisfied when all the element of the SAC matrix lie near a small domain of 0.5 [1]. The SAC results of the resulting S-boxes are shown in Table 1, along with comparisons to other schemes, demonstrating that the suggested S-boxes meet the SAC requirements.

➢ *Bit Independence Criterion (BIC)*

Bit Independence Criterion (BIC) is an evaluation of the correlation pieces created by the 8-bit constitution function [1]. This criterion verifies the correlation of the nth and mth output bits when there is a slight change on the ith input bit. When the BIC matrix's contents are close to 0.5, an S-box is considered to meet the BIC criteria [1]. The results of the BIC of the resultant S-boxes and a comparison with other existing schemes in terms of BIC, is given in Table 1, it can be seen that the proposed S-boxes satisfy the BIC criteria.

Table 1 Experimental Findings and Comparisons of Potential S-Boxes.

S-box	Scheme	SAC	BIC
Proposed-1	EC	0.5002	0.4999
Proposed-2	EC	0.5001	0.5000
Proposed-3	EC	0.4999	0.5000
Proposed-4	EC	0.5001	0.4999
Ref [3]	EC	0.4990	0.5063
Ref [8]	EC	0.4873	0.5063
Ref [21]	EC	0.5025	0.5069

VII. RESULT ANALYSIS

➢ *Histogram Analysis*

Histograms visualize pixel value frequencies in images, where plain images (PIs) have varied frequencies and well-encrypted images (CIs) should display uniform frequencies to resist frequency-based attacks. It is possible to see how the distribution of pixel values has changed by looking at the encrypted pictures' histogram. Figure 3 illustrates the difference between the original and encrypted images, which shows that the encrypted images' histograms have a uniform distribution. Based on these visual cues, it seems that the suggested approach is quite resistant to statistical assaults.

➢ *Correlation Coefficient*

Adjacent pixels in plain images (PIs) often exhibit high correlation due to redundancy or gradual changes in pixel values. However, well-encrypted cipher images (CIs) should minimize this correlation to the statistical attacks. Correlation data among horizontally, vertically, and diagonally adjacent pixels for PIs versus CIs are presented in Table.2, along with correlation plots for chili in Fig. 4. The correlation coefficients (corr) are computed using Equation:

$$corr = \frac{mean\,(X-\mu x).(Y-\mu y)}{\sigma x.\sigma y} \quad (4)$$

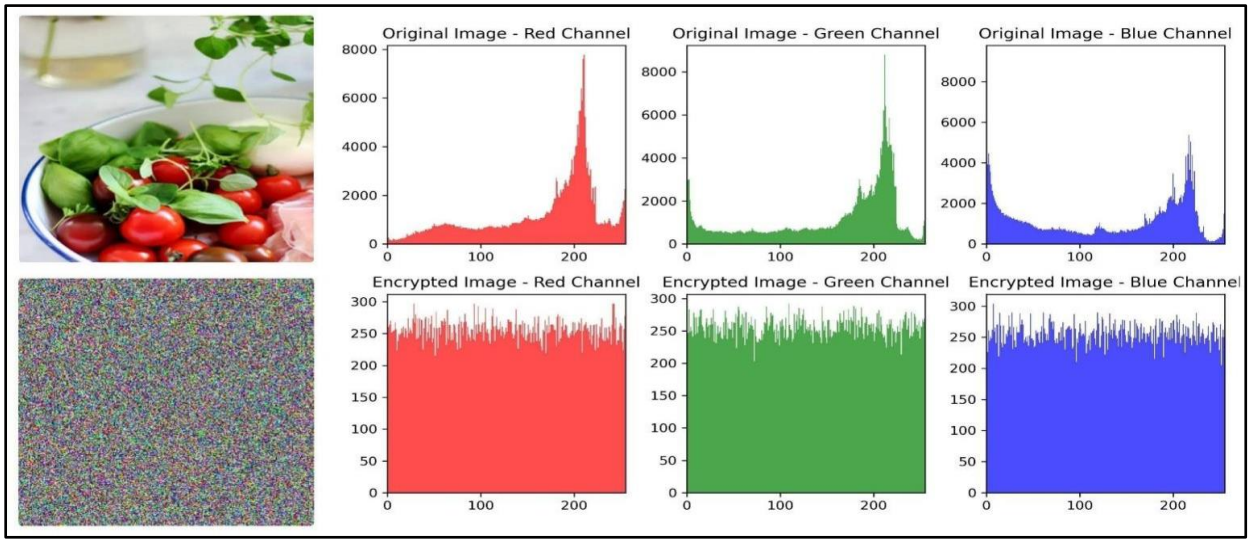

Fig 3 Histogram Analysis of Original and Encrypted Image of Chili.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug864

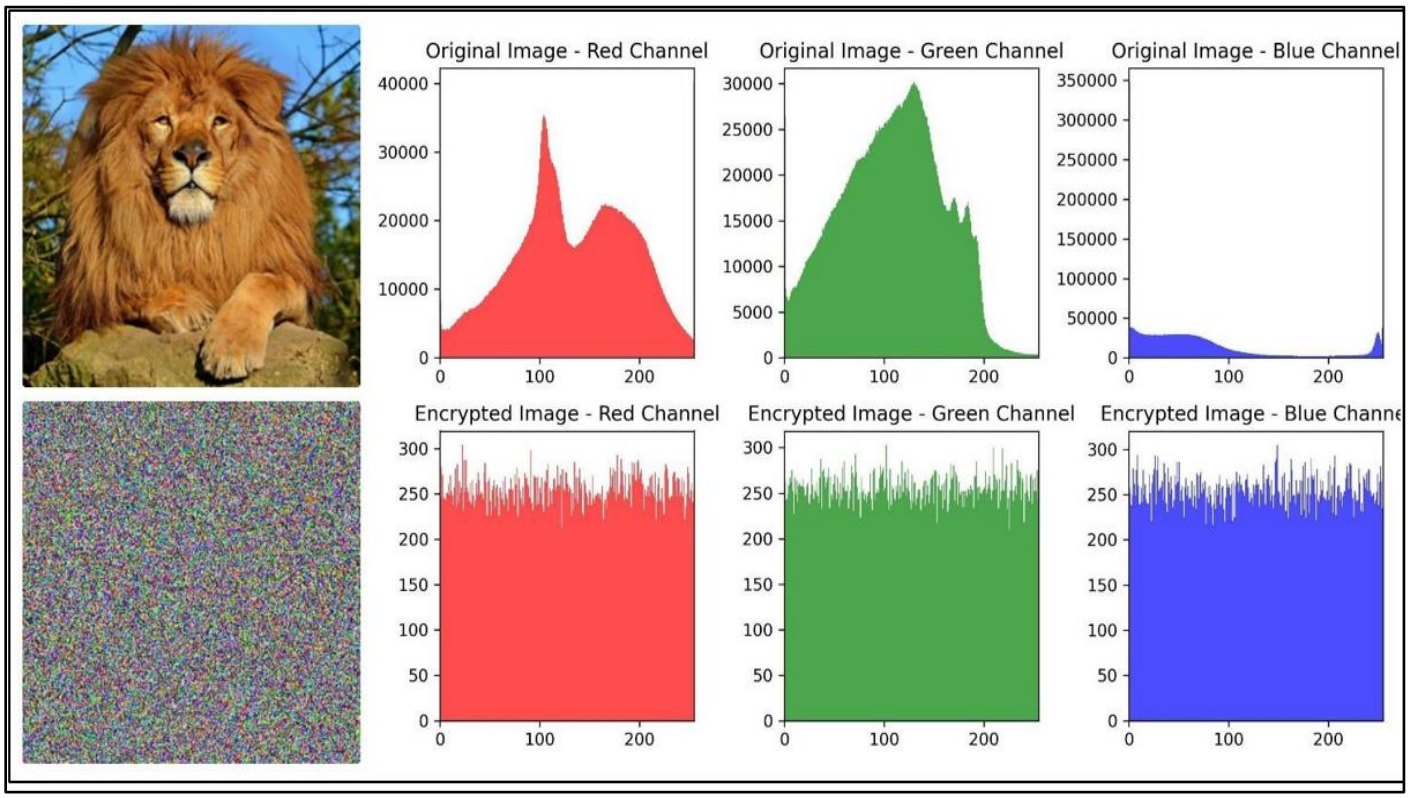

Fig 4 Histogram Analysis of Original and Encrypted Image of Lion.

where μx represents the mean of X and μy represents the mean of Y, and σx and σy are the standard deviations of X and Y, respectively.

Table 2 Correlation Analysis of Plain Image (PI) and Ciphered Image (CI)

Image	Horizontal		Vertical		Diagonal	
	PI	***CI***	***PI***	***CI***	***PI***	***CI***
Lena	0.9586	0.0091	0.9644	-0.0099	0.9320	0.0097
Baboon	0.8953	-0.0105	0.8893	0.0053	0.8481	0.0082
Chili	0.9871	0.0050	0.9905	-0.0024	0.9810	-0.0075
Earth	0.8920	-0.0023	0.8557	0.0007	0.8184	0.0002

➢ *Information Entropy*

Entropy is one of the statistical scalar features that are used to evaluate photo encryption. The patterns that appear most often are shown. The degree of unpredictability is measured by it, which is dependent on the probability of the pixel values [15]. In the context of image encryption, maximizing entropy in the cipher image (CI) is desirable as it indicates higher unpredictability and complexity, making it more resistant to cryptographic attacks. The proposed encryption algorithm achieves this by increasing the entropy of CI

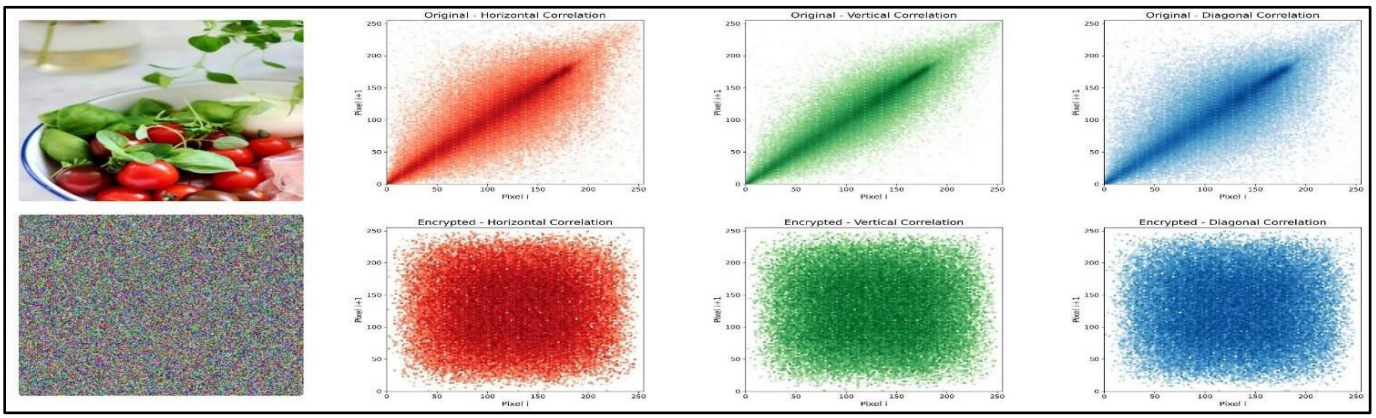

Fig 5 Correlation Analysis of the Chili Original and Encrypted Image

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug864

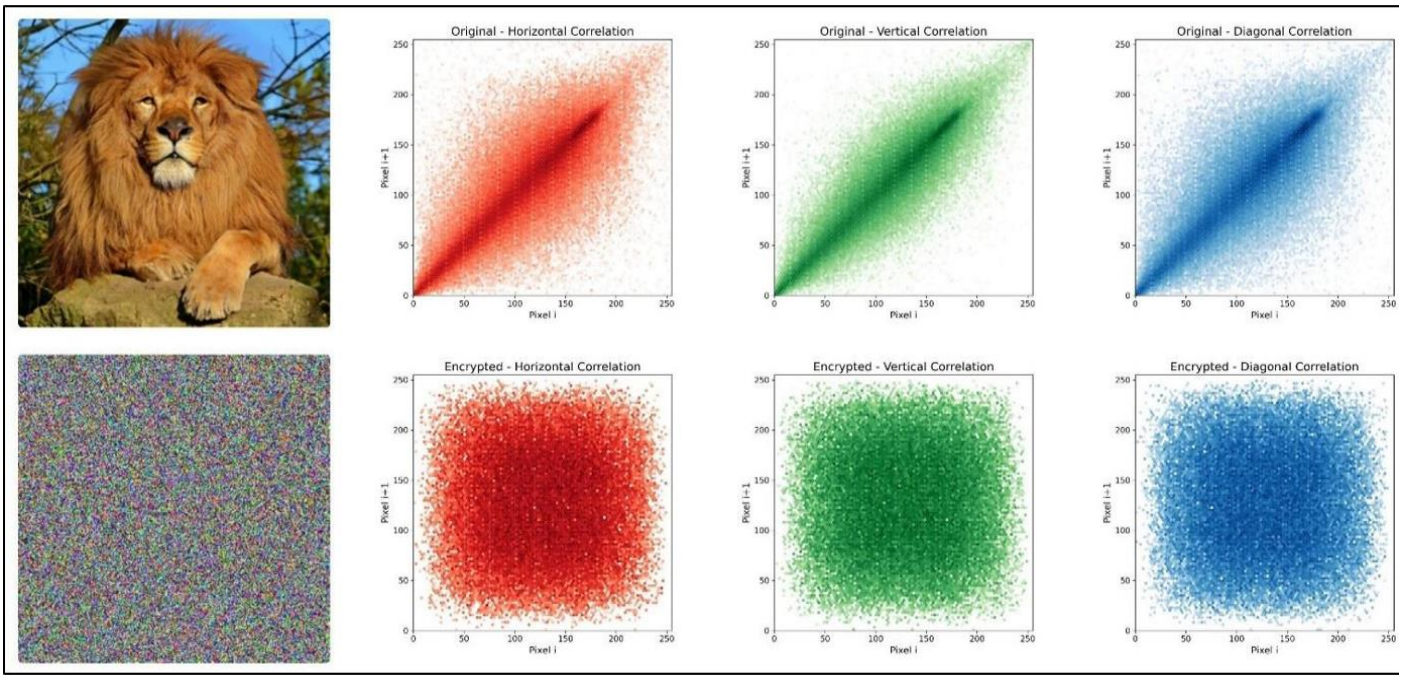

Fig 6 Correlation Analysis of the Lion Original and Encrypted Image

pixels compared to their corresponding plain images (PIs). Entropy is calculated using Equation:

$$H(t)=\sum_{q=0}^{2N-1} p(t_q)*log\ [\ ^{1}_{p(t_g)}]\quad (5)$$

➢ *Peak Signal-to-Noise Ratio (PSNR)*

An encrypted image's Peak Signal-to-Noise Ratio (PSNR) can be used to assess its integrity. It calculates the difference between the two (the encrypted where p denotes the probability of each grayscale value tq and original pictures) and the ratio of the noise power to the maximum power of the signal (the original picture)[17] in decibels (dB). Table 4 displays the PSNR values for the present systems and the suggested system. When comparing the plain image (PI) with the cipher image (CI), PSNR shows how consistent the pixel changes are. The formula is used to determine PSNR:

$$PSNR = -10\ log\ (\frac{MSE}{P_2}) \quad (6)$$

where P is the maximum pixel value (255 for 8-bit pixels) and MSE is Mean Squared Error.

Table 3 Comparison of the Entropy Results of the Ciphered Images

Image	Our	Ref. [4]	Ref. [5]	Ref. [8]	Ref. [20]
Baboon	7.6302	7.9974	7.9976	7.9929	7.9969
Cameraman	7.6280	-	7.9973	7.9929	
Lena	7.6283	7.9971	-	7.9957	7.9971
Peppers	7.6282	-	7.9969	-	

Table 4 Comparison Results of PSNR

Image	Our	Ref. [2]	Ref. [15]
Baboon	10.3994	27.7937	-
Cameraman	9.1076	28.5427	9.4531
Lena	10.0504	27.5912	12.1861
Peppers	6.4941	-	8.9167

➢ *NPCR & UACI*

Metrics such as the Unified Averaged Changed Intensity (UACI) and the Number of Pixel Change rate (NPCR) are used to evaluate how well an encryption technique modifies picture data. The non-perturbative pixel ratio (NPR) is a measure of how many encrypted pixels change in response to a random change in the original image's pixel value [13]. UACI is a measure of how much the encrypted image's pixel value changes when the source image's pixel value is randomly altered [13]. The fraction of pixels in cipher images (CIs) Q1 and Q2 that are different from one another... The computation is based on comparing adjacent pixels in two encrypted pictures made from original, plain images that vary by a single pixel. One way to determine it is by using the Equation:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug864

$$NPCR\ (Q_1, Q_2) = \Sigma_{i,j} \frac{Diff\ (i,j)}{Tp} * 100\% \quad (7)$$

The average pixel intensity difference between adjacent pixels in two cipher pictures is computed using UACI. The total change in pixel values over the whole picture is measured by this metric. This is calculated by using the Equation:

$$UACI\ (Q_1, Q_2) = \Sigma_{i,j} \frac{|Q_1(i,j) - Q_2(i,j)|}{maxPV * TP} * 100 \quad (8)$$

Improving resistance to differential attacks requires evaluating the suggested encryption method's correlation with the original picture data, which these metrics assist with [1]. Scores for the suggested encryption technique, as well as NPCR and UACI, are shown in Table 5, which also includes scores for different color pictures. Greater pixel change rates between encrypted pictures due to minor input changes are indicated by a higher NPCR score, which is desired.

Table 5 Comparison of NCPR and UACI Analysis with Existing Schemes.

Scheme	Name	NPCR	UACI
Proposed	EC	99.5483	53.3244
Proposed	EC	99.5651	48.7242
Proposed	EC	99.5865	45.4214
Proposed	EC	99.7757	54.3110
Ref [2]	EC	99.5972	33.4281
Ref [5]	Chaotic	99.6368	33.5591
Ref [6]	Chaotic + EC	99.6600	33.4800

➢ *Time Complexity*

An important issue with picture encryption is the time it takes to encrypt the image. An algorithm's encryption time is dependent on a number of parameters, including operating system, hardware specifications, programming language, and the expertise of the coder, among others. Here are the findings obtained using the suggested strategy, as shown in Table 6.

Table 6 Time Complexity of Proposed Method for Different Image

Image	Time(s)
Baboon	0.1072
Cameraman	0.0989
Earth	0.0710
Lena	0.0960
Lion	0.0959
Peppers	0.0922

VIII. CONCLUSION

The suggested picture encryption solution combines SHA-256 hashing for seed derivation and verification with ECC safe key creation. LFT introduces nonlinear changes in pixel values to enhance confusion. A dynamically generated S-box based on ECC improves substitution strength. XOR operation with a pseudo- random key matrix adds diffusion and unpredictability to the encrypted image. During decryption, SHA-256 verifies the seed to maintain data integrity. Required metadata such as LFT parameters, key matrix, and S-box are securely stored for accurate image reconstruction. The hybrid approach ensures high security, reversibility, and computational efficiency. Experimental results show strong performance with, NPCR above 99.4%, and UACI ranging from 44% to 60%. Correlation coefficients drop from 0.93 to nearly 0.01, showing high resistance to statistical attacks. The system is highly effective for secure image transmission and storage applications.

FUTURE SCOPE

The suggested algorithm's effectiveness is demonstrated by the test results for different settings; nonetheless, the encrypted image's obtained entropy value of 7.62 falls short of the intended threshold of eight. Enhancing the Entropy threshold will allow this work to be expanded. For future enhancement, integrating parallel processing or GPU acceleration is suggested to enable real-time performance, making the system more suitable for practical and large-scale multimedia security applications.

REFERENCES

[1]. Sajjad Shaukat jamal, Zaid Bassfar, Ouafae Lahlou, Amer Aliaedi and Mohammad Mazyad Hazzazi, “Image Encryption based on Elliptic Curve point and Linear Fractional Transformation”, IEE access, vol. 12, 2024, doi:01.

[2]. H.U.Rehman, M.M.Hazzazi, T.Shah, A.Aljaedi, and Z.Bassfar, ‘‘Color image encryption by piecewise function and elliptic curve over the Galois field GF(2n),’’ AIMS Math., vol. 9, no. 3, pp. 5722–5745,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25aug864

2024,doi:02.
[3]. 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, Jul. 2023, doi:03.
[4]. RadhaKrishna M, Sridevi KS, Sowmya BS, Susmita TJ, “Digital Image Encryption and Decryption based on RSA Algorithm”, Int. J. Sci. Res. Sci. Eng. Technol., vol. 9, no. 4, pp. 168–173, Jul.–Aug. 2022, doi:04.
[5]. Y. Xian and X. Wang, ‘‘Fractal sorting matrix and its application on chaotic image encryption,’’ Inf. Sci., vol. 547, pp. 1154–1169, Feb. 2021, doi:05.
[6]. Ibrahim and A. M. Abbas, ‘‘Efficient key-dependent dynamic S-boxes based on permutated elliptic curves,’’ Inf. Sci., vol. 558,pp. 246–264, May 2021, doi:06.
[7]. A. A. El-Latif, B.Abd-El-Atty, M.Amin, and A.M.Iliyasu, ‘‘Quantum inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications,’’ Sci. Rep., vol. 10, no. 1, pp. 1–16,Feb. 2020, doi:07.
[8]. M. I. Haider, A. Ali, D. Shah, and T. Shah, ‘‘Block Cipher’s nonlinear component design by elliptic curves, An image encryption application,’’ Multimedia Tools Appl., vol. 1, pp. 1–26, Jan. 2020, doi:08.
[9]. A. H. Zahid, E. Al-Solami, and M. Ahmad, ‘‘A novel modular approach based substitution-box design for image encryption,’’ IEEE Access, vol. 8, pp. 150326–150340, 2020,doi:09.
[10]. Q. Lu, C. Zhu, and X. Deng, ‘‘An efficient image encryption scheme based on the LSS chaotic map and single S-box,’’ IEEE Access, vol. 8, pp. 25664–25678, 2020, doi:10.
[11]. Y. Lu, K. Yu, and X. Lv, ‘‘Image encryption with one-time password mechanism and pseudo-features,’’ Multimedia Tools Appl., vol. 80, no. 10, pp. 15041–15055, Apr. 2021,doi:11.
[12]. A. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, ‘‘Image encryption process based on chaotic synchronization phenomena,’’ Signal Process., vol. 93, no. 5, pp. 1328–1340, May2013, doi:12.
[13]. Q. Liu and L. Liu, ‘‘Color image encryption algorithm based on DNA coding and double chaos system,’’ IEEE Access, vol. 8, pp. 83596–83610, 2020, doi:13.
[14]. Wang and Y. Li, ‘‘Chaotic image encryption algorithm based on hybrid multi- objective particle swarm optimization and DNA sequence,’’ Opt. Lasers Eng., vol. 137, Feb. 2021, Art. no. 106393, doi:14.
[15]. Z. E. Dawahdeh, S. N. Yaakob, and R.B. Othman, ‘‘A new image encryption technique combining elliptic curve cryptosystem with Hill cipher,’’ J. King Saud Univ. Comput. Inf. Sci., vol. 30, no. 3, pp. 349–355, Jul. 2018, doi:15.
[16]. 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, Dec. 2017, doi:16.
[17]. 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, Dec. 2017, doi:17.
[18]. Amnah Firdous, Aqeel Ur Rehman, and Malik Muhammad Saad Missen, “A Gray Image encryption using of water waves, chaos and hash Function”, IEEE Access, vol. 9, pp. 11675– 11693, Jan. 2021, doi: 18.
[19]. D. S. Laiphrakpam, R. Thingbaijam, K.M. Singh, and M. Alawida, “Encrypting multiple images with an enhanced chaotic map,” IEEE Access, vol. 10, pp. 87844–87859, Aug. 2022,doi: 19.
[20]. Wei, L. Guo, Q. Zhang, J. Zhang, and R Lian, ‘‘A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system,’’ J. Syst. Softw., vol. 85, no. 2, pp. 290–299, Feb. 2012, doi:20.
[21]. M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi, and A. R. Alharbi, ‘‘Construction of S- boxes using different maps over elliptic curves for image encryption,’’ IEEE Access, vol. 9, pp. 157106–157123, 2021, doi:21.