IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 42, No. 6, December, 2025, pp. 3115-3123
Journal homepage: http://iieta.org/journals/ts

A Secure Image Cryptosystem for Satellite Imaging Using Henon Map, Legendre Function, and Circulant Matrices

Fahima Hajjej[1], Shamsa Kanwal[2*], Saba Inam[2], Ala Saleh Alluhaidan[1]

[1] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[2] Department of Mathematical Sciences, Fatima Jinnah Women University, Rawalpindi 46000, Pakistan

Corresponding Author Email: shamsa.kanwal@fjwu.edu.pk

https://doi.org/10.18280/ts.420607

Received: 16 October 2025
Revised: 12 November 2025
Accepted: 29 November 2025
Available online: 31 December 2025

Keywords:
image encryption, Henon map, Legendre function, multilayer diffusion

ABSTRACT

A multitude of information may be found in images, which are also essential for the visual representation, interpretation, and expression of data. However, researchers worldwide face major obstacles due to the difficulties of storing and retrieving images. A robust image encryption method tailored for colored images is presented in this study. To achieve high security levels, it makes use of multilayer Circulant matrices, Legendre functions, and the Henon map. The Henon map is used as the very first step in our encryption scheme that adds depth and randomness by shuffling the pixel value. Then, for substitution, a mathematical transformation is introduced to further secure the image content by applying the Legendre function. Lastly, the Circulant matrices are employed for multilayer diffusion, which efficiently mixes pixel values and offers robustness against cyber-attacks. The conventional image encryption techniques depend on a single algorithm, which leaves them vulnerable to numerous security risks. Our novel design combines three algorithms: mathematical replacement, chaotic map, and multilayer diffusion that increase cryptographic security. Experimentally, the low correlation between pixels, high entropy, and successful resistance to different attacks demonstrate the strength of the proposed approach. A comparison with the current technique demonstrates the advantages in the field of digital image encryption.

1. INTRODUCTION

Development in digital technology has transformed the way we assess and distribute information, making it easier to manage large amounts of data. But this development has caused a huge risk of security threats to the private data, especially image threats, including unauthorized alteration, interception, and illegal access. As images are being extensively used in industries including social networking, satellite images, health care, and defense, they are susceptible to cyberattacks. In cryptography, the major difficulty these days is maintaining the confidentiality, integrity, and authenticity of image-based data. Due to the distinct features and massive data size of images, it is difficult to manage image encryption using conventional encryption techniques, as it differs greatly from text encryption [1].

DES (Data Encryption Standard) [2], AES (Advanced Encryption Standard) [3], and RSA [4] were the first developed traditional encryption techniques for text and numerical data. These methods fail for images due to certain features of image data, such as high pixel correlation, big data volumes, and significant redundancy, but these methods work very efficiently for structured datasets. To deal with such complex image layouts, specific image encryption techniques have been developed to maintain confidentiality.

Chaos systems play a vital role in various areas of mathematics and are used for evaluating an extensive variety of complex structures because of their interesting characteristics, like being sensitive to initial conditions, which means that minor alterations in the input may result in a variety of different output series [5]. While dealing with image encryption, the chaotic map effectively works and reduces the association between the pixels, which helps to enhance the image's resistance to statistical attacks. Moreover, combining a chaotic map for scrambling with a mathematical transformation for substitution and a diffusion mechanism would significantly enhance the security and complexity of the enciphering technique.

The proposed encryption technique for colored images integrates three effective techniques: chaotic scrambling, mathematical substitution, and multilayer diffusion, which provides an innovative encryption framework. The Henon map is a widely recognized 2D chaotic map that disturbs the pixel's position while making it unpredictable, and it undermines the image's structural coherence, scrambling the image in such a way that the encrypted image appears entirely different from the original one. For further distorting the image pixels, we will use the Legendre function for substitution by transforming the pixel values into complicated geometric patterns. Finally, for multilayer diffusion, we will use circulant Matrices, which will provide an extra layer of protection against the various security attacks by diffusing the pixels in

the image.

The proposed encryption technique has two primary objectives: achieving precise reconstruction and ensuring high security. As the proposed scheme uses a combination of chaos map, mathematical transformation, and multilayer diffusion helps to get high security against brute-force, statistical, and differential attacks. The decoded image is guaranteed to match exactly to the actual image while keeping its visual appeal and statistical properties without losing any data.

The proposed method has been extensively tested on several image types, including satellite high-resolution colored images. Key sensitivity, encryption speed, and attack resistance are the performance indicators that demonstrate the method's dependability and effectiveness.

The organization of this manuscript is explained as follows: By furnishing a complete summary of the underlying concepts and pertinent research, Section II creates the context for the proposed approach. The encryption approach, multilayer circulant matrices for diffusion, Legendre function for substitution, and the use of Henon map for pixel scrambling, are all covered in Section III. The experimental and assessment aspects the discussed in Section IV, including computing efficiency, security analysis, and resilience to various threats. Additionally, a comparison with previous approaches is provided. The research's major findings are emphasized in Section V, which also acknowledges its significant contributions and suggests potential directions for future study.

2. LITERATURE REVIEW

In today's data-driven world, where strict observance of digital image security and preservation is a concern, the need to provide satellite imagery with equivalent levels of protection becomes obvious. The increasing hazards arising from illegitimate use and access to satellite imagery highlight how important information security is to safeguard a nation's crucial infrastructure [6]. Cyber-attacks have significantly increased due to the cloud invasion, which has increased by 75% in the past year, as reported by Crown Strike Global Threat in 2024 [7]. Among the numerous technologies that produce several photos daily are Satellite images, medical images; these photos are shared for analytical, scientific, and diagnostic purposes [8].

Chaotic systems are one of the best techniques for leaving beyond these restrictions. Chaos-based image encryption is different from the traditional image encryption method that uses a mathematical equation; chaos-based encryption takes into account the inherent uncertainty and randomness of chaotic systems, which provides a key with dual encryption and decryption capabilities [9]. The basic components of cryptographic techniques that are renowned for their efficiency and variation are confusion and diffusion, as proposed by Shannon [10]. To address security threats, several encryption schemes have been developed over the past few years, integrating the use of chaotic systems and mathematical transformations. The authors [11] introduced an innovative image encryption technique; this technique comprises a sine map, a chaotic tent map, and circulate matrices.

Yadav et al. presented an article in 2024, studying the use of the Arnold transform and Bessel function for image encryption in a blockchain context. This encryption scheme addressed security issues in image data transactions and shows that the use of a chaotic map and mathematical equation together on a blockchain can greatly improve the security and reduce the chances of cyber-attacks, especially for image-based data. To scramble the image pixel value in a complex but systematic manner Arnold transform is used, it protects the encrypted image from different security attacks because it is a cryptographic approach that generates confusion and dispersion. Furthermore, to add a layer of complexity Bessel Function a mathematical equation, is applied for substitution. This approach provides a customized encryption for every single image that provides strength to the encryption scheme for image-based data [12].

This study introduces a novel three-staged framework that combines chaotic scrambling, substitution, and multilayer diffusion for a colored image encryption. First, we use the Henon chaotic map to unpredictably permute the pixel positions, disrupting the original structure, followed by a Legendre function-based substitution that transforms pixel values into the complex geometric patterns. Finally, a multilayer diffusion technique through a circulant matrix spread the modified pixels, providing an additional layer of security against various attacks. Two main goals are achieved by this amalgamation of chaos, mathematical transformation, and diffusion: the first is accuracy and high security, and the second is resistance against different statistical and differential attacks, as demonstrated by extensive testing on diverse high-resolution satellite images and validated through key sensitivity, encryption speed, and attack resistance. The comparison of the current study with the latest literature also demonstrates its better performance. The brute force and different cryptanalytic attacks are rendered less effective because the proposed method uses a key from the Legendre function.

2.1 Henon map

It is a well-known 2D chaotic system applied in various cryptographic techniques, especially used in image encryption. Henon map [13] was instituted by Michel Henon in the year 1976.

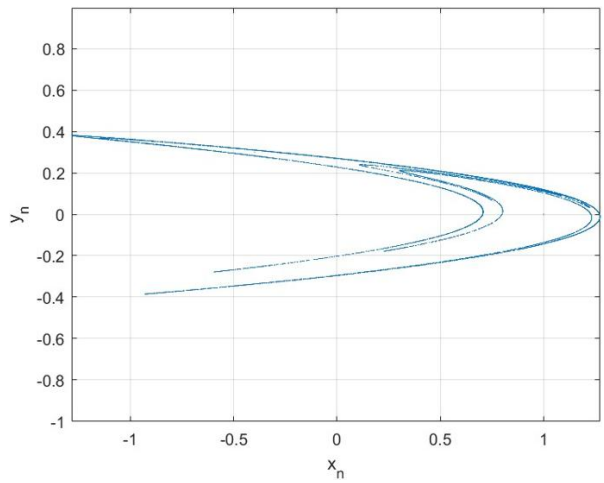


Figure 1. Henon map

The following iterative Eqs. (1) and (2) drive the Henon map:

$$x_{n+1} = 1 - ax_n^2 + y_n \tag{1}$$

$$y_{n+1} = bx_n \quad (2)$$

where, a=1.4 and b=0.3 are system parameters, the value of a ranges from [1, 1.5] and b ranges from [0.2, 0.4], (xn, yn) and (x_{n+1}, y_{n+1}) denote the old and new positions. The permutation in image pixels happens through iterative processes, which makes it a simple and efficient method. The Henon map is distinct in this regard because it is a one-to-one mapping that depends only on integer calculations. Figure 1 shows the behavior of the Henon map.

2.2 Legendre function

In past years, cryptographers have shown keen interest in using Legendre function [14] in substitution processes due to its ability to solve Legendre differential equation. It is also used in the field of physics and engineering. Legendre's differential equation is expressed as in Eq. (3):

$$(1-x^2)\frac{d^2y}{dx^2} - 2x\frac{dy}{dx} + n(n+1)y = 0 \quad (3)$$

where, $y = P_n(x)$, represents the Legendre polynomial of degree n (that can be 1-50), x lies in the range [−1, 1], and n is a non-negative integer, real number, depending on the type of Legendre function.

The Legendre function, characterized by its nonlinearity and orthogonality, introduces a high degree of unpredictability and randomness into the encryption process. This randomness plays a pivotal part in achieving confusion, a basic characteristic that hides the relationship between the original and encrypted images. By applying the Legendre function to pixel values, even minor changes in the input or encryption key result in notable alterations to the visual structure of the image, enhancing security.

2.3 Circulant matrices

A circulant matrix [11] is a type of square matrix in which each row is a rightward cyclic shift of the previous row. An $n \times n$ circulant matrix is considered prime circulant if the greatest common divisor of these elements in its circulant vector is 1. Figure 2 illustrates the proposed encryption scheme utilizing the specified algorithms.

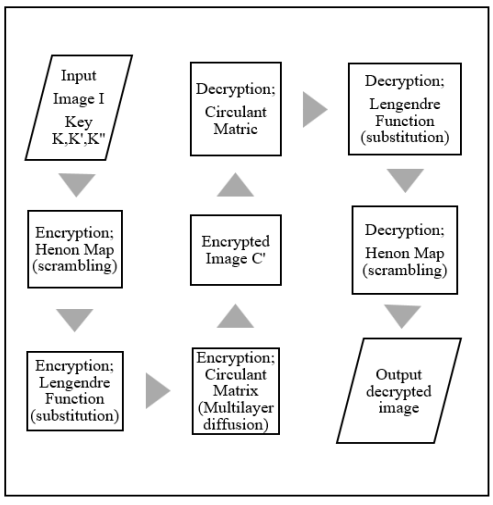


Figure 2. Flowchart of the suggested image encryption algorithm

3. PROPOSED ENCRYPTION AND DECRYPTION TECHNIQUE

Algorithm 1 explains the scrambling technique for colored images.

Algorithm 1. Scrambling technique

Input: The private key parameters (a, b, x_0, y_0) of Henon map and a primary color image *I* of size *mn*.
Output: Scrambed image C_1.
m=number of rows in I
n=number of columns in I

1. Generate chaotic sequence for all pixels by iterate Henon map for *mn* steps and store these values in an array X_{mn}.
2. Obtain a permutation matrix *Perm* by sorting X_{mn} , ascendingly.
3. Permute each pixel of *I using Perm* to get the Henon-scrambled image C_1.

Algorithm 2 explains the substitution technique or colored images.

Algorithm 2. Substitution technique

Input: C_1 the Henon-scrambled image, the degree *n* of the Legendre polynomial and the linear domain *[−1, 1]*.
Output: intermediate ciphered image C_2

1. Compute Legendre polynomial defined recursively:

$$P_0(x) = 1,\ P_1(x) = x,$$

$$P_{k+1}(x) = \frac{(2k-1)xP_k(x) - (k-1)P_{k-1}(x)}{k}, k \geq 2$$

Here, k goes from 1 to *n*.
2. Take *mn* random points x_{mn} from the interval *[-1, 1]*.
3. Compute $P_{k+1}(x)$ for each x_{mn} .
4. Reduce each value x_{mn} modulo 256 as.

$$K_{mn} = mod(|P_{k+1}(x_{mn})|, 256)$$

5. For each pixel of C_1 perform the following:

$$C_2(i,j) = C_1(i,j) \oplus K_{mn},$$

This alters pixel values.

Algorithm 3. Diffusion technique

Input: Substituted image C' and a numeric seed *s*.
Output: Final encrypted image C_3 .

1. Generate first row of circulant matrix as $r = randi(\mathbb{R}, 1, \max(m,n))using\ seed\ s$.
2. Construct the circulant matrix C by the row r as follows:

$$C(i,:) = circshift(r, [0, i-1]).$$

3. Convert C to integer values to generate F as follows:

$$F = floor\big(mod(C \times 10^{14}, 256)\big)$$

4. Convert the martices F, C_2 in to 1D array to get E and M, respectively.
5. Perform XOR diffusion as

$$Q_i = E_i \oplus M_i \oplus Q_{i-1}, \qquad i = 1,2, \ldots mn.$$

6. The $C'$is produces by reshaping vector$Q$.

In Algorithm 3 diffusion technique for colored images is explained.

The image is decrypted through operations that are the inverse of the encryption steps. The procedure is detailed in Algorithm 4.

Algorithm 4. Decryption technique

Input: Ciphered image C', private key parameters (a, b, x_0, y_0) the values X_{mn} and r.

Output: Original Image I.

1. Reverse the diffusion step as:

$$R_j = C'_j \oplus E_j \oplus R_{j-1},$$

$$C_2 = mod(|C - (R * r)|, 256)$$

2. Do XOR the Legendre key stream K_{mn}, with R as:

$$C_1 = C_2 \oplus K_{mn},$$

This recovers the Henon-scrambled image C_1.

3. Henon Map Scrambling reversal is obtained by applying inverse permutation $Perm^{-1}$ to obtain original pixel as follows:

$$I = Perm^{-1}(C_1)$$

4. This recovers the original image I.

4. PROPOSED ALGORITHMS IMPLEMENTATION

In our study, image testing is conducted using MATLAB 2018a. Several test images are selected, including the 512 × 512-pixel Baboon color image, along with four satellite images: Satellite image 1, Satellite image 2, Satellite image 3, and Satellite image 4. The satellite images are with a resolution of 512 × 512-pixel and sourced from the USC-SIPI database [15], are used to estimate the performance of our suggested method. For result comparison, the Baboon image and satellite images are encrypted using different encryption schemes. The outcomes of the Baboon and Satellite images processed with the proposed methods are presented in Figures 3-7.

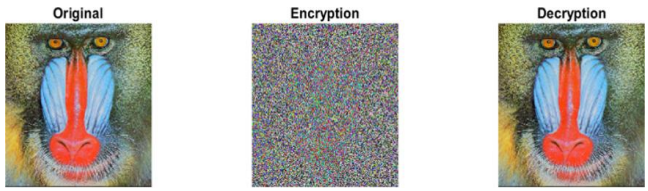


Figure 3. Encryption and decryption of images of Baboon (512 × 512)

In Figure 3, the original image shows the baboon colored image, the middle image shows the distorted image, result of our encryption scheme, and after performing the decryption process, the image is similar to the original image, which shows that our encryption scheme is practical and effective.

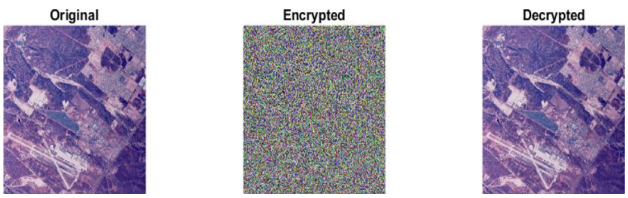


Figure 4. Encryption and decryption of Satellite image 1 colored (512 × 512)

Figures 4-7 show the encryption scheme applied to different Satellite images.

To assess the efficiency of the suggested technique, a round of numerical investigates are conducted on the developed algorithms. The detailed results are presented in this section, with the Baboon and Satellite Image 1 selected for the test analysis.

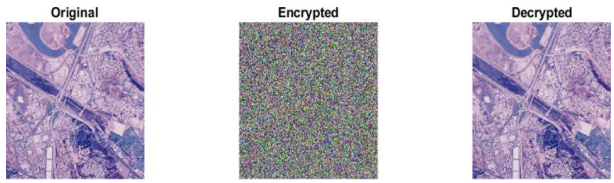


Figure 5. Encryption and decryption of Satellite image 2 colored (512 × 512)

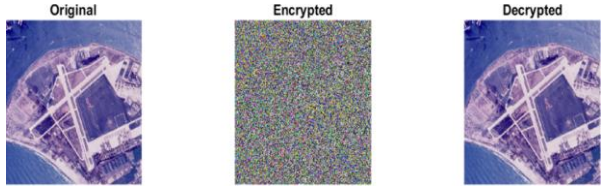


Figure 6. Encryption and decryption of Satellite image 3 colored (512 × 512)

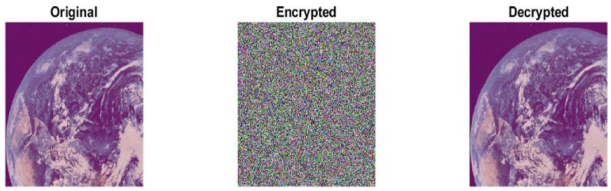


Figure 7. Encryption and decryption of Satellite image 4 colored (512 × 512)

4.1 Histogram analysis

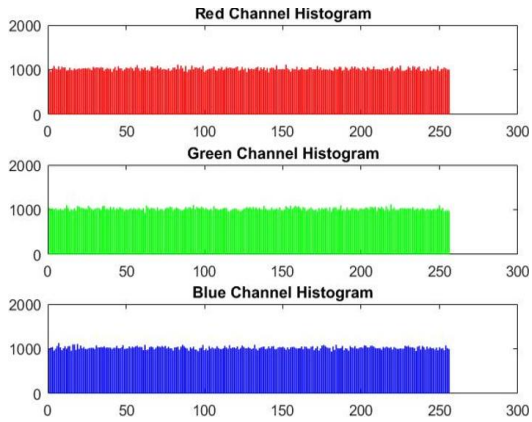


Figure 8. Histogram of Baboon's ciphered image colored (512×512)

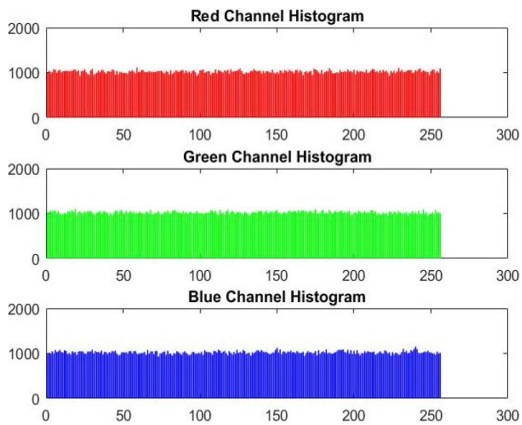


Figure 9. Histogram of Satellite's ciphered image colored (512×512)

Figures 8 and 9 display the histograms of the ciphered images for the Baboon and Satellite Image 1, showing the red, green, and blue channels. As seen in these figures, the histograms of the enciphered images are largely congruous.

4.2 Correlation analysis of adjacent pixels

Correlation is used in image processing, especially in cryptographic applications such as image encryption, to assess the dependency or relationship between adjacent pixels. Figure 10 illustrates the correlation of the plain Baboon image, while Figure 11 displays the correlation of the encrypted Baboon image.

Figure 12 shows the correlation of the plain satellite color image, while Figure 13 displays the correlation of the satellite cipher image.

Table 1 presents a comparison of the correlation coefficients for the plain and ciphered images. The lower correlation coefficient value of the encrypted image indicates that the encryption process has efficiently disrupted the natural correlation between adjacent pixels.

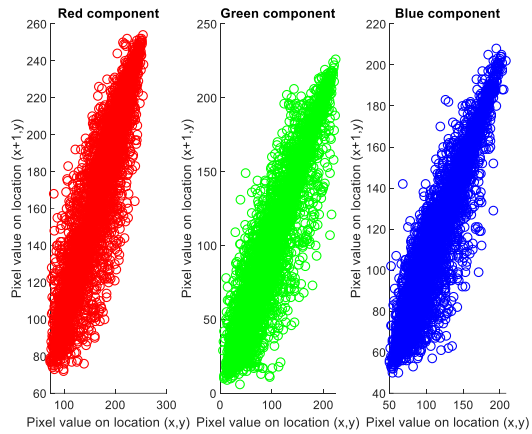


Figure 10. Correlation of Baboon's original image (512×512)

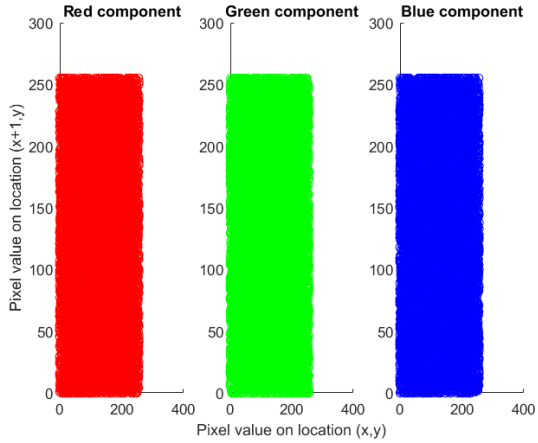


Figure 11. Correlation of Baboon's ciphered image (512×512)

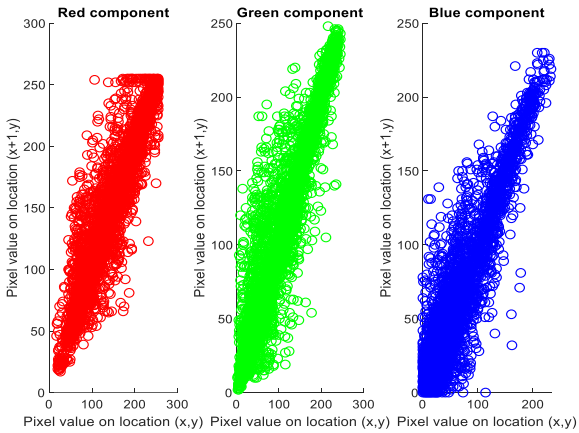


Figure 12. Correlation of satellite's plain image (512×512)

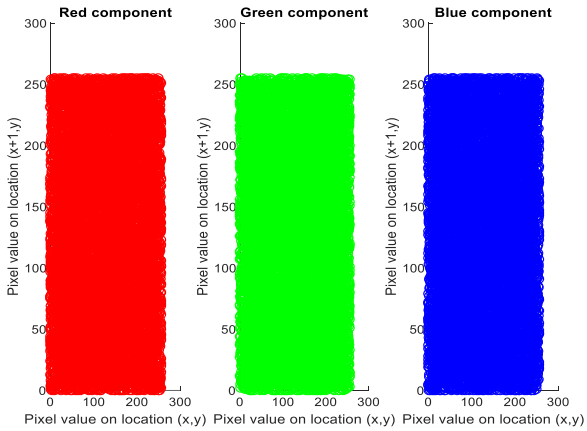


Figure 13. Correlation of Satellite's ciphered image colored (512×512)

Table 1. Correlation coefficients of Baboon, Lena, and Satellite images

		Direction	Red Plain Cipher	Green Plain Cipher	Blue Plain Cipher
Proposed	Baboon	Column-wise	0.8660 0.0030	0.7650 0.0038	0.8809 0.0037
		Diagonal-wise	0.8543 -0.0017	0.7348 -0.0043	0.8399 0.0037
		Row-wise	0.9231 -0.0018	0.8655 -0.0030	0.9073 0.0005
	Lena	Column-wise	0.9724 -0.0071	0.9708 0.0083	0.9473 0.0033
		Diagonal-wise	0.9226 0.0038	0.9174 0.0029	0.8806 0.0024
		Row-wise	0.9474 0.0033	0.9419 -0.0010	0.0035
	Satellite image 1	Column-wise	0.8657 -0.0004	0.8657 0.0019	0.8643 0.0022
		Diagonal-wise	0.8487 -0.0039	0.8591 -0.0048	0.8572 -0.0012
		Row-wise	0.8861 -0.0003	0.8844 -0.0034	0.8793 -0.0044
Reference [16]	Satellite image 1	Column-wise	0.8657 0.0003	0.8657 0.0013	0.8643 0.0002
		Diagonal-wise	0.8487 0.0011	0.8591 -0.0028	0.8572 -0.0012
		Row-wise	0.8861 -0.0002	0.8844 -0.0032	0.8793 -0.0044

4.3 Information entropy

Entropy determines the randomness of pixel intensity distributions in a ciphered image. For an 8-bit image, an encryption technique is considered effective if its entropy rate is near to 8. The entropy is computed by the following Eq. (4):

$$H(C) = \sum_{i=0}^{2^N-1} P(C_i) \log_2 \frac{1}{P(C_i)} \quad (4)$$

where, C represents an encrypted image, $P(C_i)$ be the probability of pixel C_i of the ciphered image. In order to secure an image encoding technique, it must be difficult to guess the plain image from the encoded version. An entropy value close to 8 indicates a low likelihood of predicting the plaintext from the ciphertext. Using MATLAB 2018a, the entropy rate of the ciphered Baboon image is found to be 7.9992, for Lena it is 7.9972, and for the Satellite image, the original entropy value is 7.1533. After applying our encryption scheme, the entropy value for the Satellite image increases to 7.9993. Table 2 provides a comparative overview of the information entropy values obtained.

Table 2. Entropy value analysis

Proposed Encryption Algorithm	Baboon	Lena	Satellite
Reference [17]	7.9771	7.9971	--
Reference [18]	7.9767	7.9967	--
Reference [19]	7.9700	7.9970	--
Reference [20]	7.9454	7.9970	--
Reference [21]	7.9992	--	7.9989
Suggested algorithm	7.9992	7.9972	7.9993

4.4 Number of Pixels Change Rate

NPCR (Number of Pixels Change Rate) is a test used in image encryption to assess the effectiveness of an enciphering technique in modifying the pixel value of the image. It computes the percentage of pixels that differ in the ciphered image upon the alteration of one pixel in the original image. Its calculating equation is expressed in Eq. (5):

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \quad (5)$$

where, M and N represent the dimensions of the image. $D(i,j)$ is 0 if the pixel values are identical and $D(i,j)$ is 1 if the pixel values are different. Table 3 displays the evaluation of NPCR values.

Table 3. The result of NPCR values

Image Encryption Algorithm	NPCR Value Baboon	NPCR Value Satellite
[21]	99.5992%	--
[22]	99.6045%	--
[23]	99.6096%	99.6032%
Proposed algorithm	99.6076%	99.6043%

4.5 Mean Square Error Analysis

The Mean Square Error (MSE) measures the variation between the plain and ciphered images. A higher MSE value indicates a greater difference between the original and ciphered images. To find MSE, the following Eq. (6) is used:

$$MSE = \frac{1}{m \times n \times 3} \sum_{i=0}^{m-1}\sum_{i=0}^{n-1} \left[I_p(i,j) - I_D(i,j) \right]^2, \quad (6)$$

where, m *and* n show the number of rows and columns independently, I_p *and* I_D show the original and enciphered images, respectively. Table 4 shows the assessment of MSE values.

Table 4. MSE values of different algorithms

Algorithm	MSE Value Baboon	MSE Value Satellite
Reference [22]	12595	--
Proposed algorithm	8641.2263	7421.7734

4.6 Peak Signal-to-Noise Ratio

The Peak Signal-to-Noise Ratio Analysis (PSNR) quantifies the similarity between the original and ciphered images. PSNR is measured by the following Eq. (7):

$$PSNR = 10.\log \frac{255^2}{MSE}(db) \quad (7)$$

For an effective encryption algorithm, the PSNR value between the plain and ciphered images should be as low as possible. Table 5 shows the comparison of PSNR values.

Table 5. The comparison of the data PSNR value

Image Encryption Algorithm	PSNR Value of Baboon	PSNR Value of Satellite
Reference [24]	19.4197 dB	--
Reference [16]	8.7827 dB	--
Proposed algorithm	8.780156 dB	9.4344 dB

4.7 Chi-Square test

This test is a numerical approach used to measure the randomness and consistency of pixel intensity distribution in enciphered images. In image encryption, it determines whether the pixel distribution in the ciphered image significantly differs from the plain image, ensuring that the encryption procedure efficiently hides the image content. This statistical attribute for an image is computed using the following Eq. (8):

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i} \quad (8)$$

where χ^2 denotes the Chi-square, n denotes the total number of observations (such as pixel values in an image), O_i denotes the observed value (pixel intensity in the ciphered image), and E_i denotes the expected value (pixel intensity in the original image or derived from a uniform distribution). The Chi-Square values for the analysis images are provided, comparing the values for the Baboon and Satellite color images. Table 6 presents the Chi-Square values for the Baboon and Satellite Image 1.

Table 6. The data of Chi-square value

Image Encryption Algorithm	Chi-Square Test Value Baboon	Chi-Square Test Value Satellite Image 1
Proposed algorithm	Chi-Square Statistic: 54329643 Critical value (α=0.05): 263336	Chi-Square Statistic: 47457580 Critical value (α=0.05): 263336

4.9 Key space analysis

Three different keys (a, b, x_0, y_0), x_{mn} and r are used in our proposal. The key parameters $(a, b, x_0, y_0)$are the control parameters of Henon map. If we take the precision of (a, b, x_0, y_0) to be 10^{-15}, there are $(10^{15})^2 \times (10^{15})^2 = (10)^{60} \approx (2)^{240}$ number of ways, exist of choosing these parameters. This shows that our proposed technique has a huge keyspace to resist brute force attack. The values x_{mn} and r may be chosen randomly, that is why there are infinite many possibilities for choosing them. Table 7 displays the evaluation of key space size with a current study.

Table 7. Key space size

Encryption Technique	Keyspace Size
Reference [21]	$(2)^{232}$
Proposed algorithm	$(2)^{240}$

4.10 Computational time

Suppose that the fastest processor calculates 2^{80} calculations in one second. The number of calculations obtained through the processor is $2^{80} \times 365(\text{days}) \times 24(\text{hrs}) \times 60(\text{min}) \times 60(\text{sec})$. So, the total of $2^{240}/2^{80} \times 365 \times 24 \times 60 \times 60 = 10^{36}$ years is required that is sufficient to protect the entire encryption. This computational load is sufficient to resist brute force attack.

4.11 Key sensitivity analysis

For an extremely small change in the key, the ciphered image is completely different from the original image. For example, if we add 0.0000000000000001 to the key parameters a, b, one cannot get the original image after decryption.

4.12 Cryptanalysis

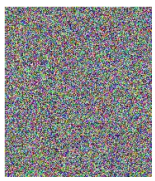
4.12.1 Chosen-plaintext attack

In this attack, the attacker has an encrypted image, without knowing the encryption key. He possesses an original image P^0 of all-zeroes (or all-one) and its relevant encrypted image C^0 attained with the similar key. The attacker makes the following sub key equations that are further used to extract the unknown key:

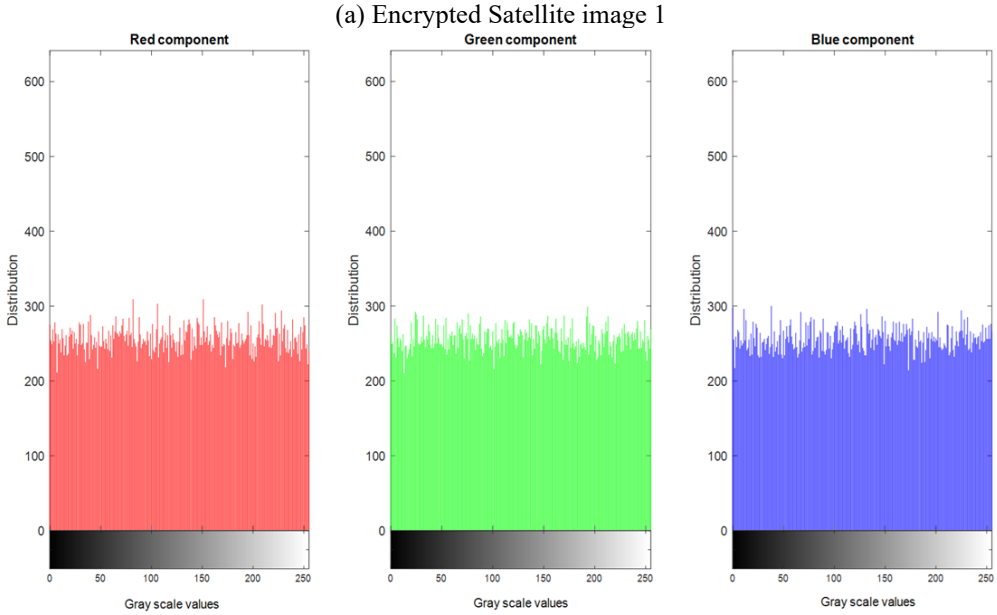
$$S_{i,j}^0 = C_{i,j}^0 \oplus P_{i,j}^0 \tag{9}$$

where, $P_{i,j}^0$ is a null image and $C_{i,j}^0$ is its relevant ciphered variation and (i,j) is the pixel position. Eq. (9) provides a key stream $S_{i,j}^0$. To find the original image $P_{i,j}$ of the encrypted $C_{i,j}$, the attacker uses the key-stream $S_{i,j}^0$ as given in Eq. (10):

$$P_{i,j} = C_{i,j} \oplus S_{i,j}^0 \tag{10}$$

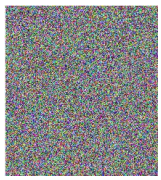


(a) Encrypted Satellite image 1

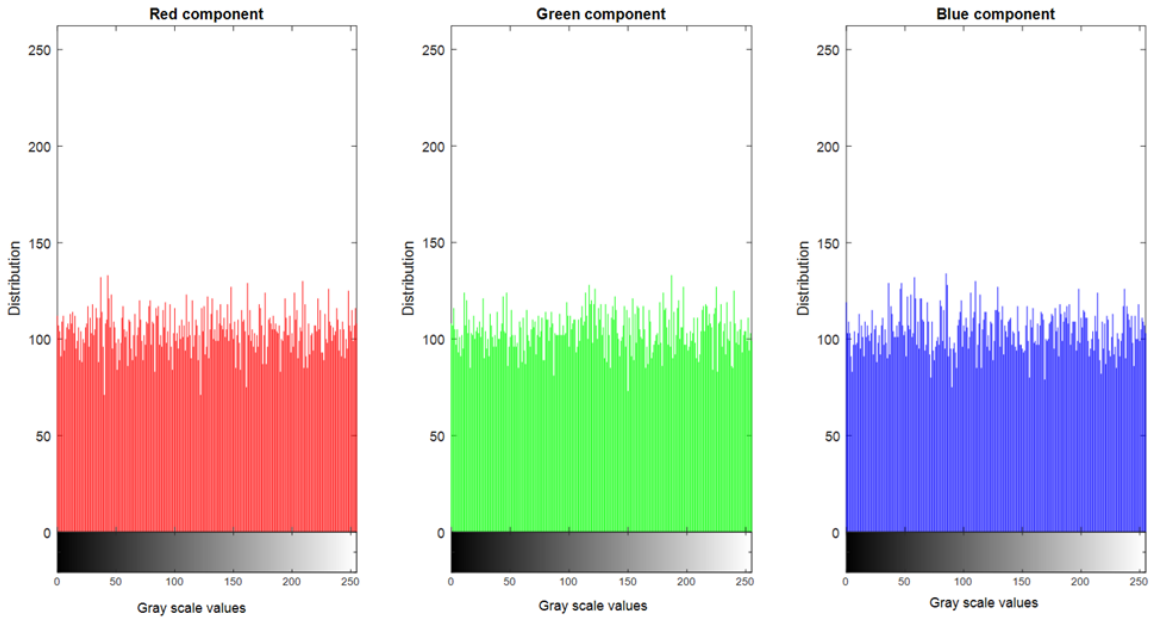


(b) Histogram of the Satellite image 1 ciphered image

Figure 14. Chosen-plaintext attack and corresponding image histograms



(a) Encrypted Satellite image 1



(b) Histogram of Satellite image 1 ciphered image

Figure 15. Chosen-chiphertext attack and corresponding image histograms

Figure 14(a) indicates that the chosen-plaintext attack using a null image to encrypt the image was unsuccessful. The corresponding histograms are shown in Figure 14(b).

4.12.2 Chosen-ciphertext attack

In this attack, with a knowledge of encrypted C' of all-one (or all-zero), and its equivalent ciphered alternate P', he makes attempts to decide the key sequenc $K'_{i,j}$ by the Eq. (9). The original image $P_{i,j}$would be obtained by Eq. (10).

Figure 15(a) indicates that the chosen-ciphertext attack using a null image to encrypt the image was unsuccessful. The corresponding histograms are shown in Figure 15(b).

5. CONCLUSIONS

This paper presents an inventive cryptographic scheme for the encryption of colored and satellite images by integrating the Henon map, Legendre function, and multilayer diffusion. The proposed approach surpasses conventional chaos-based encryption methods in terms of entropy and resistance to differential attacks. Experimental findings confirm its effectiveness in ensuring high security, randomness and resilience against various attacks. the combination of chaotic, algebraic and diffusion techniques enhances the scheme's robustness against different attacks, making it suitable for high-resolution images and real-life applications. This work represents a significant advancement in securing multimedia data within modern cryptographic systems, offering multi-level encryption with enhanced security, which reduces the chances of cyber-attack. Its performance has been authenticated through comparisons with existing techniques.

FUNDING

This research project was funded by the Deanship of Scientific Research and Libraries, Princess Nourah bint Abdulrahman University, through the Program of Research Project Funding After Publication, grant No. (RPFAP-73-1445).

REFERENCES

[1] Kanwal, S., Inam, S., Othman, M.T.B., Waqar, A., Ibrahim, M., Nawaz, F., Hamam, H. (2022). An effective color image encryption based on Henon map, tent chaotic map, and orthogonal matrices. Sensors, 22(12): 4359. https://doi.org/10.3390/s22124359

[2] Mahajan, P., Sachdeva, A. (2013). A study of encryption algorithms AES, DES and RSA for security. Global Journal of Computer Science and Technology, 13(15): 15-22. https://www.academia.edu/download/103623264/4-A-Study-of-Encryption-Algorithms.pdf

[3] Advanced Encryption Standard (AES). https://doi.org/10.6028/nist.fips.197-upd1

[4] Milanov, E. (2009). The RSA algorithm. RSA Laboratories, *1*(11). http://susanka.org/MathPhysics2/RSA_Algorithm_Yevgeny.pdf.

[5] 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(1): 5499538.

https://doi.org/10.1155/2021/5499538
[6] Muhaya, F.T.B. (2013). Chaotic and AES cryptosystem for satellite imagery. Telecommunication Systems, 52(2): 573-581. https://doi.org/10.1007/s11235-011-9462-z
[7] Widiono, S., Safriandono, A.N., Budi, S. (2024). Phishing website detection using bidirectional gated recurrent unit model and feature selection. Journal of Future Artificial Intelligence and Technologies, 1(2): 75-83. https://doi.org/10.62411/faith.2024-15
[8] Al-Khasawneh, M.A., Abu-Ulbeh, W., Khasawneh, A.M. (2020). Satellite images encryption review. In 2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI), Sanya, China, pp. 121-125. https://doi.org/10.1109/ICHCI51889.2020.00034
[9] Bensikaddour, E.H., Bentoutou, Y., Taleb, N. (2020). Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher. Journal of King Saud University-Computer and Information Sciences, 32(1): 50-56. https://doi.org/10.1016/j.jksuci.2018.05.002
[10] Usama, M., Khan, M.K. (2008). Classical and chaotic encryption techniques for the security of satellite images. In 2008 International Symposium on Biometrics and Security Technologies, Isalambad, Pakistan, pp. 1-6. https://doi.org/10.1109/ISBAST.2008.4547663
[11] Kanwal, S., Inam, S., Hajjej, F., Cheikhrouhou, O., Nawaz, Z., Waqar, A., Khan, M. (2022). A new image encryption technique based on sine map, chaotic tent map, and circulant matrices. Security and Communication Networks, 2022(1): 4152683. https://doi.org/10.1155/2022/4152683
[12] Yadav, A.K., Vishwakarma, V.P. (2024). An integrated Arnold and Bessel function-based image encryption on blockchain. Evaluation, 15(4): 797-804. https://dx.doi.org/10.14569/IJACSA.2024.0150482
[13] Hénon, M. (1976). A two-dimensional mapping with a strange attractor. Communications in Mathematical Physics, 50(1): 69-77. https://doi.org/10.1007/BF01608556
[14] Seres, I.A., Horváth, M., Burcsi, P. (2025). The Legendre pseudorandom function as a multivariate quadratic cryptosystem: Security and applications. Applicable Algebra in Engineering, Communication and Computing, 36(2): 223-253. https://doi.org/10.1007/s00200-023-00599-2
[15] The USC-SIPI Image Database. http://sipi.usc.edu/database/, accessed on May 5, 2025.
[16] Zhao, J., Zhang, T., Jiang, J., Fang, T., Ma, H. (2022). Color image encryption scheme based on alternate quantum walk and controlled Rubik's Cube. Scientific Reports, 12(1): 14253. https://doi.org/10.1038/s41598-022-18079-x
[17] Wang, X., Zhang, H.L. (2015). A color image encryption with heterogeneous bit-permutation and correlated chaos. Optics Communications, 342: 51-60. https://doi.org/10.1016/j.optcom.2014.12.043
[18] Huang, L., Cai, S., Xiong, X., Xiao, M. (2019). On symmetric color image encryption system with permutation-diffusion simultaneous operation. Optics and Lasers in Engineering, 115: 7-20. https://doi.org/10.1016/j.optlaseng.2018.11.015
[19] Alvarez, G., Li, S. (2003). Cryptographic requirements for chaotic secure communications. arXiv preprint nlin/0311039. https://doi.org/10.1142/S0218127406015970
[20] Wang, X., Liu, L., Zhang, Y. (2015). A novel chaotic block image encryption algorithm based on dynamic random growth technique. Optics and Lasers in Engineering, 66: 10-18. https://doi.org/10.1016/j.optlaseng.2014.08.005
[21] Sethi, J., Mishra, S.K., Dash, P.P., Bhutani, M. (2025). Secure image encryption with optimized chaotic sequences and multi-layer cryptographic operations. SN Computer Science, 6(7): 879. https://doi.org/10.1007/s42979-025-04407-1
[22] Sarkar, P., Das, A.K., Saha, A., Mandal, M.K. (2025). Two dimensional chaotic scheme for image encryption in FPGA. Analog Integrated Circuits and Signal Processing, 123(3): 1-15. https://doi.org/10.1007/s10470-025-02401-4
[23] Shahna, K.U., Mohamed, A. (2020). A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. Applied Soft Computing, 90: 106162. https://doi.org/10.1016/j.asoc.2020.106162
[24] Ihsan, A., Doğan, N. (2023). Improved affine encryption algorithm for color images using LFSR and XOR encryption. Multimedia Tools and Applications, 82(5): 7621-7637. https://doi.org/10.1007/s11042-022-13727-w