International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ROBUST COLOR IMAGE ENCRYPTION FRAMEWORK LEVERAGING CHAOTIC LOGISTIC MAP AND CONIC CURVES

[1]Ratheesh T K, [2]Dr. Varghese Paul
[1]Research Scholar, Division of Information Technology, School of Engineering, Cochin University of Science and Technology (CUSAT), tk.ratheesh007@gmail.com
[2]Professor (Rtd), Division of Information Technology, School of Engineering, Cochin University of Science and Technology (CUSAT), vp.itcusat@gmail.com

Abstract

In the digital era, securing visual information has become critically important due to the exponential growth of multimedia data sharing over insecure channels. Image encryption plays a critical role in preserving data confidentiality, especially when transmitting sensitive visual information. Traditional encryption methods often struggle to efficiently handle the high redundancy, pixel correlation, and dimensionality of color images, making them vulnerable to statistical and differential attacks. To overcome these limitations, this study introduces a robust color image encryption framework that integrates the chaotic behavior of the logistic map with dynamically modulated conic curves to generate spatially adaptive key maps. A user-defined password is hashed using Secure Hash Algorithm (SHA)-256 to generate a seed for the chaotic logistic map, which produces six values used to modulate conic curve coefficients. These coefficients form a spatially varying key map that is applied via pixel-wise XOR across RGB channels. The logistic map ensures high sensitivity to initial conditions, while the conic transformation enhances entropy and diffusion, resulting in a secure and unpredictable encryption process. Experimental validation is conducted on a benchmark image dataset, using evaluation metrics such as Number of Pixel Changing Rate **(**NPCR), Unified Averaged Changed Intensity (UACI), and Shannon entropy to assess encryption strength. The proposed model achieves an average NPCR of 99.61%, UACI values up to 33.40%, and entropy values approaching 7.89, indicating high resistance to differential and statistical attacks. Additionally, the decryption process accurately reconstructs the original image when the correct password is provided, confirming the reversibility and reliability of the scheme. This framework provides a reliable and computationally efficient approach for encrypting color images securely.

Keywords: Encryption, Conic curves, Histogram, Decryption, Chaotic logistic map, Secure hash algorithm

INTRODUCTION

With the continuous growth of digital data and the widespread use of multimedia content across communication platforms, the need for secure image transmission and storage has become essential. The color images, which are widely used in domains like healthcare, digital forensics,

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

surveillance, and social networking, are highly susceptible to unauthorized access, tampering, and privacy breaches [1, 2]. Image encryption transforms readable image data into unintelligible cipher forms, thus ensuring confidentiality, integrity, and authenticity during storage and transmission [3, 4]. Unlike text data, images have unique characteristics such as a high level of repetitive pixel information, occupy a large amount of storage due to their size, and exhibit effective correlations between adjacent pixels. These features require dedicated encryption strategies rather than direct application of classical cryptographic algorithms. Figure 1 illustrates the general workflow of image encryption and decryption.

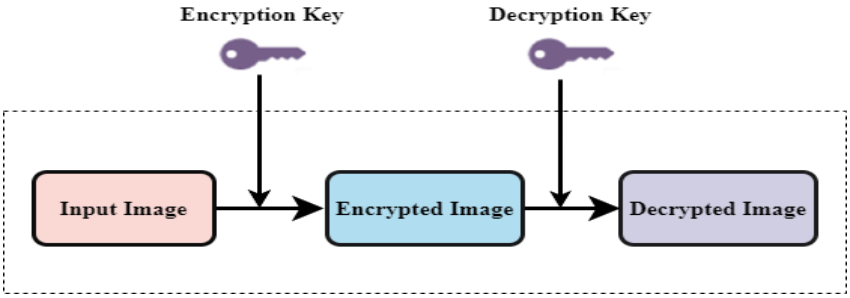


Fig. 1. Overview of the Image Encryption and Decryption Process

Color images are usually represented using the RGB model, in which each pixel is characterized by a mix of intensity values for the red, green, and blue components. Encryption schemes must protect not only just grayscale intensity, but also multi-channel data while maintaining computational efficiency. Common encryption algorithms are broadly categorized into symmetric, asymmetric, and hybrid methods. Symmetric encryption algorithms use a single shared key for both encryption and decryption, providing high speed but necessitating secure key distribution [5]. In contrast, asymmetric encryption employs a pair of public and private keys, offering efficient security but with greater computational demands [6]. Hybrid systems attempt to balance performance and robustness by combining the two approaches [7, 8]. However, these conventional schemes are often insufficient for image data due to limitations in key generation, sensitivity, and resistance to modern attacks. To overcome such challenges, chaos-based encryption techniques have emerged as a powerful alternative. Chaos theory introduces properties such as sensitivity, deterministic randomness and unpredictability, making it highly suitable for cryptographic key generation and pixel scrambling [9]. Among various chaotic systems, the logistic map is especially popular for its simplicity and effective nonlinear dynamics. When integrated into encryption systems, chaotic maps generate pseudo-random key streams that effectively disrupt pixel correlation and enhance confusion and diffusion mechanisms.

Even chaos-based methods are susceptible to cryptanalytic attacks if not properly implemented with spatial complexity or password sensitivity. Weak key design or predictable structures leave encrypted data vulnerable to brute-force, statistical, or differential attacks. Hence, modern research in image encryption increasingly explores the fusion of chaotic behavior with mathematical

Received: August 02, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

transformations or spatial modulation techniques to strengthen the cryptosystem. This study contributes to this evolving field by presenting an advanced encryption framework that ensures high entropy, efficient key dependence, and resilience to standard attack vectors. The approach promises a practical, lightweight solution for real-time image protection with effective cryptographic guarantees. The key objectives of the proposed encryption method are:

- To design a robust and lightweight color image encryption and decryption frameworks that integrates chaotic logistic map dynamics and conic curve-based spatial modulation.
- To implement a password-based key generation mechanism using SHA-256 hashing.
- To evaluate the security and performance of the model using standard metrics such as NPCR, UACI, and entropy.

The subsequent section of the paper is arranged as follows: Section 2 reviews recent developments in image encryption. Section 3 details the suggested methodology. Section 4 discusses the results and analysis, while Section 5 includes conclusion.

RELATED WORKS

Color image encryption method was developed by Pirdawood et al. [10], using the Elzaki transformation in combination with an infinite series of hyperbolic functions and coefficients of the Maclaurin series. Encryption was achieved by performing the Elzaki transform on image data and keying the obtained coefficients using modular arithmetic. The decryption method uses the inverse Elzaki transform. The model was evaluated with statistical metrics like correlation coefficients, histogram analysis, MSE, and PSNR. Results demonstrated that the model performed better encryption with high confidentiality due to the complexity of the private key, defined as a sum of modular multiples, which resists brute-force attacks. This approach had relatively high computational effort in processing time and introduced overheads due to transform-based processing. The lack of adaptive key management and dependency on continuous mathematical series limit real-time applicability. Alexan et al. [11] introduced an encryption scheme combining several chaotic maps with the Key Agreement Algorithm (KAA) map to provide enhanced security. Confusion was created using two keys from the 2D logistic-sine map. Diffusion was applied through the KAA map. The technique was tested using histograms, entropy, correlation, MSE, PSNR, NPCR, UACI, and NIST SP 800 tests. Experiments demonstrated the algorithm's security against statistical, visual, differential, and brute-force attacks based on very low correlation coefficients and a large key space. System dependence on multiple chaotic maps made computation more complex and key management overhead.

He et al. [12] suggested compressive sensing (CS) with DNA coding and chaotic systems for color image encryption. The model applied 2D CS to compress the image into measurement matrices, optimized by Singular Value Decomposition (SVD) for enhanced reconstruction. These matrices were subsequently scrambled via a Josephus-based permutation algorithm and encrypted with random DNA rules, followed by chaotic sequence-based diffusion. Original chaotic system

Received: August 02, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

parameters were image-dependent, which increased immunity to known-plaintext and chosen-plaintext attacks. Simulation on standard images verified better security metrics, high entropy, and immunity to common attacks. However, the model had limitations in terms of reconstruction speed and susceptibility to occlusion attacks. Further, its performance reduced with application on images of non-square sizes, reflecting limited flexibility in diverse real-time transmission situations and the model had high computational overhead and was inefficient in specific operation conditions. A multiple image encryption model for fast and secure encryption utilizing parallel processing was proposed by Alexan et al. [13]. The model employed a hyperchaotic 4D Chen system to produce pseudo-random keys and generate 6 S-boxes applied to RGB channels and three spatial axes. Evaluation results showed that the model obtained a PSNR of 8.07 dB, an entropy of 7.99, 99.625 NPCR, 33.3% UACI, and an MSE of 10281.1. However, the use of multiple chaotic systems and parallel processing enhanced the system complexity and hardware dependency.

A three-phase color image encryption algorithm was developed by Cao et al. [14], integrating bit-level scrambling, sweeping operations, and an evolutionary codebook with a chaotic system. Binary bits of the image were scrambled with rectangular structures and logistic maps. This image was processed using XOR operations across the rows and columns to improve diffusion. The codebook was updated through crossover and mutation based on chaotic sequences for encryption. Experimental results on BSD dataset images outperformed the traditional models. The model had limitations due to the exponential growth of the codebook size with large bit sequence length, restricting scalability and increasing memory demands. A fast and secure color image encryption system leveraging binary tree (BT) structure and chaotic maps was proposed by Elmenyawi [15]. The model comprised three phases such as key generation using XOR operations and hash functions, confusion through BT-structured color block traversal to disrupt adjacent color continuity, and diffusion through pixel-level scrambling and DNA-based chaotic operations. The tent and duffing chaotic maps introduced dynamic unpredictability. The BT-based confusion mechanism improved color separation, contributing to encryption efficiency. One of the limitations was its reliance on proper color block partitioning and traversal rules, which were not generalized well across non-standard image formats. Bit-level BT transformations increased algorithmic complexity, affecting memory usage in constrained environments.

Es-sabry [16] proposed a 32-bit color image encryption model utilizing four 1D chaotic maps such as chebyshev, tent, sine, and logistic to produce matrices that guided the encryption of RGBA channels. The method incorporated right circular shifts based on pixel coordinates and employed the foursquare cipher for value substitution. Further confusion was introduced using the Arnold cat map for rearranging pixel positions. The use of multiple chaotic maps and layered ciphers significantly enhanced security. However, the encryption of four separate channels increased algorithmic complexity and computational load. An encryption model utilising DNA subsequence operations, integrating adaptive diffusion phases and high-speed permutation, was developed by Mirzajani [17]. The model utilized chaotic principles for shuffling and value substitution,

Received: August 02, 2025

Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

effectively securing RGB images. The algorithm achieved cryptographic performance with high NPCR values and UACI values near 32.9%. Security evaluations, including chi-square tests, entropy analysis, and pixel correlation coefficients, confirmed the encryption's robustness and randomness. The algorithm demonstrated resilience against occlusion and noise attacks and showed superiority over existing techniques in NPCR and UACI comparisons. However, the DNA subsequence operations increased processing complexity, especially for high-resolution images.

Abed [18] suggested an encryption method combining the Grey Wolf Optimization (GWO), URUK chaotic maps, and Arnold transform to improve security and efficiency. The algorithm separated RGB channels and applied unique keys to each for independent encryption. The Arnold transform ensured pixel permutation, while URUK chaotic maps generated key vectors for diffusion. GWO further shuffled pixel positions, minimizing correlation between adjacent pixels. Security evaluations, including entropy analysis, histogram uniformity, correlation coefficients, MSE, and PSNR, confirmed better efficiency. The algorithm achieved high entropy and low correlation values, demonstrating effective randomness and security. However, the approach introduced complexity due to multiple transformation stages and required high computational resources, which limit real-time applications. Hosny et al. [19] introduced an image encryption technique utilizing triple chaotic maps such as Lorenz, Henon, and 2D-Logistic to address limitations in security and efficiency. The method separated RGB channels and applied unique chaotic keys to each. The first set of keys enabled pixel permutation, while the second enabled diffusion of scrambled channels. Each channel used a distinct chaotic map, enhancing unpredictability and breaking pixel correlation. Security evaluations included entropy, histogram, correlation coefficient, MSE, PSNR, key sensitivity, and differential analysis. Comparisons with existing methods showed superior or equivalent performance in encryption quality. However, the method's complexity and reliance on multiple chaotic systems increased computational load, potentially limiting scalability in real-time systems.

Kamal et al. [20] developed an image encryption model utilizing Conic Curve Cryptography (CCC) integrated with complex number theory. Replacing Elliptic Curve Cryptography with CCC addressed known vulnerabilities, utilizing multi-hard problems such as GCC-IFP, CC-DLP, and CC-IFP. The encryption process included XOR operations and Arnold Cat Map-based permutation for enhanced confusion and diffusion. Experimental findings showed high entropy, low correlation, a PSNR of 8.51 dB, and an encryption time of 25 ms, validating the method's security and efficiency. However, reliance on complex number arithmetic and CCC increases implementation complexity, potentially limiting adaptability in constrained environments. A compression-encryption model employing Sudoku matrices, compressed sensing, and a 2D sine-logistic coupled hyperchaotic map (2D-SLCHM) was developed by Yao et al. [21]. The map exhibited enhanced chaotic behavior and broader chaotic ranges. An improved dung beetle optimization algorithm optimized compression thresholds, which improved the quality of reconstruction. Sudoku matrices were used for permutation, increasing randomness, while

Received: August 02, 2025

Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

bidirectional diffusion with dynamic key updates strengthened security. Experimental results showed effective encryption with acceptable reconstruction quality. However, limitations included image quality loss due to lossy compression, making it unsuitable for applications needing high fidelity. Additionally, the decryption process, involving the Orthogonal Matching Pursuit algorithm, resulted in longer computation times due to complex sparse signal reconstruction.

Husam et al. [22] presented an image encryption algorithm combining S-DES and present ciphers, enhanced by a 2D chaotic system for dynamic key generation. The algorithm executed four encryption rounds per cipher and the performance metrics showed encryption effectiveness such as high NPCR, UACI ranged between 19.93% and 22.00%, and correlation coefficients were near zero across all directions. High MSE (8945.72) and low PSNR (~8.61 dB) confirmed significant distortion in the cipher image. The SSIM values (0.0237, 0.0162) showed low structural similarity, and the algorithm exhibited reduced execution time compared to standard DES. However, limitations included lower UACI values than ideal and the use of lossy encryption quality metrics, which were unsuitable for high-fidelity image requirements. A lightweight symmetric block cipher for color image encryption with an F-function and a 3D Hindmarsh-Rose model to generate dynamic 6-bit octal S-boxes was proposed by Khudhair et al. [23]. A Gauss map was utilized to obtain shift values for enhancing confusion in addition to XOR and additive operations. Simulation on the Lena image proved better performance such as entropy values being close to 8 and correlation coefficients being almost zero in all channels, reflecting low redundancy. The F-function was found to be decisive, with its elimination reducing randomness by 30 to 40%. However, the algorithm's use of binary transformation and dynamic S-box generation was computationally expensive and impacted efficiency on resource-constrained devices.

An image cryptosystem employing a lifting scheme and chaotic systems was presented by Zhang et al. [24]. The method decomposed the image into low-frequency and high-frequency components, disturbed by pseudo-random sequences. Simulation results showed 99.60% NPCR and 33.47% UACI values for the Lena image, with faster encryption and high security. However, the system's dependence on chaotic sequences and key management posed challenges for practical implementation. Alrubaie et al. [25] developed a double-dynamic DNA sequence encryption and a chaotic 2D logistic map for image encryption. The method involved pixel scrambling, double DNA encoding, and XOR encryption with chaotic keys. Experimental results showed robust encryption, yielding a UACI of 32.81% and an NPCR of 99.55%, indicating high randomness and resistance to attacks. Hameed et al. [26] proposed a two-dimensional S-Box and Henon 2D map for color image encryption. The S-Box was evaluated using metrics such as resistance to differential attacks, histograms, correlations, and entropy, yielding a UACI of 34.58% and an NPCR of 98.87%. The results showed robust encryption performance, however, limitations included reliance on specific maps and computational time for generating the S-Box, affecting real-time applications.

2.1.Research Gap

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Despite significant progress in color image encryption techniques, existing methods suffer from trade-offs between security, computational efficiency, and adaptability. Many existing algorithms utilized chaotic maps and DNA coding, introducing increased computational complexity, limiting their real-time applicability [11, 15, 12, 17]. Transform-based models such as the Elzaki transform and compressed sensing are computationally intensive and sensitive to image size and format [10, ,12, 21]. Several studies depend on multilayer chaotic systems, which enhance security but complicate key management and scalability in constrained environments [13, 19, 20]. Moreover, approaches like conic curve cryptography or evolutionary codebooks introduce high randomness but lack flexibility when applied to irregular or high-resolution images [14]. Others include the lack of adaptive key management systems, limited validation on diverse datasets, insufficient testing under noise scenarios, and minimal attention to encryption schemes compatible with compressed or real-time streaming formats. Additionally, many algorithms focus only on encryption strength without equal emphasis on robust and accurate decryption under practical constraints. These limitations highlight the need for a secure, scalable, and lightweight encryption model for color images.

PROPOSED METHODOLOGY

The proposed model employed a robust and high-performance encryption model for color images using chaotic logistic mapping and conic curve-based spatial transformation. The methodology comprises six core stages such as password-based key generation, chaotic sequence generation, coefficient computation, key map creation, pixel-level encryption, and final reconstruction. The process begins with user input in the form of a textual password. This password is processed using the SHA-256 hashing algorithm to ensure high entropy and eliminate predictability. The first four bytes of the resulting hash are extracted and converted into a floating-point seed value within the range (0,1). This seed initializes the chaotic logistic map, known for its sensitivity to initial conditions. Using the logistic map, a sequence of chaotic values is produced. These values are then used to derive the coefficients of a conic curve. The conic curve introduces spatial variation by generating a key value for each pixel coordinate in the image. This spatially dependent key ensures that even identical pixel values at different locations receive different encrypted outputs. The input RGB image is split into its three-color channels. For each channel, a pixel-wise XOR operation is performed using the spatially varying key map. The encrypted channels are then merged to generate the final encrypted image, which appears visually random and structureless.

3.1.Dataset Description

The proposed model was evaluated using the Kodak image dataset, a well-established benchmark in image processing and computer vision, publicly available in the Kaggle repository [27]. The dataset comprises 24 high-quality true-color images stored in PNG format, each with 24 bits per pixel (8 bits per channel in the RGB scheme). Each image has a default size of 768×512 pixels and provides a full-frame, realistic scene with diverse textures, lighting conditions and

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

color distributions. Such features make the dataset most suitable for testing encryption algorithms since it is representative of real-world visual complexity in the form of high-contrast edges, gradients, and soft textures. This dataset is most commonly known and most frequently cited in the evaluation of image compression, denoising, restoration, and encryption methods, mainly because of its natural image data and high visual quality. Its moderate size of around 15 MB ensures that it remains lightweight for experimentation while still maintaining the robustness needed for academic and industrial validation. In this study, all images were employed to assist in achieving consistency and generalizability of results with respect to different types of content, including indoor and outdoor environments, smooth and textured areas, as well as contrasts of varying levels. These images were encrypted separately, and their security performance was measured using both statistical and visual metrics. Some of the sample images in the dataset are visualized in Figure 2.

Fig. 2. Sample images from the dataset

3.2.Password Based Key Generation

The preprocessed encryption method begins with a secure password-based key generation mechanism that transforms user input into a set of chaotic and geometric parameters [28]. This transformation depends on the cryptographic strength of the SHA-256 hashing algorithm, which ensures that minimal changes in the input password result in entirely different output values. This feature ensures high sensitivity, a desirable option for secure encryption. SHA-256 generates a 256-bit hash from any arbitrary-length input message. The process begins by padding the input to ensure its length becomes a multiple of 512 bits. The padding included a 1 bit followed by 0s and then a 64-bit representation of the original message length L, resulting in a padded message length that is a multiple of 512, as expressed in Equation (1).

$$Padded\ Length = L + 1 + K + 64 = 0\ (mod\ 512) \tag{1}$$

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

where K is the number of '0' bits added as padding. The message is then split into N 512-bit blocks and each block is processed using an eight initialized 32-bit words such as H_0 to H_7, with values defined by the SHA-256 standard. Each 512 block is expanded into 64 words $W_0, W_1, \ldots W_{63}$ using a message scheduling function as in Equation (2), (3) and (4).

$$W_t = \begin{cases} M_t & for\ 0 \le t \le 15 \\ \sigma_1(W_{t-2} - 2) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16} & for\ 16 \le t \le 63 \end{cases} \quad (2)$$

$$\sigma_1(x) = (x \gg 17) \oplus (x \gg 19) \oplus (x \gg 10) \quad (3)$$

$$\sigma_0(x) = (x \gg 7) \oplus (x \gg 18) \oplus (x \gg 3) \quad (4)$$

where $\oplus$ denotes bitwise XOR operation and $\sigma_0(x)$ is the non-linear bit wise transformation. In the compression phase, each word undergoes 64 rounds of bitwise operations and logical functions including AND, OR, XOR, Right Rotate (ROTR) and Modular additions. The main functions are expressed in Equations (5) to (8).

$$\Sigma_0(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \quad (5)$$

$$\Sigma_1(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x) \quad (6)$$

$$Ch(x, y, z) = (x \wedge y) \oplus (\neg x \wedge z) \quad (7)$$

$$Maj(x, y, z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) \quad (8)$$

where $\oplus$ denotes bitwise XOR operation, $ROTR^n(x)$ denotes right rotation of the 32-bit word x by n positions. Ch is the choose function and Maj is the majority function. Each round updates temporary variables using the Equations (9) and (10).

$$T_1 = h + \Sigma_1(x) + Ch(e, f, g) + K_t + T_t \quad (9)$$

$$T_2 = \Sigma_0(a) + Maj(a, b, c) \quad (10)$$

The hash values are then updated after each block, and the final digest is the concatenation of all updated H_0 through H_7, resulting in a 256-bit output as expressed in Equation (11).

$$Digest = H_0 \| H_1 \| \ldots . \| H_7 \quad (11)$$

3.3.Chaotic Sequence Generation via Logistic Map

Chaos theory is applied in encryption systems due to its intrinsic sensitivity characteristics to initial conditions, pseudo-randomness, ergodicity, and deterministic unpredictability [29, 30]. These features are used in image encryption tasks, where the objective is to eliminate visual redundancies, maximize entropy and ensure that the encryption relies heavily on the input key. Among the various chaotic systems available, the Logistic map is popular due to its simplicity, speed of

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

computation, and proven statistical characteristics. The logistic map is a non-linear, one dimensional, discrete-time recurrence relation, defined as given in Equation (12).

$$z_{n+1} = \mu \cdot z_n \cdot (1 - z_n), \;\; 0 < z_n < 1, \;\; 3.57 < \mu \leq 4 \tag{12}$$

where z_n is the current state, μ represents a control parameter that determines the system's behaviour, and z_0 is the initial seed value. The logistic map exhibits chaotic behaviour when the control parameter μ is set above 3.57. In the proposed model, μ is fixed at 3.99, a value known to generate fully chaotic sequences. These are sensitive to the initial value z_0, which is derived from a user defined password through SHA-256 hashing and normalization. The generated chaotic sequence is utilised to modulate the coefficients of a conic curve equation that governs spatial key variation in the image. The logistic map effectively eliminates the correlation between neighbouring pixels and introduces high entropy in the encrypted output. This enhances the encryption model's resistance to statistical and differential attacks. This logistic map utilization helps the proposed encryption framework to provide a lightweight and highly effective mechanism for key expansion, security reinforcement, and pixel confusion, all while maintaining computational efficiency suitable for real-time applications.

3.4.Conic Curve coefficient Computation

In the proposed encryption model, the spatial variation in pixel-level encryption is governed by a dynamically generated conic curve which serves as a nonlinear spatial key map. A conic curve is the locus of points that result from the intersection of a plane with a double-napped cone. Depending on the orientation and values of its parameters, it represents geometric shapes such as ellipses, parabolas and hyperbolas. The general form of a second-degree conic equation in two-dimensional space is expressed as in Equation (13).

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0 \tag{13}$$

where $A, B, C, D, E,$ and F are real constants (coefficients) and x, y are variables such as pixel coordinates. Each coefficient has a specific role such as A controls the curvature along the x-axis, B introduces rotation or skew, C controls the curvature along the y-axis, D, E introduce Linear shifts in x and y, and F represents global shift (constant offset). To ensure session-wise uniqueness and password dependence, the coefficient A through F are dynamically generated using values from a chaotic sequence generated by the logistic map. For each coeffcient, a base value a_i and scale factor s_i are obtained from the SHA-256 hash of the user's password. The coefficients are then computed as in Equation (14).

$$Coefficient = a_i \; + \; s_i \cdot z_i \; for \; i = 0 \; to \; 5 \tag{14}$$

This aproach ensures effective password sensitivity, slight changes in the password result in entirely different encryption outcomes. The use of a dynamically modulated conic equation adds geometric non-linearity, enhancing the model's complexity and resistance to cryptanalytic attacks.

3.5.Spatial Key Map Generation

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

After the coefficient calculation, the next step in the proposed encryption framework involves the generation of a spatial key map. This key map confirms that the encryption varies spatially across the image, introducing geometric non-linearity into the encryption process. To generate the spatial key, the conic expression is evaluated for every pixel coordinate (i, j) in the image as given in Equation (15).

$$H(i,j) = Ai^2 + Bij + Cj^2 + Di + Ej + F \quad (15)$$

where $A, B, C, D, E,$ and F are the conic coefficients calculated in the previous stage using password-dependent chaotic values, i and j represent the row and column indices in the image. The conic expression is evaluated for every pixel (i, j) in the image. $H\ (i, j)$ field is used as the spatially varying key map for encryption. The values are reduced to mod 256 to match the 8-bit range of pixel intensities, as expressed in Equation (16).

$$K(i,j) = H(i,j)\ mod\ 256 \quad (16)$$

This spatial key map $K(i, j)$ is then used in a pixel-wise XOR operation with the original image as given in Equation (17).

$$I'_{i,j,k} = I_{i,j,k} \oplus K(i,j) \quad (17)$$

where $I_{i,j,k}$ denotes the original intensity value of pixel (i, j) in color channel k, $I'_{i,j,k}$ is the encrypted output and $K(i, j)$ is the spatial key value from the conic map. This spatially dependent XOR operation confirms that identical pixel values at different positions are encrypted differently.

3.6.Image Encryption

The proposed image encryption model integrates password-based chaotic key generation and conic curve encryption to provide secure and efficient RGB image protection, as shown in Figure 3. The encryption process comprises six key stages, ensuring that each image is uniquely encrypted based on the user's input password and pixel coordinates.

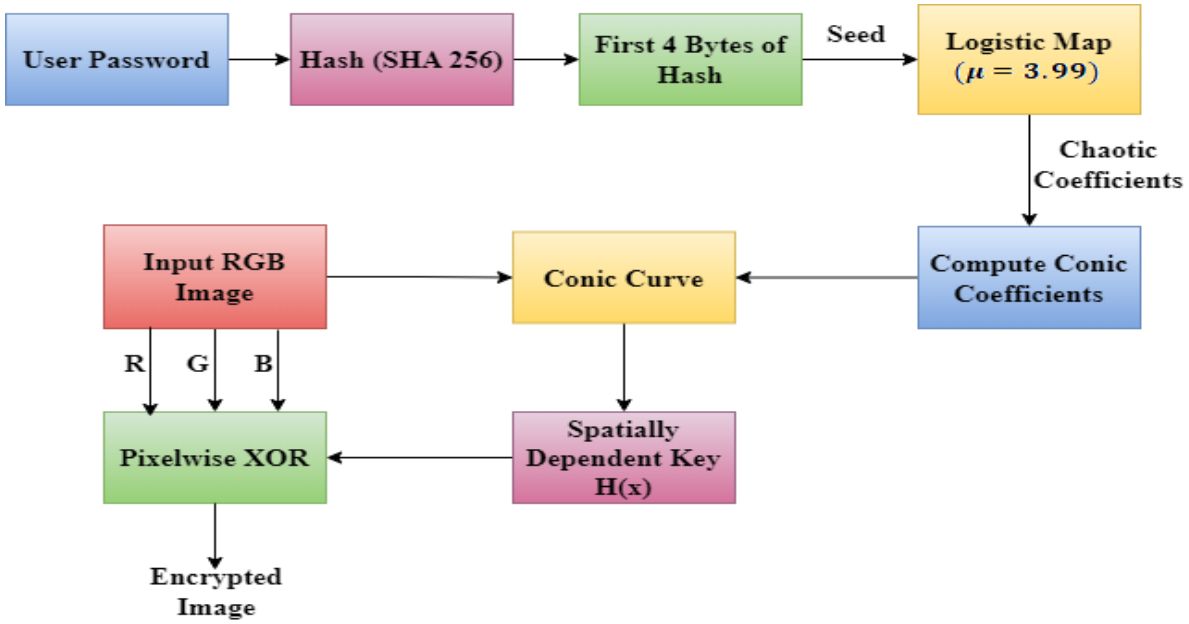


Fig.3. Work Flow of Proposed Image Encryption

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The process begins with the input of a standard RGB image, which is read as a three-dimensional array, where the first two dimensions represent the spatial resolution, such as height and width, and the third denotes the color channels such as red, green, and blue. This format allows individual access to each color component of every pixel for encryption. After that the user provides a textual password that is processed using the SHA-256 hashing algorithm. The resulting 256-bit hash digest serves as the basics for key generation. The first four bytes of the hash are converted into a floating-point number to act as the seed value for the chaotic logistic map. Additional bytes from the hash are utilised to derive a set of base values and corresponding scale factors, which are used to compute the coefficients of the encryption function. Next, a chaotic sequence is produced through the logistic map function, which is a simple and highly sensitive recursive function. The map was repeatdly iterated using the previously generated seed, generating a sequence of pseudo-random values. A subset of these chaotic values is used to calculate six dynamic coefficients that determine the structure and behavior of a conic curve.

These coefficients are used to evaluate a mathematical conic expression over the entire image. For each pixel location, the equation generates a unique value, which is reduced to match the valid range of pixel intensity values. This results in a spatial key map, where each pixel position is assigned a unique key based on its coordinates and the derived conic function. Finally, the RGB channels of the image are individually encrypted using a pixel-wise XOR operation. Each pixel's intensity in all three channels is masked using its corresponding value from the spatial key map. The result is a highly randomized, password-dependent encrypted image. This encrypted output, visually unrecognizable and statistically secure, is saved in PNG format to retain lossless quality and precision, ensuring it is reliably decrypted later using the correct key. The algorithm for the proposed image encryption process is given below.

Algorithm 1: Image encryption process using chaotic logistic map and conic curves

Input: *Static RGB image dataset. (natural color images in PNG format)*

User-defined encryption password

Output: *Efficiently encrypted images with high entropy and security.*

Start:

Step 1: Input RGB Image

- *Load the color image in RGB format.*
- *Image is loaded as a NumPy array of shape (H, W, 3).*

Step 2: Password-Based Key Initialization

- *Accept a user-defined password.*
- *Generate a SHA-256 hash from the password.*
- *Extract the first 4 bytes of hash to save as the seed for chaotic sequence generation.*

Step 3: Chaotic Sequence Generation

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- *Initialize the logistic map with the seed and parameter* $\mu = 3.99$.
  $z_{n+1} = \mu \cdot z_n \cdot (1 - z_n)$ $\mu = 3.99$ *is used to generate*
  6 chaotic values $z_1, z_2, \ldots . z_6$.

Step 4: Conic Coefficient Computation

- *Use the chaotic values to compute conic coefficients:*

$$A = a_0 + s_0 z_1, \quad B = a_1 + s_1 z_2, \ldots \ldots , \qquad F = a_5 + s_5 z_6$$

where a_i *are the base values and* s_i *are scale factors.*

Step 5: Spatial Key Map Generation

- *Evaluate the conic curve over the entire image grid* (i, j). *For each pixel (i, y), compute:*

$$H(i,j) = Ai^2 + Bij + Cj^2 + Di + Ej + F$$

- *Reduce results modulo 256 to produce the spatial key map* $K(i,j)$

$$K(i,j) = H(i,j)\ mod\ 256$$

Step 6: Pixel-wise XOR Encryption

- *Perform bit-wise XOR between each pixel value in R, G, B channels and the key map.*

$$I'_{i,j,k} = I_{i,j,k} \oplus K(i,j)$$

- *Apply the operation independently for all three channels.*

Step 7: Encrypted Image Output

- *Construct the encrypted image from the XOR results*
- *Save the encrypted output as a PNG file.*

End

3.7.Image Decryption

The image decryption process is employed to accurately reverse the encryption operations while maintaining security integrity. It follows the same sequence of operations as the encryption stages, depends on the same password input and mathematical framework to retrieve the original image from its encrypted version, as visualized in Figure 4. An efficient decryption depends entirely on the use of the identical password that was employed during the encryption process, which ensures robustness and brute-force attacks. The decryption process begins by uploading the encrypted image. The image is converted into a 3D array, preserving the structure of its red, green, and blue color channels. This format is important for enabling element-wise operations during the decryption phase. After that, the user provided a decryption password. The system processes this password using the same SHA-256 hashing mechanism as in the encryption phase. The resulting 256-bit hash digest is used to extract a seed value for the logistic map and a set of base values and scale factors. These parameters are critical for regenerating the exact chaotic sequence and conic coefficients that were used during encryption. Once the seed is obtained, the logistic map is

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

repeatedly applied to generate the necessary sequence of pseudo-random values. The sequence is then used to reconstruct the six dynamic coefficients of the conic curve.

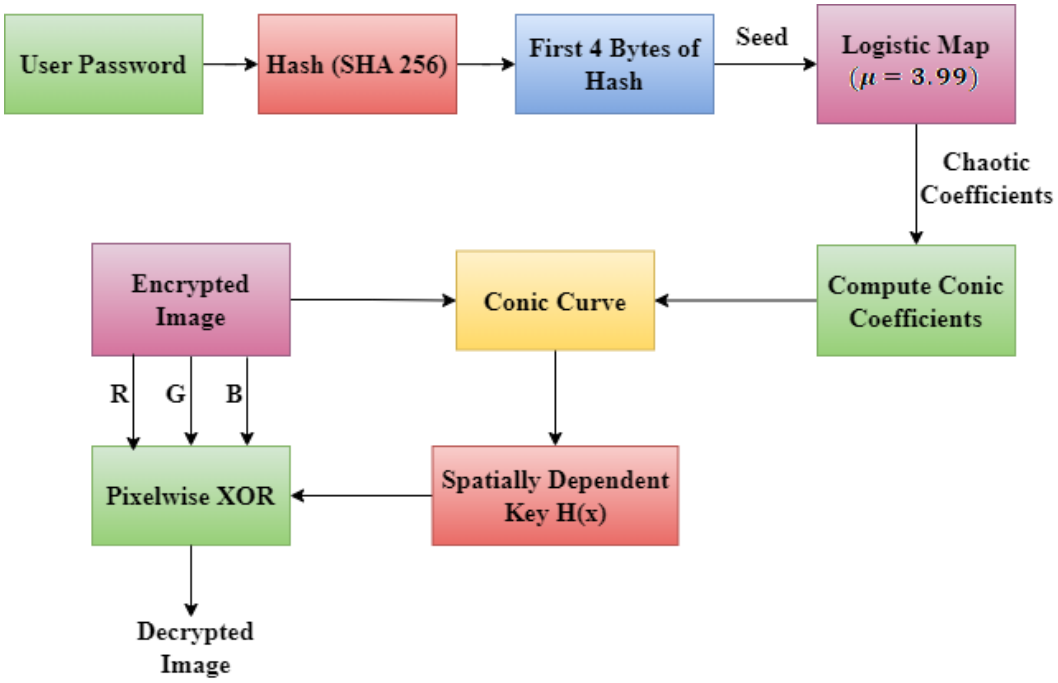


Fig. 4. Work Flow of Proposed Image Decryption

The system evaluates the conic expression over each pixel coordinate, producing a spatially varying key map. This key map is guaranteed to match the one used during the encryption process, assuming the password is correct. Finally, the actual decryption is performed by applying a pixel-wise XOR operation between the encrypted image and the spatial key map. Each color channel, such as R, G, and B is individually processed using the same logic applied during encryption. The resulting output is a visually accurate reconstruction of the original image, effectively decrypted and ready for further use. The algorithm for the proposed image decryption process is given below.

Algorithm 2: Image decryption process using chaotic logistic map and conic curves

Input: *Static encrypted image in PNG format*
User-defined decryption password

Output: *Efficiently decrypted images with high entropy and security.*

Start:

Step 1: Input encrypted image

- *Load the encrypted image.*
- *Convert it into a NumPy array of shape (H, W, 3).*

Step 2: Password-Based Key Regeneration

- *Accept a user-defined password.*

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- *Ensure the password is the same as the one used during encryption.*
- *Hash the password using SHA-256.*
- *Extract the seed and coefficient paarmeters from the hash..*

Step 3: Chaotic Sequence Generation

Initialize the logistic map with $\mu = 3.99$ *generates 6 chaotic values* $z_1, z_2, \ldots\ldots z_6$.

$$z_{n+1} = \mu \cdot z_n \cdot (1 - z_n)$$

- *Generate six pseudo-random chaotic values through iteration.*

Step 4: Reconstruct Conic Coefficents $A, B, C, D, E,$ *and* F.

- *Use the chaotic values, base values, and scale factors to compute the original six conic curve coefficients.*

$$Coefficient = a_i + s_i \cdot z_i \; for \; i = 0 \; to \; 5$$

Step 5: Spatial Key Map Regeneration

- *Evaluate the conic curve expression over the entire image grid* (i, j)

$$H(i,j) = Ai^2 + Bij + Cj^2 + Di + Ej + F$$

- *Reduce results modulo 256 to regenerate the spatial key map.*

Step 6: Pixel-wise XOR Decryption

- *Apply bit-wise XOR between each encrypted pixel value and the corresponding key map value.*

$$I'_{i,j,k} = I_{i,j,k} \oplus K(i,j)$$

- *Perform this operation independently for all three RGB channels.*

Step 7: Output Decrypted Image

- *Combine the decrypted R,G,and B channels*
- *Save the final decrypted image.*

End

RESULTS AND DISCUSSIONS

4.1 Simulation Setup

The suggested image encryption and decryption model was implemented in a high-performance computing environment equipped with an Intel Core i7 processor and an NVIDIA GTX 1080Ti GPU to ensure efficient computation. The development and implementation were carried out using Python, with deep learning support provided by the Keras API running on the TensorFlow backend. For training and experimentation, Google Colab was utilized, taking advantage of its cloud-based GPU acceleration to enhance accessibility, scalability, and reproducibility. This setup

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

allowed for encrypted and decrypted image processing and performance evaluation under consistent conditions.

4.2 Experimental Results

The experimental evaluation of the proposed chaotic logistic map and conic curve-based encryption model demonstrated reliable security features and consistent reversibility. Encryption outcomes showed that the image data was sufficiently randomized, making visual and statistical inference difficult. The decryption process effectively recovered the original images, suggesting the model's suitability for secure image communication. Performance evaluations including entropy, correlation, NPCR, and UACI indicated acceptable levels of diffusion and confusion, essential for reducing vulnerability to common attacks. Overall, the model performed efficiently without introducing excessive computational overhead, supporting its potential use in applications requiring lightweight and dependable image protection.

4.2.1 Encryption Results

Figure 5 visualizes the comparison between the original and the encrypted image. The original image displays a clear and natural scene, while the encrypted image, generated using the password 123456789, appears as a highly randomized, noise-like pattern. This visual distortion ensures that no structural or color-based cues from the original image are retained in the encrypted version, thereby confirming the encryption scheme's ability to conceal image content.

(a) (b)

Fig. 5. (a) Original Image (b) Encrypted Image

The chaotic sequence produced by the logistic map using the seed derived from the password is shown in Figure 6. The plot showcases the pseudo-random, non-repeating nature of the sequence over multiple iterations. This behavior forms the backbone of the key generation process, ensuring that slight changes in the password result in a significantly different encryption output.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

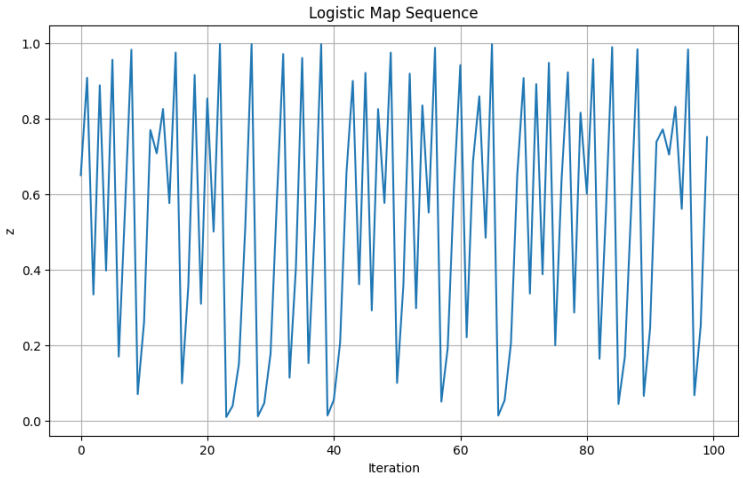
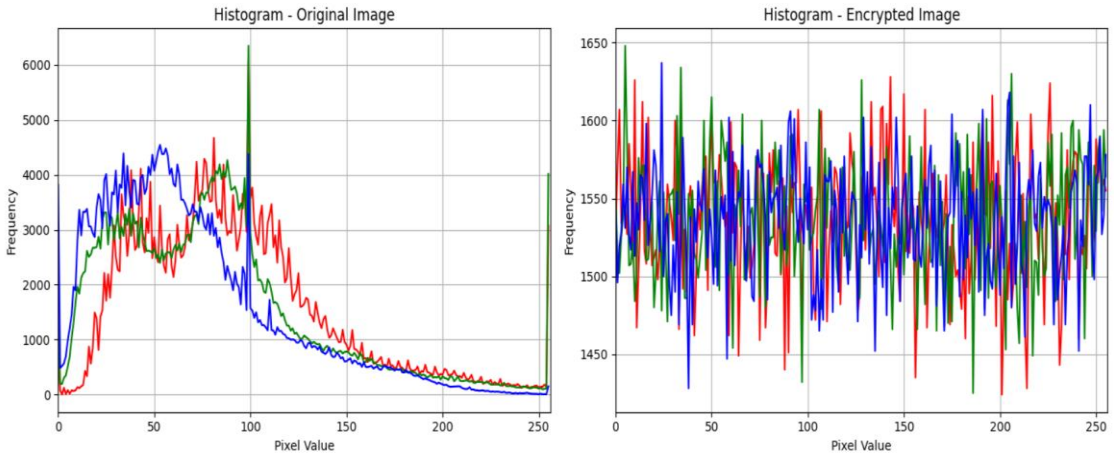


Fig. 6. Logistic Map Sequence

Figure 7 presents the histogram comparison between the original and encrypted images. A histogram displays how often each pixel intensity occurs in an image. For effective encryption, the histogram of the encrypted image should differ greatly from that of the original, ideally showing a uniform distribution. This uniformity demonstrates that the encrypted image has no statistical patterns, making it resistant to histogram-based attacks. The histogram of the original image displays uneven peaks and valleys, reflecting the natural distribution of pixel intensities in the R, G, and B channels valleys typical of natural scenes with structured color distributions. In contrast, the encrypted image exhibits a nearly uniform histogram across all three channels. This uniformity demonstrates that the proposed algorithm effectively disrupts the original statistical characteristics, thereby concealing color and intensity patterns. The flattened histogram demonstrates that the encryption process significantly enhances resistance to statistical and histogram-based attacks, a critical attribute for secure image transmission.



(a) (b)

Fig. 7. Histogram of (a) Original image (b) Encrypted Image

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

To emphasize the extent of modification between the original and encrypted images, a difference map is generated, as shown in Figure 8. This map visually depicts the pixel-wise changes and confirms that a significant portion of the image content has been altered. This visual transformation aligns with the high values observed in NPCR and UACI metrics.

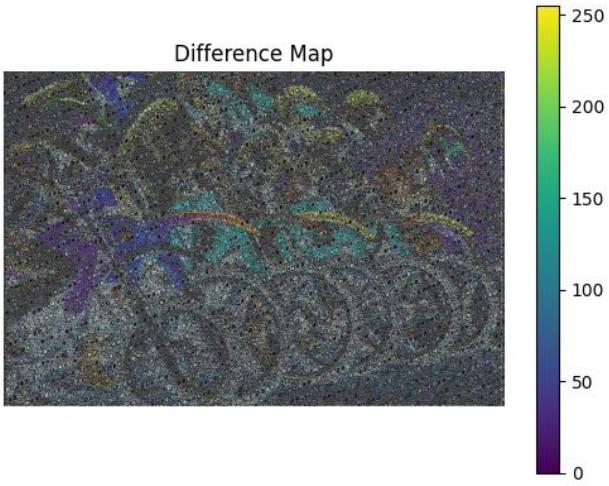


Fig. 8. Difference Map

Finally, pixel correlation plots are presented to compare the statistical dependency between adjacent pixels in the original and encrypted images, as depicted in Figure 9. While the original image demonstrates high correlation in all directions, the encrypted image shows almost no correlation. This confirms that the encryption algorithm disrupts spatial coherence, making the encrypted data resistant to statistical and structural analysis.

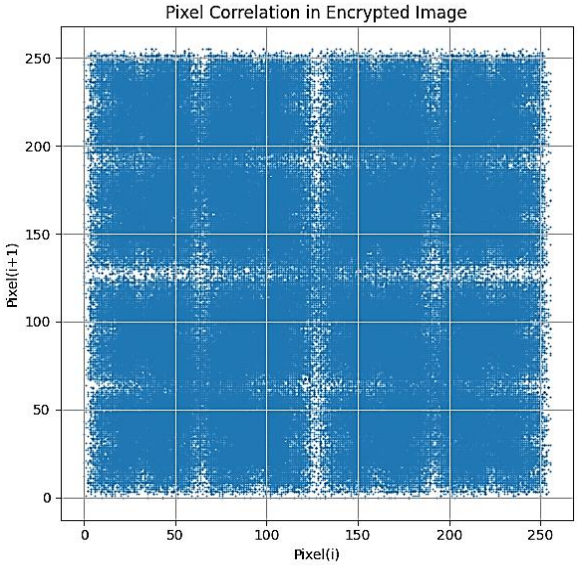


Fig. 9. Pixel Correlation in Encrypted Image

Received: August 02, 2025

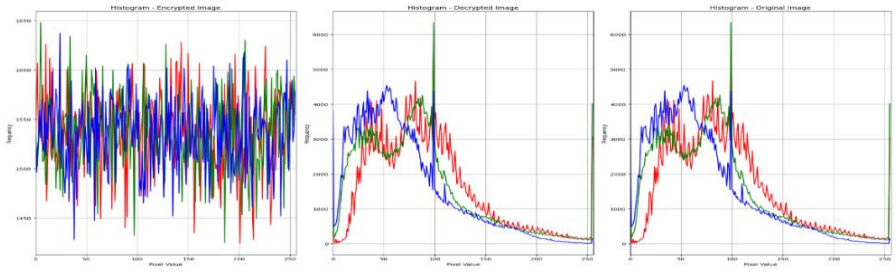
International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

i. Decryption Results

When the correct password 123456789 is used during the decryption process, the system successfully reconstructs the original image, demonstrating the accuracy and robustness of the proposed encryption-decryption framework. As visualised in Figure 10, the encrypted image appears completely noise-like and visually unrecognizable, reflecting robust security against visual attacks. Upon applying the correct decryption key, the output image is nearly identical to the original input, with no visible distortion, confirming perfect reversibility. The histogram comparison is shown in Figure 11. The encrypted image's histogram is uniformly distributed demonstrating a high level of randomness, while the decrypted histogram closely aligns with that of the original image, preserving the pixel intensity distribution across all RGB channels. Figure 12 visualizes the pixel correlation plot for the decrypted image, which demonstrates a dense diagonal structure, highlighting the recovery of natural spatial relationships between adjacent pixels. Lastly, Figure 13 illustrates the difference map between the decrypted and original images, which reveals near-zero deviation across most pixels, affirming that the decryption process yields a highly accurate reproduction. These results collectively validate the effectiveness of the suggested model in restoring encrypted images without loss, provided the correct password is used.

(a) (b) (c)

Fig. 10. Visual comparison of (a) Encrypted, (b) Decrypted and (c) Original images generated using the correct password



(a) (b) (c)

Fig. 11. Histogram Comparison of (a) Encrypted (b) Decrypted and (c) Original images generated using the correct password

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

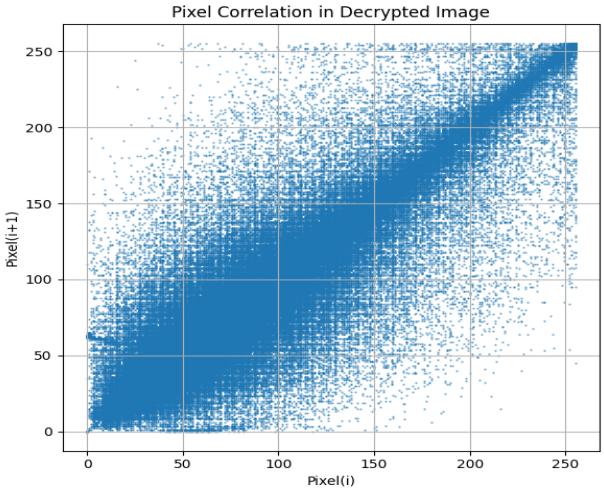


Fig. 12. Pixel correlation in decrypted image generated using the correct password

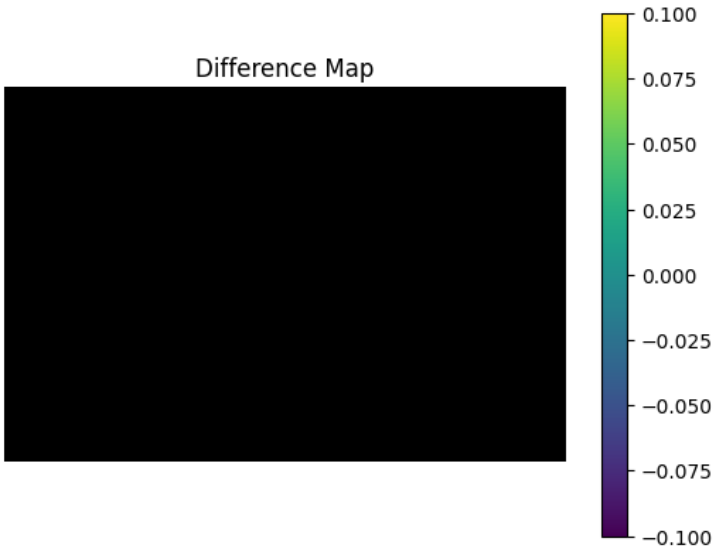
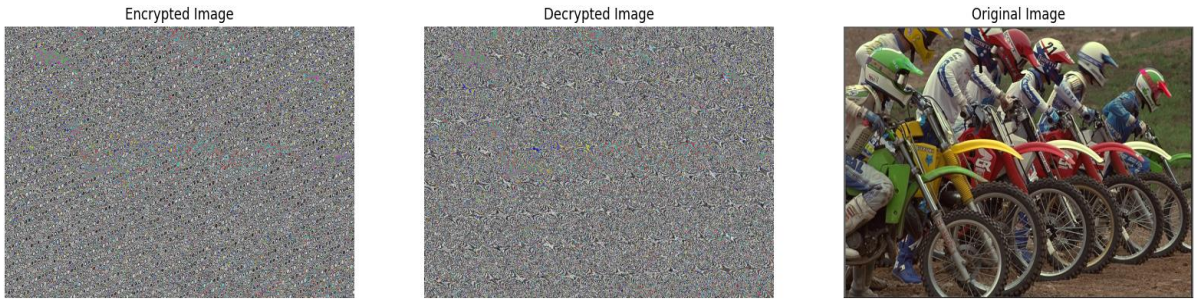


Fig. 13. Difference map generated using the correct password.

When the wrong password 87654321 is used for decryption, the resulting output significantly deviates from the original image, as observed in Figure 14. While the encrypted image remains visually indistinguishable from random noise, the decrypted image, due to incorrect key generation, does not reconstruct any meaningful visual content and still exhibits a noise-like structure. This contrasts sharply with the original image, highlighting the model's high sensitivity to password correctness. Histogram analysis is shown in Figure 15. The encrypted and incorrectly decrypted images both display uniformly distributed pixel intensity histograms across all color channels, indicative of intense diffusion, while the original image exhibits a natural, structured distribution. The pixel correlation plot in Figure 16 reveals the absence of any visible linear pattern, suggesting a total loss of spatial correlation typically found in natural images, a desirable

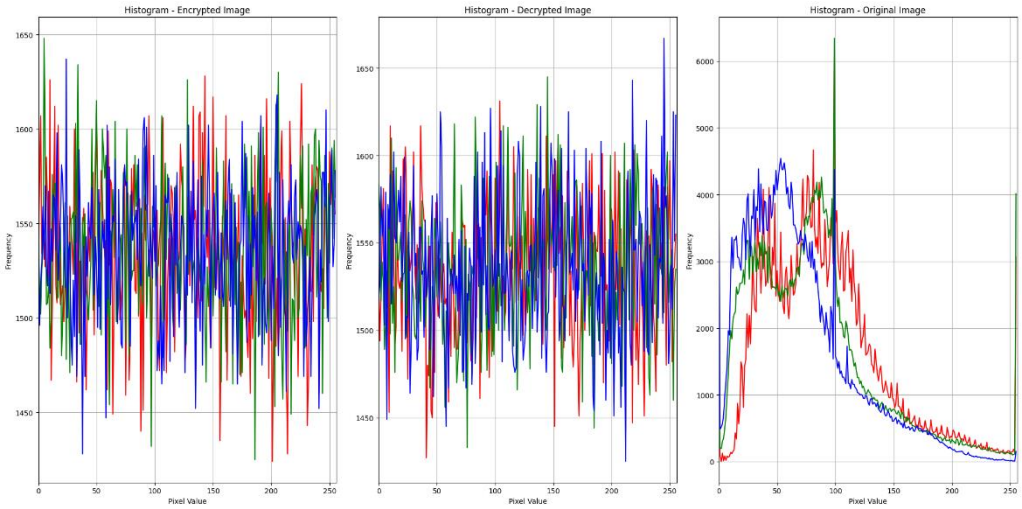
International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

characteristic for encryption robustness. Lastly, the difference map in Figure 17 illustrates the high level of dissimilarity between the decrypted and original images, as indicated by widespread non-zero differences across the image space. Collectively, these results demonstrate that the suggested scheme maintains robust security by ensuring that decryption is only possible with the exact password used during encryption, thereby preventing unauthorized access and maintaining data integrity.



(a) (b) (c)

Fig. 14. Visual Comparison of (a) Encrypted (b) Decrypted and (c) Original images generated using the wrong password.



(a) (b) (c)

Fig. 15. Histogram of (a) Encrypted image (b) Decrypted image and (c) Original image generated using the wrong password.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

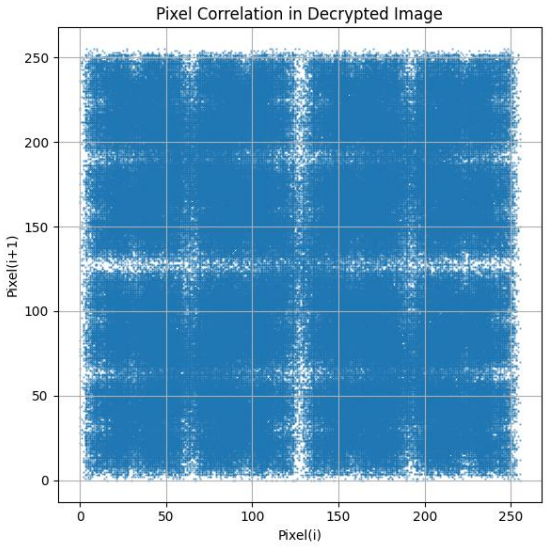


Fig. 16. Pixel correlation in decrypted image generated using the wrong password.

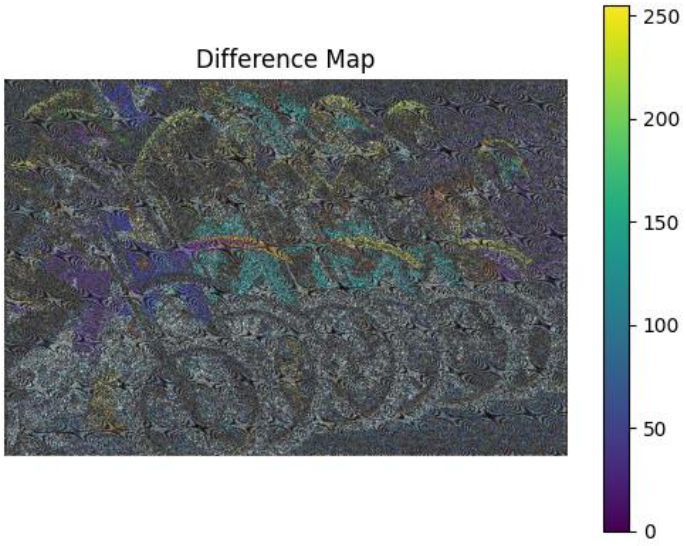


Fig. 17. Difference map generated using the wrong password.

ii. Performance Evaluation

NPCR metric is used to measure the percentage of pixels that differ between the original and encrypted images. It evaluates how effectively the encryption algorithm alters the pixel value in response to small changes. NPCR is defined by the following Equation (18) and $D(i,j)$, which compares the pixel values, is expressed in Equation 19.

$$NPCR: N(C^1, C^2) = \sum_{i,j} \quad \frac{D(i,j)}{T} \times 100\% \tag{18}$$

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 5, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$D(i,j) = \{0, if\ C^1(i,j) = C^2(i,j)\ 1, if\ C^1(i,j) \neq C^2(i,j) \tag{19}$$

where C^1 is the input image, C^2 denotes the cipher image, and T is the total number of pixels. An ideal NPCR value for a secure system should be close to 100%, demonstrating high intensity and excellent resistance to differential attacks. The proposed model consistently obtained NPCR values above 99.6% across all test images.

UACI measures the average intensity difference between the original and encrypted images, which reflects how much the pixel values have been altered overall. UACI is expressed as in Equation (20).

$$UACI: U(C^1, C^2) = \sum_{i,j} \quad \frac{|C^1(i,j) - C^2(i,j)|}{F \cdot T} \times 100\% \tag{20}$$

where C_1(i, j) and C_2(i, j) are the original and encrypted pixel values, H and W are the dimensions of the image. The results of the proposed model yielded UACI values within the desired range, confirming the high disruption of pixels intensity patterns post-encryption.

Entropy measures the degree of randomness or unpredictability in an image. According to Shannon's information theory, the entropy $H(X)$ of an image source X is calculated as in Equation (21).

$$H(P) = -\sum_{i=0}^{255} \quad P(x_i) log_b P(x_i) \tag{21}$$

where $H(P)$denotes the entropy in bits ($b = 2$), $P(x_i)$ is the probability of pixel intensity x_i in the image (usually from 0 to 255 for 8-bit images) and log_b is the logarithm base b, often base 2 in digital image processing.

Table 1 illustrates the evaluation results of the proposed image encryption method using standard metrics such as NPCR, UACI, and entropy for five input images. The NPCR values remain consistently high at around 99.61 to 99.62%, demonstrating effective sensitivity to pixel changes and excellent diffusion properties. The UACI values range from 28.55% to 33.40%, confirming significant alterations in pixel intensities during encryption. Moreover, the entropy values of the encrypted images with values between 7.3894 and 7.8943, reflecting high randomness and resistance to statistical attacks. Compared to the original images, which show lower entropy, the significant increase after encryption highlights the robustness and efficiency of the proposed chaotic logistic map and conic curve-based encryption approach.

Table 1: Evaluation Results of Proposed Image Encryption

Input Image	**NPCR (%)**	**UACI (%)**	**Entropy (Original)**	**Entropy (Encrypted)**

Received: August 02, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

kodim01	99.61	28.55	7.1610	7.8943
kodim02	99.61	33.40	5.5651	7.3894
kodim03	99.61	29.86	7.0919	7.8622
kodim04	99.62	29.97	7.1183	7.8064
kodim05	99.61	32.31	7.3621	7.8718

Table 2 visualizes the results of the decryption process for five test images, confirming the accuracy and integrity of the suggested scheme. The UACI and NPCR values for all decrypted images are 0%, indicating that there are no differences between the original and decrypted images, demonstrating a successful decryption process. This shows that pixel positions and intensities are perfectly restored. Furthermore, the entropy values of the decrypted images exactly match those of the original images, validating that the statistical characteristics of the data are fully preserved. These results demonstrate the proposed model's ability for lossless and efficient image recovery.

Table 2: Evaluation Results of Proposed Image Decryption

Input Image	**NPCR (%)**	**UACI (%)**	**Entropy (Original)**	**Entropy (Decrypted)**
kodim01	0	0	7.1610	7.1610
kodim02	0	0	5.5651	5.5651
kodim03	0	0	7.0919	7.0919
kodim04	0	0	7.1183	7.1183
kodim05	0	0	7.3621	7.3621

Table 3 compares various advanced image encryption techniques based on NPCR and UACI values, which are essential indicators of differential attack resistance and intensity change effectiveness. Methods such as chaos-enhanced hybrid algorithms and hybrid 2D chaotic maps, although effective in certain cases, often face limitations such as low encryption speed and high computational complexity. DNA-based encoding, enhances confusion and diffusion but introduces significant processing overhead, while multiple chaotic systems require careful parameter tuning and are hardware-intensive, reducing scalability on resource-constrained platforms. The proposed method, which combines the Chaotic Logistic Map with Conic Curves, achieves a notable NPCR of 99.61% and the highest UACI of 33.40% among the compared methods. This result highlights the model's superior capability in pixel variation and intensity transformation, confirming its robustness and effectiveness in resisting differential and statistical attacks.

Table 3: Comparison of UACI and NPCR of the Proposed Model with Existing Methods

Authors	**Methodology**	**NPCR (%)**	**UACI (%)**
Husam et al. [22]	Chaos-enhanced hybrid algorithm	99.49	22.00

Received: August 02, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Hameed et al. [26]	Hybrid 2D Chaotic Map	98.87	34.58
Alrubaie et al. [25]	Double-dynamic DNA sequence encryption and chaotic 2D logistic map	99.55	32.81
Zhang et al. [24]	Lifting scheme and chaos	99.60	33.47
Alexan et al. [13]	Multiple-image encryption algorithm	99.62	33.30
Proposed Model		**99.61**	**33.40**

CONCLUSION

This study presented a robust and lightweight image encryption framework that effectively combines the chaotic behavior of the logistic map with the conic curve-based spatial key generation. By introducing sensitivity to initial conditions through chaos and spatial variation through conic transformations, the proposed method ensures high levels of confusion and diffusion in the encryption process. Extensive simulations performed on standard color images demonstrated the model's strength, with NPCR values exceeding 99.61%, UACI values reaching up to 33.40%, and high entropy. These metrics confirm that the encrypted images are highly secure, statistically random, and resistant to differential attacks. Furthermore, the system's reliance on password-derived keys makes it adaptable and user-controlled, enhancing its practical applicability. In future work, this model will be extended to support video frame encryption, medical image security, and real-time embedded systems. Additionally, optimizing the framework using parallel computing or GPU acceleration improves processing speed for large-scale applications. The integration of multiple chaotic maps will further elevate the security level, making the scheme suitable for deployment in military-grade and cloud-based multimedia encryption scenarios.

REFERENCES

1. Mahadik, S. S., Pawar, P. M., Muthalagu, R., Prasad, N. R., Hawkins, S. K., Stripelis, D., ... & Hecht, B. (2024). Digital privacy in healthcare: State-of-the-art and future vision. *IEEE Access*, *12*, 84273-84291.
2. Abdo, A. (2023). *A FRAMEWORK FOR HEALTH INFORMATION SHARING AND PRIVACY PRESERVATION USING INFORMATION HIDING AND DIFFERENTIAL PRIVACY* (Doctoral Dissertation, Haramaya University).

Received: August 02, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3. Choudhary, S., & Husain, S. (2023). Analysis of cryptography encryption for network security and image steganography technique. *algorithms*, *7*(10).
4. Xing, T. (2023, November). Investigation into Essential Technologies and Common Applications of Digital Encryption. In *2023 International Conference on Image, Algorithms and Artificial Intelligence (ICIAAI 2023)* (pp. 756-765). Atlantis Press.
5. Alenezi, M. N., Alabdulrazzaq, H., & Mohammad, N. Q. (2020). Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, *12*(2), 256-272.
6. Meraouche, I., Dutta, S., Tan, H., & Sakurai, K. (2023). Learning asymmetric encryption using adversarial neural networks. *Engineering Applications of Artificial Intelligence*, *123*, 106220.
7. Mohamed, N. N., Yussoff, Y. M., Saleh, M. A., & Hashim, H. (2020). Hybrid cryptographic approach for internet ofhybrid cryptographic approach for internet ofthings applications: A review. *Journal of Information and Communication Technology*, *19*(3), 279-319.
8. Zhang, Q. (2021, January). An overview and analysis of hybrid encryption: the combination of symmetric encryption and asymmetric encryption. In *2021 2nd international conference on computing and data science (CDS)* (pp. 616-622). IEEE.
9. Shaukat, S., Ali, A., Eleyan, A., Shah, S. A., & Ahmad, J. (2020). Chaos theory and its application: an essential framework for image encryption. *Chaos Theory and Applications*, *2*(1), 17-22.
10. Pirdawood, M. A., Kareem, S., & Al-Rassam, O. (2024). Encryption of Color Images with a New Framework: Implementation Using the Elzaki Transformation. *ARO-THE SCIENTIFIC JOURNAL OF KOYA UNIVERSITY*, *12*(1), 170-180.
11. Alexan, W., Elkandoz, M., Mashaly, M., Azab, E., & Aboshousha, A. (2023). Color image encryption through chaos and kaa map. *Ieee Access*, *11*, 11541-11554.
12. He, Q., Li, P., & Wang, Y. (2024). A color image encryption algorithm based on compressive sensing and block-based dna coding. *IEEE Access*, *12*, 77621-77638.
13. Alexan, W., Hosny, K., & Gabr, M. (2025). A new fast multiple color image encryption algorithm. *Cluster Computing*, *28*(5), 1-34.
14. Cao, Y., & Song, Y. (2024). Color Image Encryption Based on an Evolutionary Codebook and Chaotic Systems. *Entropy*, *26*(7), 597.
15. Elmenyawi, M. A., Aziem, N. M. A., & Bahaa-Eldin, A. M. (2024). Efficient and secure color image encryption system with enhanced speed and robustness based on binary tree. *Egyptian Informatics Journal*, *27*, 100487.
16. Es-sabry, M., El Akkad, N., Khrissi, L., Satori, K., El-Shafai, W., Altameem, T., & Rathore, R. S. (2024). An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers. *Egyptian Informatics Journal*, *25*, 100449.

Received: August 02, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

17. Mirzajani, S., Moafimadani, S. S., & Roohi, M. (2024). A new encryption algorithm utilizing dna subsequence operations for color images. *AppliedMath*, *4*(4), 1382-1403.
18. Abed, Q. K., & Al-Jawher, W. A. M. (2024). Optimized color image encryption using arnold transform, URUK chaotic map and GWO algorithm. *Journal Port Science Research*, *7*(3), 219-236.
19. Hosny, K. M., Elnabawy, Y. M., Elshewey, A. M., Alhammad, S. M., Khafaga, D. S., & Salama, R. (2024). New method of colour image encryption using triple chaotic maps. *IET Image Processing*, *18*(12), 3262-3276.
20. Kamal, A., El-Kamchochi, H. A., El-Fahar, A., & Hagras, E. A. (2025). Conic curve encryption and digital signature based on complex number theory for cybersecurity applications. *Scientific Reports*, *15*(1), 21566.
21. Yao, M., Chen, Z., Deng, H., Wu, X., Liu, T., & Cao, C. (2025). A color image compression and encryption algorithm combining compressed sensing, sudoku matrix, and hyperchaotic map. *Nonlinear Dynamics*, *113*(3), 2831-2865.
22. Husam, S., Hoomod, H. K., & Hussein, K. A. (2025). Hybrid Algorithm (DES-Present) for encryption image color using 2D-Chaotic System. *Mustansiriyah Journal of Pure and Applied Sciences*, *3*(1), 49-63.
23. Khudhair, A. A. T., Maolood, A. T., & Gbashi, E. K. (2025). Color Image Encryption Based on a New Symmetric Lightweight Algorithm. *Mesopotamian Journal of CyberSecurity*, *5*(2), 436-452.
24. Zhang, Y. (2020). The fast image encryption algorithm based on lifting scheme and chaos. *Information sciences*, *520*, 177-194.
25. Alrubaie, A. H., Khodher, M. A. A. A., & Abdulameer, A. T. (2023). Image encryption based on 2DNA encoding and chaotic 2D logistic map. *Journal of Engineering and Applied Science*, *70*(1), 60.
26. Hameed, B. A. (2024). New S-Box Generation Based on Hybrid Two-Dimensional Chaotic Map for Color Image Encryption. *International Journal of Intelligent Engineering & Systems*, *17*(6).
27. https://www.kaggle.com/datasets/sherylmehta/kodak-dataset/data
28. Appel, A. W. (2015). Verification of a cryptographic primitive: SHA-256. ACM Transactions on Programming Languages and Systems (TOPLAS), 37(2), 1-31.
29. Moysis, L., Petavratzis, E., Volos, C., Nistazakis, H., & Stouboulos, I. (2020). A chaotic path planning generator based on logistic map and modulo tactics. Robotics and Autonomous Systems, 124, 103377.
30. Yan-Bin, Z., & Qun, D. (2011, December). A new digital chaotic sequence generator based on logistic map. In 2011 Second International Conference on Innovations in Bio-inspired Computing and Applications (pp. 175-178). IEEE.

Received: August 02, 2025