WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Secure Transmission of Digital Images using Multiple Chaotic Maps and Elliptic Curve

Javaria Akbar[1], Nasir Siddiqui[1], Shamsa Kanwal[2], Saba Inam[2]

[1]Department of Mathematical Sciences, University of Engineering and Technology Taxila, Pakistan
[2]Department of Mathematical Sciences, Fatima Jinnah Women University, The Mall, Rawalpindi
***Email:** shamsa.kanwal@fjwu.edu.pk*
Doi https://doi.org/10.55248/gengpi.5.0624.1412

A B S T R A C T

The use of the internet for visual communication has risen during the previous decade. Content protection is seen as a critical concern in today's environment. As a result, encrypting such contents is a difficult challenge for researchers. They are focusing on protecting important data such as images, videos, and audio from various eavesdropping attempts. Many encryption algorithms have been created and developed specifically for this purpose. New encryption systems based on chaos theory provide safe and speedy communication. This research proposes an effective image encryption scheme using chaotic maps and an elliptic curve theory in the Hill cipher that meets the basic requirements of a safe image encryption algorithm. Chaotic maps serve a vital part in the encryption procedure. The suggested cryptosystem is resistant to numerous assaults, including brute force, differential, and statistical. Instead of eye examination, the suggested approach is evaluated using a variety of tests, including the correlation coefficient, information entropy and uniformity. The simulation results of the provided scheme is compared to the advanced image encryption algorithms. Based on statistical study, we believe our encryption algorithm is safe.

Keywords: Chaotic map, Hill cipher, Elliptic curve, Chebyshev map, Entropy, Correlation.

1. Introduction

Due to massive advancements in network technology have enabled individuals to digitally communicate information across networks. The protection of this digital information is critical, including confidentiality and integrity [7]. Cryptography serves as a practical method for securing private and sensitive information. The progress of network technology has led to a rise in demand for data exchange over the internet. The efficiency of most cryptographic systems relies on generating lengthy and random key sequences and these sequences need to possess sufficient size and randomness. Images now plays a very significant role in various fields, from medicine to social media. With such widespread use and the necessity for digital images, security has become a pressing concern. As a result, there is a significant desire for a strong image cryptosystem to enable secure communication over insecure networks.

In past few years, numerous improvements have been made in encryption of different images. Proposed techniques in previous literature treated images as binary bits stream, similar to textual data, and then encrypted them by using well recognized algorithms like AES, TDES and RSA [1, 2]. However, these approaches were not demonstrated to be effective for handling image files [3, 4]. The challenge lies in the vast quantity of image data, which contrasts sharply with text information. Unlike text data, where adjacent cells have limited correlation as compared to data of image which exhibits a strong correlation among adjacent pixels. In comparison, DNA operation [5], and chaos theory [6] are better for encrypting images.

To ensure the security of the image, the most popular technique is the chaotic scheme of image encryption. This method utilizes the chaos inherent properties, such as initial values sensitivity to seed value and irregular behavior name as non-linearity [7-9]. The method comprises on chaos, incorporating features such as pseudo-randomness, ergodicity, and sensitivity to beginning circumstances, which provide security. For instance, in [10], Chai et al. used the preprocessing-permutation-diffusion structure to implement a safe cipher image technique. In this cryptosystem, the key stream for the system is generated by using memristive system which is hyperchaotic. For example, in [11] author designed a method for gray scale images using dynamical chaotic system which was established by two different chaotic maps, Logistic map and sine map name as 2D Logistic-Sine-coupling map. Setiadi et al. in [12] presents a novel image encryption system that combines 2D series with logistic map and permutation replacement functions and this aimed at enhancing both the security and effectiveness of encryption processes. This technique provides a reasonable diffusion degree. In [13] Zhang with his team generated keys using a chaotic system and random sequences using an S-Box. For the enhancement of the chaotic scheme complexity in [14] Li et al. uses a fractional order technique to introduced a novel cryptosystem based on optical system featuring a laser hyperchaotic. An efficient encoding algorithm is proposed by Kanwal et al. in [15] employed different chaotic functions with orthogonal matrices.

The concept of Elliptic curve-based cryptography (ECC) was proposed by Miller [16] and Koblitz [17], which enhanced the efficacy of several other cryptographic techniques. ECC employs a smaller key size in comparison with other techniques while maintaining the same level of security, making it

computationally quicker and reduced processing resource usage. The discrete logarithm problem (DLP) on elliptic curves is the foundation of ECC's security. For a correctly chosen curve which is elliptic, here is no sub-exponential technique for solving this logarithmic problem. Numerous image encryption techniques have been proposed which are based on ECC.

A novel encryption technique is suggested by author in [18], for the medical imaging data employed elliptic curve cryptography (ECC) and an improved ElGamal scheme. Instead of encoding the message into an elliptic curve point as typically done in ECC, this scheme directly utilizes pixel values represented as elliptic curve coordinates. By encrypting pixel blocks directly, this approach proves to be more efficient. Additionally, [19] presents a color image encryption system where ECC is utilized for key and parameter generation, while a discrete chaotic map is employed to scramble the image. Patro et al. [20] suggested a new method for color image encoding promoting non-overlapping block-level diffusion operations.

The concept and functions used in past literature influence the current work. This study aims to propose a novel picture encryption technology for strong security that combines chaotic maps with the Hill cipher. The suggested approach uses chaotic maps for permutation, Elliptic curves for substitution, and bit-wise XOR for diffusion. Higher security levels create the Hill cipher key using the Self-invertible matrix derived from the elliptic curve. Security measures such as entropy, histogram analysis, correlation factors were utilized to evaluate the efficacy of the suggested approach. Chaotic techniques are the main focus of the most of the researchers because of some distinctive qualities include sensitive beginning circumstances, pseudo-randomness, and control parameters.

The remaining sections of the paper is arranged as follows. Theoretical background of propose scheme is investigated by Section 2. Section 3, discusses a suggested hybrid picture encryption approach. In Section 4, some of the analysis results from the suggested scheme with chaotic maps and assess the algorithm robustness against different attacks. Conclusion follows by Section 5.

2. Mathematical Background

This section introduces the mathematical concepts of the suggested image encryption scheme. Dynamic mathematical functions characterized by continuous feedback loops are chaotic maps. These maps are extremely dynamic and highly responded to control parameters and initial states. The resultant value of the map significantly modified by a slight alteration in seed values or controlling elements. Consequently, chaotic maps are employed to produce random sequences. Figure 1. depicts the standard design for chaos-based image cryptosystems.

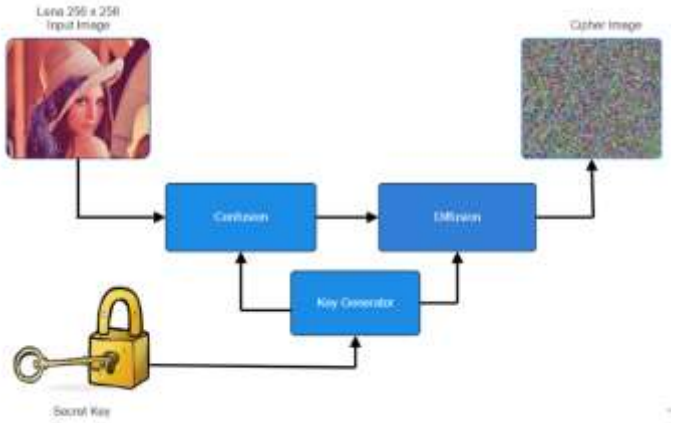


Fig 1. Structure of Chaotic Image Encryption Model

2.1 Altered Sine-Logistic based Tent Map (ASLT)

By integrating features of the sine map, logistic map, and tent map author in [21] suggested a novel compound one-dimensional piece wise chaotic system which is hybrid in nature to overcome the issues inherent in theses maps. The proposed map provides more chaotic characteristics than either map alone. The equation for this combination is presented below.

$$u_{n+1} = \begin{cases} \left(\frac{4-h}{4}\right)\sin(\pi u_n) + \frac{h}{2}u_n, & if\ u_n < 0.5 \\ (4-h)u_n(1-u_n) + \frac{h}{2}(1-u_n), & if\ u_n \geq 0.5 \end{cases}$$

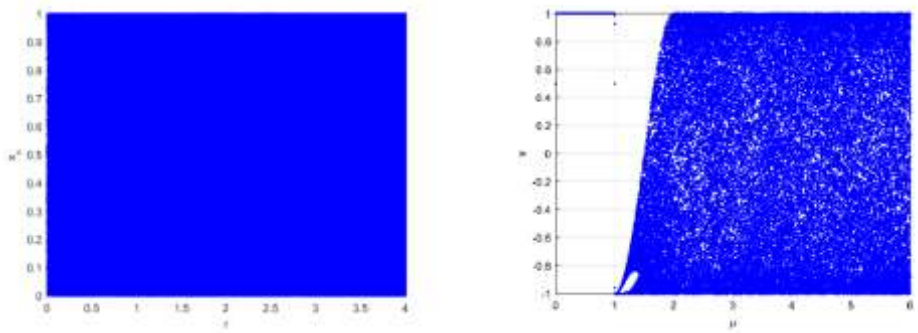
When h ∈ [0, 4], a controlling variable lies in given interval. Fig 2 (a), displays the bifurcation diagram for the ASLT chaotic system. This map possesses a notably broader chaotic interval in comparison with other maps such as Logistic, Sine, and Tent maps. ASLT map yields a uniformly distributed sequences within [0, 1]. Therefore, the ASLT map performs very effectively in chaotic scenarios.

2.2 Chebyshev map

In [22-24] different authors explore one-dimensional map which is chaotic in nature, name as Chebyshev map and described by the following equation:

$$u_{n+1} = cos(\mu\, cos^{-1}(u_n))$$

where the controlling variable μ belongs to N. The Chebyshev map exhibits chaotic behavior, characterized by sensitivity to initial conditions and aperiodicity. It has a extensive use in chaos theory, chaotic based cryptography, and other scientific domains due to its unpredictability and randomness. Figure 3, displays the graphical representation of map term as bifurcation diagram. Controlling parameter μ > 1, chaotic behavior occurs, with output chaotic sequences ranging from [-1, 1]. Although chaotic, the distribution of output sequence is non-uniform in the range of μ in between 1 and 2.



a **b**

Fig 2. (a) Display the Bifurcation diagram of ASLT Map (b) Display the Bifurcation diagram of Chebyshev Map

2.3 Elliptic Curve Cryptography Concept

Public-key cryptography stands out as a modern system based on elliptic curve technique appreciated for its efficiency. It is based on curves which are elliptic, introduced by an equation of the form:

$$y^2 \equiv x^3 + ax + b$$

where constants are represented by a and b. ECC provides notable advantages as compared to other techniques like RSA. It achieves equivalent security levels with much smaller key sizes. It plays an important in those environments where the processing and storage ability are constrained, that's why it particularly good for environments which are constrained by different resources such as IOT and mobile devices. To ensure secure communication over insecure networks and encryption ECC utilizes the elliptic curve mathematical properties. In ECC, encryption keys are derived from points on an elliptic curve over a finite field. Elliptic Curve Discrete Logarithm Problem (ECDLP) solving complexity decides the security of ECC, which entails finding a point X_1 given another point X_2 and a scalar m, we can write it as $X_1 = mX_2$. ECC Security depends on the task of solving the discrete logarithmic problem, which is not feasible computationally for the elliptic curves which are enough large. Because of security point of view ECC are highly recommended in terms of digital signature, data security over insecure channels and in process of key exchange. ECC is highly efficient in terms of computational power. The operations which are used by elliptic curve cryptography are:

- **Point Addition:** Mathematically, $x1 + x2 = X$ defines the addition of two points on elliptic curve.
- **Point Subtraction:** On elliptic curve subtraction between two points is calculated by: $x1 - x2 = X$
- **Point Multiplication:** Mathematically, it is calculated by: $x + x + x + x + x + \ldots = nx = X$
- **Point Doubling:** Point doubling operation define as: $x + x = X$

2.3.1 Elliptic Curve Diffie-Hellman Key exchange

The Elliptic Curve Diffie-Hellman (ECDH) key exchange utilizes elliptic curve cryptography (ECC) for secure key exchange in comparison with classic Diffie-Hellman key exchange protocol. ECDH is a modified version of the classic Diffie-Hellman key exchange technique. In ECDH, two parties, typically referred to as user A and B, can agree upon a shared secret key over an insecure communication channel without exchanging any secret information. To exchange keys, follow these steps:

- **Step 1:** A and B are the users produce the secret keys K_A and K_B. After that, both the users utilize generator point G on the curve, and compute the public key using:

$A_{pub} = K_A \cdot G_p$

$B_{pub} = K_B \cdot G_p$

- **Step 2:** Users A and B apply these two equations to compute the shared ECDH key.

$AB_{share} = K_A \cdot B_{pub}$

$AB_{share} = K_B \cdot A_{pub}$

3. The Proposed Scheme

In this study, encryption of RGB images is achieved by integrating Hill cipher with a chaotic system. RGB image comprises of three different codes name as: red, green, blue. Each colored matrix has pixels with 8 bits, resulting in a range of 256 values. Consequently, all operations are performed modulo 256. The complete image encryption scheme unfolds in three distinct phases. Initially, ASLT map is introduced to obtain a sequence for rearranging the image's pixels. Subsequently, in the second stage, these rearranged pixels with an invertible matrix generated from Elliptic Curve Diffie-Hellman Key exchange method undergo multiplication. Finally, in the last phase a sequence, originating from a freshly initiated chaotic Chebyshev map, is XORed with the previously obtained outcomes. This intricate scheme's complexity serves as a robust defense against potential attacks from unauthorized persons. The following sections will outline the encoding and decoding procedures of the proposed methodology. Figure 4. depicts a suggested algorithm's flowchart. The following steps included in the suggested scheme are:

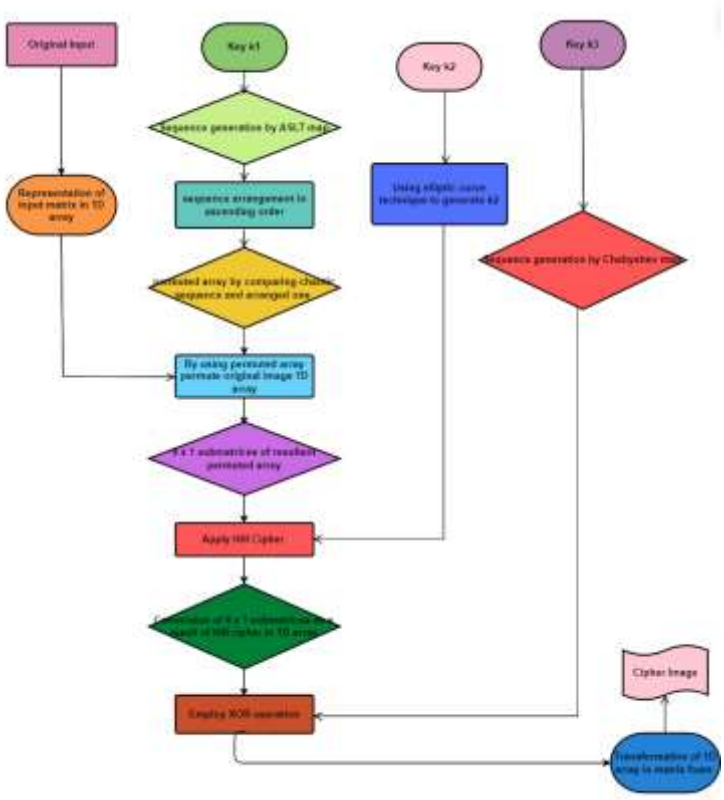


Fig 3. Flow chart of the Proposed Scheme

3.1 Encryption Scheme

Selection criteria for the image is to select a digital photo with dimensions $R \times C \times 3$, where rows and columns are denoted by R and C respectively. The dimensions of the encode picture will match those of the original image. This subsection introduces the three different phases of our proposed encryption scheme.

Algorithm 1: Image Encryption Scheme

Input: Digital image DI, Hidden keys k_1, k_2, k_3, ASLT Map, Chebyshev Map

Output: Encoded image C of same size as an original image size is D

1. The test image DI, with rows and columns are expressed by R and C of image respectively, is converted into a 1D array.
2. By utilizing chaotic ASLT map with key k_1 to produce the random sequence, then structure the obtained result in an increasing arrangement and after comparing the chaotic sequence with arranged one we obtained the permutation array. By using the transformed sequence permute the original matrix 1D array.
3. Calculate the matrix of order 2 x 2 name as M_{11} by using ECDHKE and then find M_{12}, M_{21}, M_{22} to obtain a self-invertible matrix M of order 4 x 4 and I is an identity matrix of order 2 x 2. Here b is any integer should be coprime with gcd $(b, 256)$=1.
$$M_{12} = (b(I - M_{11}),\ 256),$$
$$M_{21} = (b^{-1}\ (I - M_{11}),\ 256),$$
$$M_{22} = ((\ M_{11}), 256)$$
4. Permuted array obtained in step 2 transmute into block size of 4 x 1.
5. All the submatrices produced in step 4 are employed with k_2, which generates the M self-invertible matrix in above step to implement the Hill cipher using:
$$New_{Submatrices} = (M * \{Submatrices\})\ (mod\ 256)$$
then convert the new submatrices in previous step in array of 1D name as S.
6. By using Chebyshev map with secret key k_3, build a real number sequence and by using formula convert the result into an integer number.
$$Integer_{sequence} = floor(mod(Real_{sequence} * 10^{14}), 256)$$
7. Apply bitwise XOR on each element of S, integer sequence component, and ciphered elements obtained in previous iteration and transform the result array in matrix to obtain the encoded image C.
$$Result_i = Integer_{sequence}(i) \oplus (S_i \oplus Result_{i-1}] \qquad i = \{1,2,3 \dots \dots . . D\}$$

Algorithm 1. Image Encryption Scheme Pseudocode

3.1.1 Shuffling Procedure

In our proposed cryptosystem, the permutation stage rearranges the pixels of an input image. Firstly, ASLT map is employed with key k_1, utilized to construct a sequence which is then sorted in increasing pattern. Chaotic sequence produced by the ASLT map is employed to shuffle the pixel units of input picture. As a result, we get the permuted sequence a one-dimensional array that depicts the original image.

3.1.2 Substitution Procedure

It explores the second step, that is the substitution stage. This step, generates the secret key represented by k_2 by utilizing Elliptic curve Diffie Hellman key exchange technique (ECDH) and this key is used for Hill cipher. The Hill cipher, is renowned in encryption for its effectiveness and simplicity [25]. Because of its polygraphic nature it offers resilience against traditional frequency analysis attacks [26]. The permuted 1D array is separated into $\frac{M}{4}$ sub-blocks. The produced 4 × 4 self-invertible matrix to allow decryption multiplies the $\frac{M}{4}$ sub-blocks one by one. The results are placed in a one-dimensional array S.

3.1.3 Diffusion Procedure

The concluding stage provides the dispersion of pixels. Utilizing key k_3, the last phase produce with the sequence using Chebyshev map. An integer sequence is introduced by transmuting the Chebyshev map generated sequence using the formula:

$$Integer_{sequence} = floor(mod(Real_{sequence} * 10^{14}), 256)$$

The integer sequence and the 1D array are bitwise XORed in accordance. By rearranging the 1D array we get a matrix of order $R \times C \times 3$.

3.2 Decryption Scheme

The goal of picture decryption is to execute the encoding technique in reverse order in order to recover the original image pixels. technique 2 describes the three stages of the proposed decryption technique. Firstly, when an algorithm is run, the generated sequence by Chebyshev map employed with k_3 to generate unpredictable sequence and then, that sequence is converted in integer sequence and after that using bitXOR operation. The invertible matrix is subjected to the Hill cipher using k_2. After applying k1 to the random sequence produced by the ASLT map, we were able to acquire an inverse permutation. To reverse the permutation, apply the inverse permutation. We get the original input, after converting the resulting one-dimensional array into a picture format.

Algorithm 1: Image Decryption Scheme
Input: Cipher image CI, Hidden keys k_1, k_2, k_3, ASLT Map, Chebyshev Map
Output: Original input image DI

1. The image CI, which is in matrix form is transmuted into a 1D array.
2. With secret key k_3, Chebyshev map produce a sequence and then, converted it into an integer number.

$$Integer_{sequence} = floor(mod(Real_{sequence} * 10^{14}), 256)$$

3. Each value of CI passing through the bitXOR operation, with the converted integer sequence value and the value which iterated previously.

$$D_i = Integer_{sequence}(i) \oplus (CI_i \oplus D_{i-1}] \qquad i = \{1,2,3 \dots \dots . . N\}$$

4. Firstly, convert the obtained array D in 4 x 1 submatrices and then utilize the generated self-invertible matrix MI as explained in encryption scheme by secrete key k_2 employed with in Hill cipher by reversing the formula

$$New_{Submatrices} = (MI * \{Submatrices\}) \ (mod\ 256)$$

then convert the new submatrices obtained in previous step in array of 1D name as SI.

5. Using iteration technique on ASLT map with secret key k_1, to build a sequence B and then obtained the sequence array B' , which arranged in increasing pattern.
6. By introducing the inverse transformation array we compute the permuted array as P'.

Algorithm 2. Image Decryption Scheme Pseudocode

4. Experimental findings and Security assessment

To ensure the security of suggested encryption scheme different experimental and security tests have been performed. This section includes the results of various testing. For the security analysis, we take several standard images from online site USC-SIPI picture database [27] to assess a suggested image encryption scheme. We are utilizing a 256 x 256 colored Lena image for analysis. The effectiveness and robustness of the developed cryptosystem were evaluated using a variety of attacks, Shannon's entropy of the cipher pictures, histogram analysis, and correlation analysis.

4.1 Information Entropy Evaluation

The idea of Shannon's entropy was initially established by Shannon [28]. In different encryption methods, for the computation of randomness in cipher image, it is an important quantity. We make the assumption that the picture encryption technique handles each of the 2^8 symbols equally likely. In this situation, $H_{max} = 8$ is the ideal entropy value. To ensure the security of the different image encryption algorithms the value of entropy needs to approach the optimal level. Robustness of an algorithm is determined by the entropy level, comprises of the statistical assessment and the unpredictability of all data origin. A technique is deemed secure against entropy attacks when its entropy value closely aligns with the ideal value. Entropy of an encrypted image displayed by Table 1.

Table 1: Comparison of Information Entropy values of Encoded image

Encryption Schemes	**Proposed Scheme**	**Reference [15]**	**Reference [29]**
Entropy Value	7.9992	7.9991	7.9990

4.2 Histogram Evaluation

Each pixel frequency level is illustrated by the histogram of an image. Pixel units with homogeneous frequency level exhibits a well-encrypted picture. Figure 4. illustrates the frequency distribution analysis of an encode image in three different channels. We can see that the cipher image histogram is uniformly dispersed, indicating the no information is leaked.

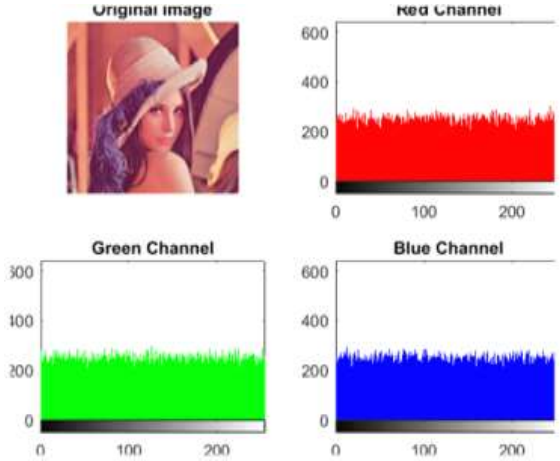


Fig 4. Colored Lena (256 x 256) encrypted image histogram analysis

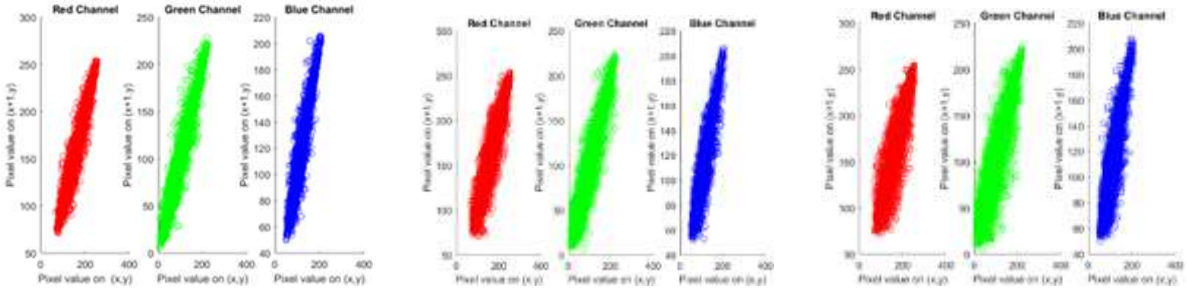
4.3 Correlation Evaluation

The images we encounter every day have pixel values that are highly correlated with their neighboring pixels. To ensure the significant level of confusion and diffusion in the proposed scheme we examining the adjacent pixel correlation test in input picture and their associated encoded result. To prevent statistical attacks, a well- encrypted cipher image has a low correlation with neighboring pixel values. Table 2. The correlation adjacent pixels coefficients for planar and cipher images are depicted by Table 2.

Table 2: Correlation values between original and encrypted Lena.

Directions	**Original Lena**			**Encrypted Lena**		
	Red	**Green**	**Blue**	**Red**	**Green**	**Blue**
Row	0.9910	0.9890	0.9846	0.0040	-0.00053	0.0040
Column	0.9781	0.9742	0.9710	0.0014	0.0021	-0.0026
Diagonal	0.9648	0.9613	0.9563	0.0016	-0.0053	0.0083

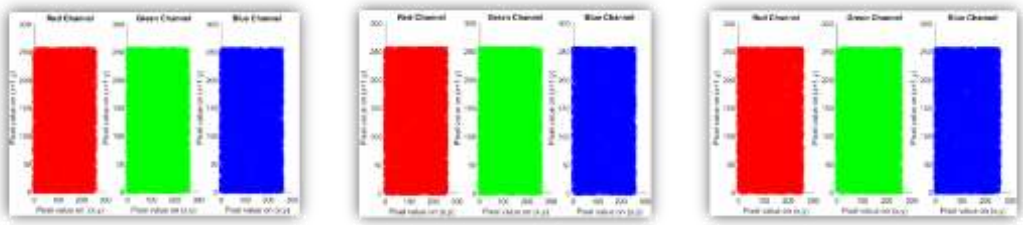
We mapped the neighboring pixel values in three different directions horizontally, vertically, and diagonally by selecting random input test image pixels units demonstrated by Fig 5.



a **b** **c**

Fig 5: Representation of pixels correlation of original image (a) Row wise (b) Column wise (c) Diagonally

pixel plots in test image are not evenly distributed, whereas pixel plots in cipher image are evenly distributed depicted by Fig 6, indicating the needed confusion and diffusion quality.



a **b** **c**

Fig 6: Representation of pixels correlation of encoded image (a) Row wise (b) Column wise (c) Diagonally

5. Conclusion

In the proposed research, we introduced a highly effective encoding scheme of digital photos which is hybrid in nature, based on chaotic maps and elliptic curve. These maps offer advantages such as ergodicity and the ability to calculate entropy. In this system, trigonometric and piecewise chaotic maps were investigated for their potential as secure, fast, and dependable encryption methods. The suggested cryptosystem provides good security, as evidenced by theoretical and experimental studies. The findings verified our proposed cryptosystem. Our encryption method is suitable for encrypting images and securely transmitting confidential information over the internet, as evidenced by positive research.

References

1. Daemen J, Rijmen V, AES Proposal, Rijndael. (2001). National institute of standards and technology, FIPS-197.
2. Rivest RL, Shamir A, Adleman L. (1977). A method for obtaining digital signatures and public key cryptosystems. Association for computing machinery, 1977.
3. Khan, J. S., Ahmad, J., Ahmed, S. S., Siddiqa, H. A., Abbasi, S. F., and Kayhan, S. K. (2019). DNA key based visual chaotic image encryption. Journal of Intelligent and Fuzzy Systems, 37(2), 2549-2561.
4. Mondal B, Kumar P, Singh S. (2018). A Chaotic Permutation and Diffusion Based Image Encryption Algorithm for Secure Communications. Multimedia Tools Applications, 77(23), 31177–31198.
5. Wang X, Su Y, Liu L, Zhang H, Di S. (2021). Color Image Encryption Algorithm Based on Fisher-Yates Scrambling and DNA Subsequence Operation. The Visual Computer, 1-16.
6. Wu, X., Wang, K., Wang, X., Kan, H., and Kurths, J. (2018). Color image DNA encryption using NCA map-based CML and one-time keys. Signal Processing, 148, 272- 287.
7. Ljupco Kocarev and S. Lian. (2016). Chaos-based Cryptography. Heidelberg: Springer Berlin.
8. Wang, Y. Li, and J. Jin. (2020). A new one-dimensional chaotic system with applications in image encryption. Chaos Solitons Fractals, 139, 110102.
9. H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman. (2018). A new hyperchaotic map and its application for image encryption. The European Physical Journal, 133, 1–14.
10. Chai, X., Fu, J., Zhang, J., Han, D., and Gan, Z. (2021). Exploiting preprocessing permutation–diffusion strategy for secure image cipher based on 3D Latin cube and memristive hyperchaotic system. Neural Computing and Applications, 33, 10371-10402.
11. Hua, Z., Jin, F., Xu, B., and Huang, H. (2018). 2D Logistic-Sine-coupling map for image encryption, Signal Processing, 149, 148-161.
12. Setiadi, D. R. I. M., and Rijati, N. (2023). An image encryption scheme combining 2D cascaded logistic map and permutation-substitution operations. Computation, 11(9), 178.
13. Zhang, L., Ma, C., Zhao, Y., and Zhao, W. (2023). A Novel Dynamic S-Box Generation Scheme Based on Quantum Random Walks Controlled by a Hyper-Chaotic Map. Mathematics, 12(1), 84.
14. Li, X., Mou, J., Cao, Y., and Banerjee, S. (2022). An optical image encryption algorithm based on a fractional-order laser hyperchaotic system. International Journal of Bifurcation and Chaos, 32(03), 2250035.
15. Kanwal, S., Inam, S., Othman, M. T. B., Waqar, A., Ibrahim, M., Nawaz, F., ... and Hamam, H. (2022). An effective color image encryption based on Henon map, tent chaotic map, and orthogonal matrices. Sensors, 22(12), 4359.
16. Miller, V. S. (1997). Elliptic Curves and their use in Cryptography. DIMACS Workshop on Unusual Applications of Number Theory, 21.
17. Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.

18. Laiphrakpam, D. S., Khumanthem, M. S. (2017). Medical image encryption based on improved ElGamal encryption technique. Optik, 147, 88-102.

19. Shankar, K., and Eswaran, P. (2016), An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. Artificial Intelligence and Evolutionary Computations in Engineering Systems: Proceedings of ICAIECES 2015, 705-714.

20. Patro, K.A.K., Acharya, B. Nath, V. (2020). Various dimensional color image encryption based on non-overlapping block-level diffusion operation, Microsystem. Technology, 26, 1437–1448.

21. Aouissaoui, I., Bakir, T., Sakly, A., and Femmam, S. (2022). Improved One-Dimensional Piecewise Chaotic Maps for Information Security. J. Commun., 17(1), 11-16.

22. Chatterjee, S., Roy, S., Das, A. K., Chattopadhyay, S., Kumar, N., and Vasilakos, A. V. (2016). Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment. IEEE Transactions on Dependable and Secure Computing, 15(5), 824-839.

23. Xiao, D., Liao, X., and Deng, S. (2007). A novel key agreement protocol based on chaotic maps. Information Sciences. 177(4), 1136-1142.

24. Hsu, C. L., and Lin, T. W. (2013). Password authenticated key exchange protocol for multiserver mobile networks based on Chebyshev chaotic map. IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 90-95.

25. L. S. Hill. (1929). Cryptography in an algebraic alphabet. The American Mathematical Monthly, 36(6), 306–312.

26. L. S. Hill. (1931). Concerning certain linear transformation apparatus of cryptography. The American Mathematical Monthly, 38(3) , 135–154.

27. USC Signal and Image Processing Institute (SIPI) Image Database. Accessed: Feb. 20, 2021. [Online]. Available: http://sipi.usc.edu/database/.

28. C. E. Shannon. (1949). Communication theory of secrecy systems. Bell Syst. Tech. J., 28(4), 656–715.

29. Kanwal, S.; Inam, S.; Cheikhrouhou, O.; Mahnoor, K.; Zaguia, A.; Hamam, H. (2021). Analytic study of a novel color Image Encryption Method Based on the chaos System and color codes. Complexity 2021, 549953