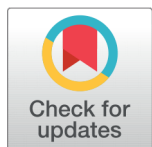


ORIGINAL ARTICLE

 OPEN ACCESS

Received: 04/05/2026

Accepted: 03/09/2026

Published: 24/09/2026

Citation: Singh N, Singh Y, Sangwan S, Singh BK (2026) A Hybrid Encryption Framework Combining Classical and Modern Techniques for Enhanced Image Encryption. Indian Journal of Science and Technology 19(33): 2366-2377. <https://doi.org/10.17485/IJST/v19i33.733>

* **Corresponding author.**yashpalsingh009@gmail.com**Funding:** None**Competing Interests:** None

Copyright: © 2026 Singh et al. This is an open access article distributed under the terms of the [Creative Commons Attribution License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Published By Indian Society for Education and Environment ([iSee](#))

ISSN

Print: 0974-6846

Electronic: 0974-5645

A Hybrid Encryption Framework Combining Classical and Modern Techniques for Enhanced Image Encryption

Naresh Singh¹, Yashpal Singh^{1*}, Sumit Sangwan², Bhupesh Kumar Singh¹¹ ASET, Amity University Rajasthan, India² Faridabad College of Engineering & Management, Faridabad, India

Abstract

Background/Objectives: Digital images exhibit substantial spatial redundancy and strong correlation among neighboring pixels, making effective disruption of spatial and intensity characteristics, an important objective in image encryption. This study proposes a two-layer hybrid image-encryption architecture that integrates Rubik's Cube-based spatial scrambling, AES-128 encryption, and Genetic Algorithm (GA)-based candidate-key selection. **Method:** The proposed architecture first applies Rubik's Cube scrambling controlled by a chaotic logistic map sequence and subsequently performs AES-128 encryption using a candidate key selected via a GA. The GA utilizes a composite fitness function based on Shannon entropy, Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI). The reported configuration uses a population size of 100, a maximum of 200 generations, a crossover rate of 0.8, and a mutation rate of 0.01. The experimental evaluation considers 512×512 benchmark images and ten repeated runs using an Intel Core i7 processor with 16 GB RAM, Python 3.9, PyCrypto, and OpenCV. **Findings:** Across the four evaluated image labels, entropy ranges from 7.995 to 7.998, NPCR from 99.58% to 99.67%, and UACI from 33.28% to 33.89%. In a comparative evaluation, the proposed hybrid method achieves an entropy of 7.998, a correlation coefficient of 0.0015, NPCR of 99.67%, UACI of 33.5%, PSNR of 56.7 dB, and an encryption time of 12.4 ms. **Novelty:** The results indicate favorable outcomes across the assessed image-encryption metrics, suggesting that the integration of spatial scrambling, evolutionary candidate-key selection, and AES-128 forms an effective hybrid framework with a manageable computational cost.

Keywords: Image encryption; Advanced Encryption Standard (AES); Rubik's Cube scrambling; Genetic Algorithm; image security; chaotic map

1 Introduction

Digital images are characterized by significant spatial redundancy and often demonstrate strong correlations between neighboring pixels. These traits provide a solid foundation for developing image-encryption techniques that can effectively disrupt spatial relationships while ensuring a robust cryptographic transformation. The Advanced Encryption Standard (AES) is a widely utilized symmetric block cipher. Additionally, techniques involving spatial permutation and chaos-based methods have been thoroughly explored for image encryption. Furthermore, metaheuristic approaches, such as Genetic Algorithms (GA), Ant Colony Optimization (ACO), the Imperialist Competitive Algorithm (ICA), and Harmony Search, have been investigated for tasks related to key generation, permutation, and optimization.

Hybrid architecture can integrate the complementary features of various approaches. Spatial scrambling can rearrange the organization of image pixels prior to cryptographic transformation, while a standard block cipher offers a robust encryption mechanism. Additionally, evolutionary optimization can be used to select candidate encryption keys based on image-specific objectives.

Driven by these considerations, this study presents a two-layer image-encryption architecture that employs Rubik's Cube scrambling before applying AES-128 encryption. A Genetic Algorithm (GA) is utilized to select a candidate AES key based on a composite objective that incorporates Shannon entropy, NPCR, and UACI. Consequently, the proposed framework effectively combines spatial permutation, evolutionary optimization, and standardized symmetric encryption into a cohesive image-encryption pipeline.

The objective of this study is to evaluate the encryption characteristics of the proposed architecture and compare its performance with selected individual and hybrid approaches. The evaluation considers entropy, adjacent-pixel correlation, NPCR, UACI, PSNR, histogram characteristics, and encryption time.

1.1 Literature Review

Genetic Algorithms have been used to generate and optimize image-encryption keys. Liang et al.⁽¹⁾ integrated a Fibonacci Q-matrix with a GA-based encryption approach. Similarly, Chai et al.⁽²⁾ combined an improved Genetic Algorithm with a matrix semi-tensor product to enhance color image encryption. These studies highlight the application of evolutionary optimization techniques in addressing image-encryption challenges, employing methodologies distinct from the Rubik's Cube and AES-based framework proposed in this research.

Additionally, other evolutionary optimization methods have been explored in the realm of image security. Sreelaja and Vijayalakshmi Pai⁽³⁾ introduced a stream-cipher technique for binary image encryption utilizing Ant Colony Optimization-based key generation. Damghani et al.⁽⁴⁾ employed the Imperialist Competitive Algorithm for JPEG image steganography, while Gholipour⁽⁵⁾ proposed a permutation-diffusion technique for image encryption based on ICA. Moreover, Harmony Search and its variations have been extensively studied in optimization research⁽⁶⁾.

Rubik's Cube methods offer a spatial permutation mechanism for image encryption. Nair et al.⁽⁷⁾ explored color image encryption by applying Rubik's Cube scrambling combined with bitmap shuffling and frame rotation. Zhu et al.⁽⁸⁾ developed a three-dimensional bit-level image-encryption algorithm based on the principles of a Rubik's Cube. Sharmila and Bhuvaneshwaran⁽⁹⁾ integrated Rubik's Cube scrambling with chaos-driven diffusion and circular shifts. Fang et al.⁽¹⁰⁾ employed three-dimensional Rubik's Cube scrambling, along with genetic information diffusion, for encrypting multi-color images. Additionally, Chen et al.⁽¹¹⁾, Fu et al.⁽¹²⁾, and Zhou et al.⁽¹³⁾ further examined hybrid approaches based on Rubik's Cube that incorporate optical chaos, DNA coding, matrix conversion, and multi-image encryption.

Various hybrid image encryption approaches have integrated elements such as chaotic maps, DNA coding, hyperchaotic systems, and quantum-classical mechanisms. Zhu et al.⁽¹⁴⁾ introduced an image encryption scheme that utilizes a newly designed chaotic map in conjunction with parallel DNA coding. Gao⁽¹⁵⁾ explored an image encryption algorithm that employs a two-dimensional hyperchaotic map. Ahmed et al.⁽¹⁶⁾ provided an extensive review of techniques for encrypting medical images. Alawida et al.⁽¹⁷⁾ developed a DNA state-machine-based image encryption method specifically for UAV data, while El-Khamy et al.⁽¹⁸⁾ examined the use of fuzzy-DNA in image encryption and steganography. Additionally, Shafique et al.⁽¹⁹⁾ proposed a quantum-classical hybrid encryption framework to ensure secure transmission of medical images in IoT-based telemedicine networks.

The existing literature demonstrates the extensive use of spatial scrambling, chaotic transformations, evolutionary optimization, and cryptographic mechanisms in image encryption. These studies provide the foundation for investigating integrated architectures that combine complementary mechanisms within a single encryption framework.

1.2 Research Gap

Previous research has highlighted the application of Rubik's Cube scrambling in conjunction with genetic mechanisms, chaos theory, and various hybrid transformations^{(9), (10), (11), (12), (13)}. Therefore, this study does not claim to be the first to combine Rubik's Cube operations with genetic mechanisms and chaos.

Instead, it centers on a specific two-layer architecture that integrates Rubik's Cube spatial scrambling followed by AES-128 encryption, using a genetic algorithm (GA) to select candidates based on a composite objective that includes entropy, NPCR, and UACI.

The proposed architecture unites three complementary mechanisms. Firstly, Rubik's Cube scrambling alters the spatial arrangement of image data. Secondly, the GA selects candidate keys aligned with the established image-encryption objectives. Finally, AES-128 performs the cryptographic transformation. The effectiveness of this architecture is assessed using a comprehensive set of image-encryption metrics and computational evaluations, and compared with selected individual and hybrid approaches.

An overview of how the proposed architecture relates to representative existing methods is presented in Table 1.

Table 1. Positioning of the proposed architecture with respect to representative image-encryption approaches.

Study	Methodology	Relevant distinction from the proposed architecture
Liang et al. ⁽¹⁾	GA + Fibonacci Q-matrix	GA-based image encryption without the Rubik's Cube + AES architecture is evaluated in this study.
Nair et al. ⁽⁷⁾	Rubik's Cube scrambling	Spatial scrambling without the AES-128 layer used in the proposed architecture.
Zhu et al. ⁽⁸⁾	3D Rubik's Cube bit-level encryption	Rubik's Cube-based bit-level design without the proposed GA-based AES key-selection procedure.
Chai et al. ⁽²⁾	Improved GA + matrix STP	GA-based color-image encryption without the Rubik's Cube + AES sequence is considered in this study.
Fang et al. ⁽¹⁰⁾	3D Rubik's Cube + genetic information diffusion	Closely related genetic/Rubik's Cube hybrid; the proposed architecture instead uses AES-128 and an entropy-NPCR-UACI key-selection objective.
Sharmila and Bhu-vaneswaran ⁽⁹⁾	Rubik's Cube + chaos-driven diffusion	Closely related to Rubik's Cube/chaos hybrid, the proposed architecture uses AES-128 as the second encryption layer.
Chen et al. ⁽¹¹⁾	Optical chaos + DNA Rubik's Cube	Chaos/Rubik's Cube hybrid with a different cryptographic construction.
Fu et al. ⁽¹²⁾	3D multi-image Rubik's Cube-Poker model	Rubik's Cube-based multi-image scheme with a different architecture and objective.
Zhou et al. ⁽¹³⁾	Optical chaos + Rubik's Cube matrix conversion	Chaos/Rubik's Cube construction that differs from the AES-based second layer.
Shafique et al. ⁽¹⁹⁾	Quantum-classical hybrid	Different cryptographic architecture and application context.

1.3 Contribution of This Study

The primary contributions of this study are outlined as follows:

- This study proposed a two-layer hybrid image encryption architecture that combines Rubik's Cube-based spatial scrambling with AES-128 encryption.
- An evolutionary algorithm (GA)-based candidate key selection mechanism has been integrated to enhance the optimization of AES key selection. This mechanism employs a composite fitness function that incorporates Shannon entropy, NPCR, and UACI.
- The proposed framework merges spatial permutation, evolutionary optimization, and standardized symmetric encryption into a cohesive image encryption pipeline.
- The architecture's performance is assessed using various metrics, including entropy, adjacent-pixel correlation, NPCR, UACI, PSNR, histogram characteristics, and encryption time.
- A comparative analysis has been conducted against AES-only, Rubik's Cube-only, GA-only, ICA, and DHS approaches.

2 Methodology

2.1 Overall Architecture

The proposed encryption architecture comprises several key components: input preprocessing, spatial scrambling based on Rubik's Cube transformations, AES-128 encryption, and decryption via the corresponding inverse operations. A GA is integrated into the AES stage to select candidate encryption keys based on a defined image-encryption fitness function.

Figure 1 illustrates the complete workflow for encryption and decryption. The first layer performs spatial scrambling using Rubik's Cube transformations, which are governed by a logistic map sequence. The second layer applies AES-128 encryption using the candidate key selected by the GA.

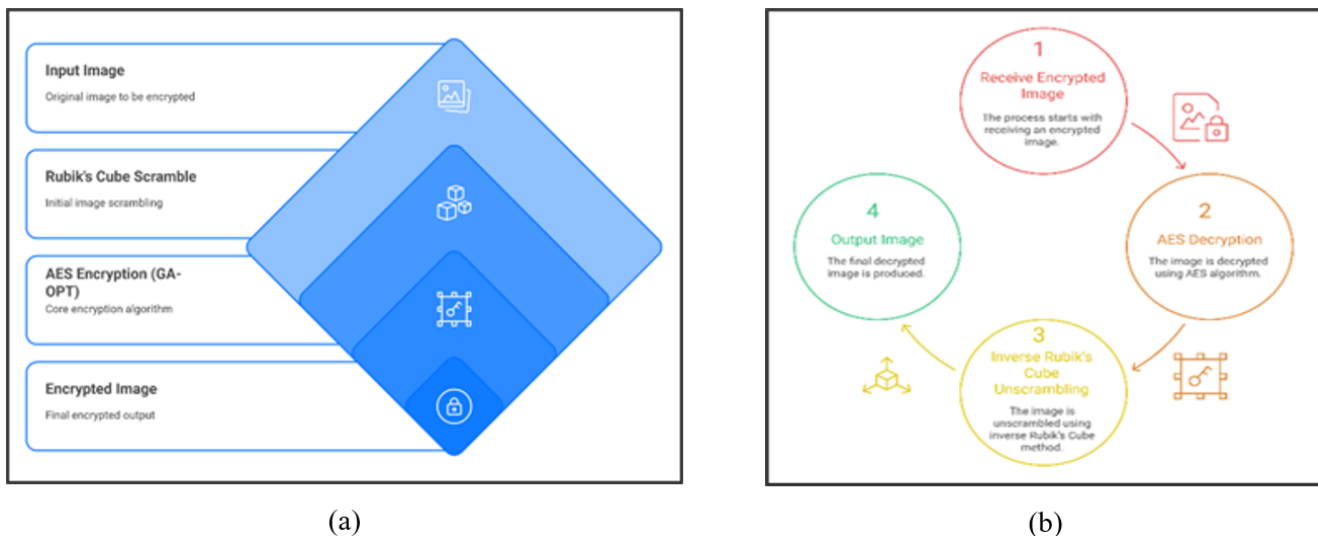


Fig 1. Proposed Method Flowgraph: (a) For Encryption technique. (b) For the decryption technique.

The proposed architecture, therefore, combines spatial transformation and cryptographic transformation in two successive layers.

2.2 Dataset and Experimental Setup

The quantitative evaluation examines four image categories: Iris flower, Baboon, Cameraman, and Peppers. The experimental setup utilizes benchmark images with a resolution of 512×512 pixels. The testing environment features an Intel Core i7 processor equipped with 16 GB of RAM. The implementation is written in Python 3.9, using PyCrypto for AES and OpenCV for image processing. Each experiment is conducted 10 times, and the reported results reflect the average values obtained.

The evaluation includes measures such as entropy, adjacent-pixel correlation, NPCR, UACI, PSNR, histogram characteristics, and encryption time.

2.3 Preprocessing

The input image ($I(x, y)$) is represented using 8-bit intensity values in the range $[0, 255]$. In this methodology, non-overlapping image blocks are utilized for the subsequent Rubik's Cube scrambling process.

Each image block corresponds to a virtual three-dimensional cube structure. The spatial arrangement of these blocks is then altered through operations inspired by the Rubik's Cube, guided by a generated scrambling sequence.

2.4 Rubik's Cube-Based Spatial Scrambling

Each image block is linked to a virtual three-dimensional cube structure. The rotation sequence controlling these blocks is derived from the logistic map, as given in Eq. (1):

$$x_{n+1} = r \cdot x_n (1 - x_n), \quad r \in (3.57, 4.0) \quad (1)$$

where x_n denotes the current state of the sequence and r represents the control parameter.

The logistic-map sequence is used to control the Rubik's Cube transformations applied to the image blocks. The resulting behavior of the logistic map sequence is illustrated in Figure 2.

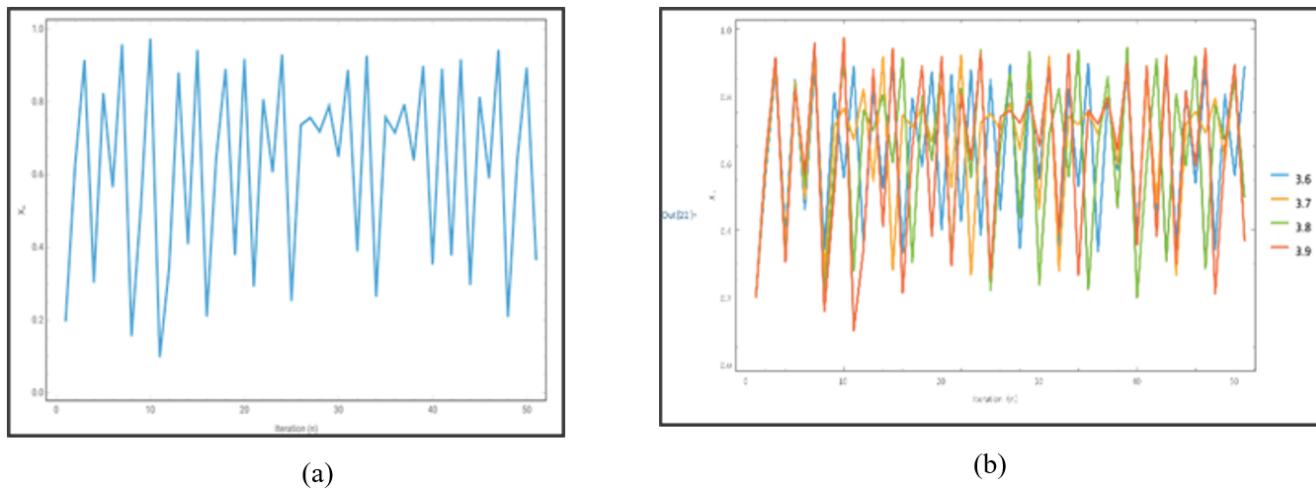


Fig 2. Dynamics of Chaotic Logistic Map: (a) Sequence evolution showing non-periodic behavior for $r = 3.9$. (b) Sensitivity of the logistic map for various control parameters $r \in (3.57, 4.0)$.

The objective of this stage is to modify the image's spatial organization and reduce local pixel correlations before the AES stage. The Rubik's Cube transformation, therefore, serves as the spatial permutation layer of the proposed architecture.

2.5 AES-128 Encryption and GA-Based Candidate-Key Selection

AES-128 is used as the cryptographic component of the proposed architecture. AES operates on 128-bit blocks using a 128-bit key⁽²⁰⁾.

The GA represents candidate 128-bit AES keys as chromosomes. The reported genetic operators include roulette-wheel selection, single-point crossover, and bit-flip mutation. The configuration uses a population size of 100, a maximum of 200 generations, a crossover rate of 0.8, and a mutation rate of 0.01.

The fitness function is defined in Eq. (2)

$$F = w_1 H + w_2 NPCR + w_3 UACI \quad (2)$$

where H is Shannon entropy measures the randomness of the key, $NPCR$ is the Number of Pixels Change Rate quantifies the variation in pixel values post-encryption, and $UACI$ is the Unified Average Changing Intensity assesses the overall intensity change.

This composite objective merges the three image encryption metrics into a single fitness function. The GA evaluates the candidate keys and selects the one with the highest fitness value. Subsequently, the chosen AES key is used to encrypt the scrambled image. Thus, the GA introduces an evolutionary mechanism for selecting candidate keys within the proposed two-layer architecture. Figure 3 shows how the weighting coefficients affect the fitness function, the optimization landscape, and the relative contribution of each security metric.

2.6 Decryption

The decryption process operates as the inverse of the encryption pipeline. Initially, the encrypted data undergoes the inverse AES operation using the designated key. The resulting data is then processed through the inverse Rubik's Cube transformations, following the corresponding scrambling sequence. This comprehensive reverse transformation reconstructs the decrypted image from the encrypted representation.

2.7 Experimental Protocol and Baselines

The quantitative comparison considers five baseline approaches:

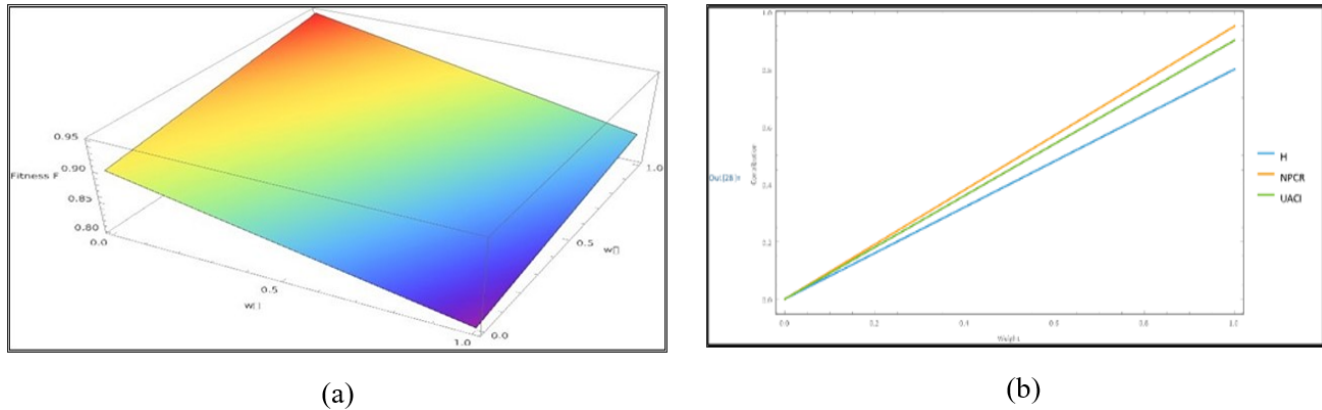


Fig 3. Visualization of fitness function (a) Three-dimensional surface plot showing variation of fitness values with respect to weighting coefficients w_1 and w_2 . (b) Sensitivity analysis of individual security metrics demonstrating the relative contribution of entropy, NPCR, and UACI to the overall fitness value.

- AES only
- Rubik's Cube only
- GA only
- ICA
- DHS

The proposed architecture and baseline approaches are evaluated using the reported image-encryption metrics and computational measurements.

2.8 Evaluation Metrics

- **Shannon Entropy:** It measures the uncertainty associated with the pixel-value distribution and is calculated using Eq. (3):

$$H(x_i) = -\sum_{i=0}^{255} P(x_i) \log_2 P(x_i) \quad (3)$$

where $P(x_i)$ represents the probability of the occurrence of an intensity value x_i .

For an 8-bit image, the theoretical maximum entropy is 8. Therefore, an entropy value close to 8 corresponds to a highly dispersed intensity distribution.

- **Adjacent Pixel Correlation:** It measures the relationship between neighboring pixels. A correlation coefficient close to zero indicates weak linear dependence between adjacent pixels. It is calculated using Eq. (4):

$$r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)D(y)}} \quad (4)$$

- **Number of Pixels Change Rate:** It measures the percentage of pixels that change between two encrypted images corresponding to a small modification in the input. It is calculated using Eq. (5).

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100 \quad (5)$$

where $D(i,j) = 1$ when the corresponding pixel values differ and $D(i,j) = 0$ otherwise.

- **Unified Average Changing Intensity:** It measures the average intensity difference between two encrypted images. It is calculated according to Eq. (6):

$$UACI = \frac{1}{W \times H} \sum_{i=1}^W \sum_{j=1}^H \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \quad (6)$$

where $W \times H$ are the width and height dimensions of the image. $C_1(i,j)$ and $C_2(i,j)$ are the intensity values of the pixel at coordinates (i,j) for the first and second encrypted images.

- **Peak Signal-to-Noise Ratio:** PSNR is used to characterize the reconstruction quality between the original and decrypted images. It is calculated using Eq. (7):

$$PSNR = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right) \quad (7)$$

where MAX_I^2 denotes the maximum possible pixel intensity, and MSE represents the mean squared error between the original and decrypted images.

- **Histogram Analysis:** Histograms are used to compare the intensity distributions of the original and encrypted images.
- **Encryption Time:** Encryption time is used to evaluate the computational performance of the proposed architecture and the considered comparison methods.

3 Result and Discussion

3.1 Visual Encryption Results

The visual transformation generated by the initial encryption layer is illustrated in Figure 4. This figure contrasts the original Iris flower image with its corresponding representation scrambled like a Rubik's Cube. The scrambling operation alters the spatial arrangement of the image while retaining the essential information needed for further encryption.

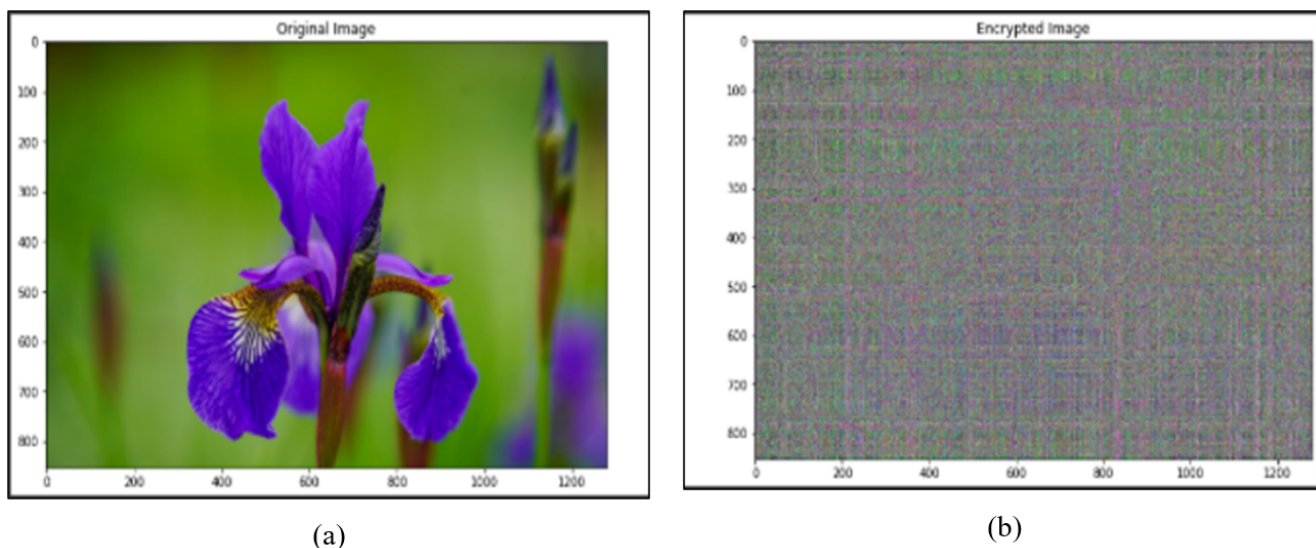


Fig 4. Visual demonstration of the proposed hybrid encryption: (a) Original Image. (b) Scrambled Using Rubik's Cube.

The AES-based encryption and decryption outputs are shown in Figure 5. The encrypted image exhibits a substantially different visual structure from the original, while the corresponding decrypted image demonstrates the reverse transformation.

The visual results demonstrate the complementary roles of the two layers. Rubik's Cube scrambling modifies the spatial organization of the input image, while AES-128 performs the subsequent cryptographic transformation.

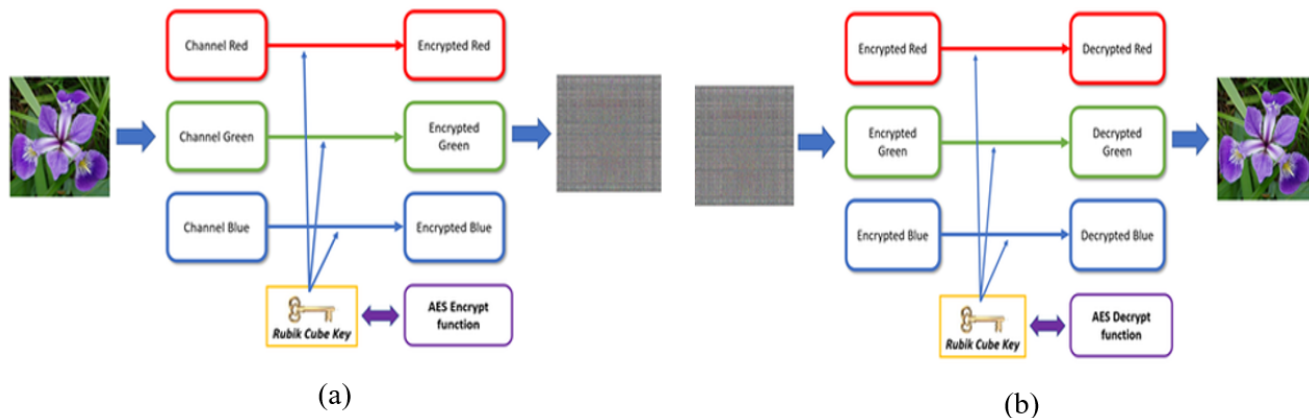


Fig 5. Encryption and Decryption Results: (a) Encrypted image using AES + GA. (b) Decrypted output.

3.2 Histogram Analysis

The histogram distributions of the original and encrypted images are compared in Figure 6.

The encrypted histogram exhibits a substantially altered distribution compared with the original image. The redistribution of pixel intensities reduces the visible intensity structure of the source image and supports the quantitative entropy and correlation results.

3.3 Quantitative Results for the Proposed Hybrid

The quantitative results obtained for the proposed hybrid architecture across the evaluated images are presented in Table 2.

Table 2. Quantitative performance of the proposed hybrid architecture

Image	Entropy	Correlation Coefficient	NPCR (%)	UACI (%)	PSNR (dB)
Iris flower	7.997	0.0012	99.61	33.42	56.71
Baboon	7.995	0.0025	99.58	33.89	54.92
Cameraman	7.996	0.0015	99.67	33.51	57.11
Peppers	7.998	Not reported	99.62	33.28	55.48

The proposed hybrid architecture delivers favorable results across the evaluated image-encryption metrics. Entropy values range from 7.995 to 7.998, indicating intensity distributions that approach the theoretical maximum for an 8-bit image. The reported adjacent-pixel correlation coefficients are close to zero, with values of 0.0012, 0.0025, and 0.0015 for the analyzed images, suggesting weak local pixel dependence within the encrypted images.

NPCR values range from 99.58% to 99.67%, with the highest, 99.67%, achieved for the Cameraman image. UACI values span from 33.28% to 33.89%, reflecting significant variation in intensity across the corresponding encrypted images.

The reported PSNR values range from 54.92 dB to 57.11 dB, indicating favorable characteristics for reconstructing the evaluated images. Overall, the consistency of these measured values across the four evaluated image labels demonstrates the effectiveness of the proposed architecture across diverse image content.

3.4 Comparative Evaluation

A comparative evaluation of the proposed architecture against AES-only, Rubik's Cube-only, GA-only, ICA, and DHS approaches is presented in Table 3.

The proposed hybrid architecture achieves the highest reported entropy among the evaluated approaches. Additionally, the correlation coefficient is the lowest among the reported values, indicating a weak dependence on adjacent pixels. The method also achieves an NPCR that surpasses the values reported for the comparison methods. Its UACI value is greater than those of AES-only, Rubik's Cube-only, GA-only, and DHS methods, and is comparable to the results from the ICA approach.

Furthermore, this architecture achieves the highest reported PSNR among the listed methods. These outcomes reflect enhanced performance across several image-encryption metrics when compared to the approaches considered.

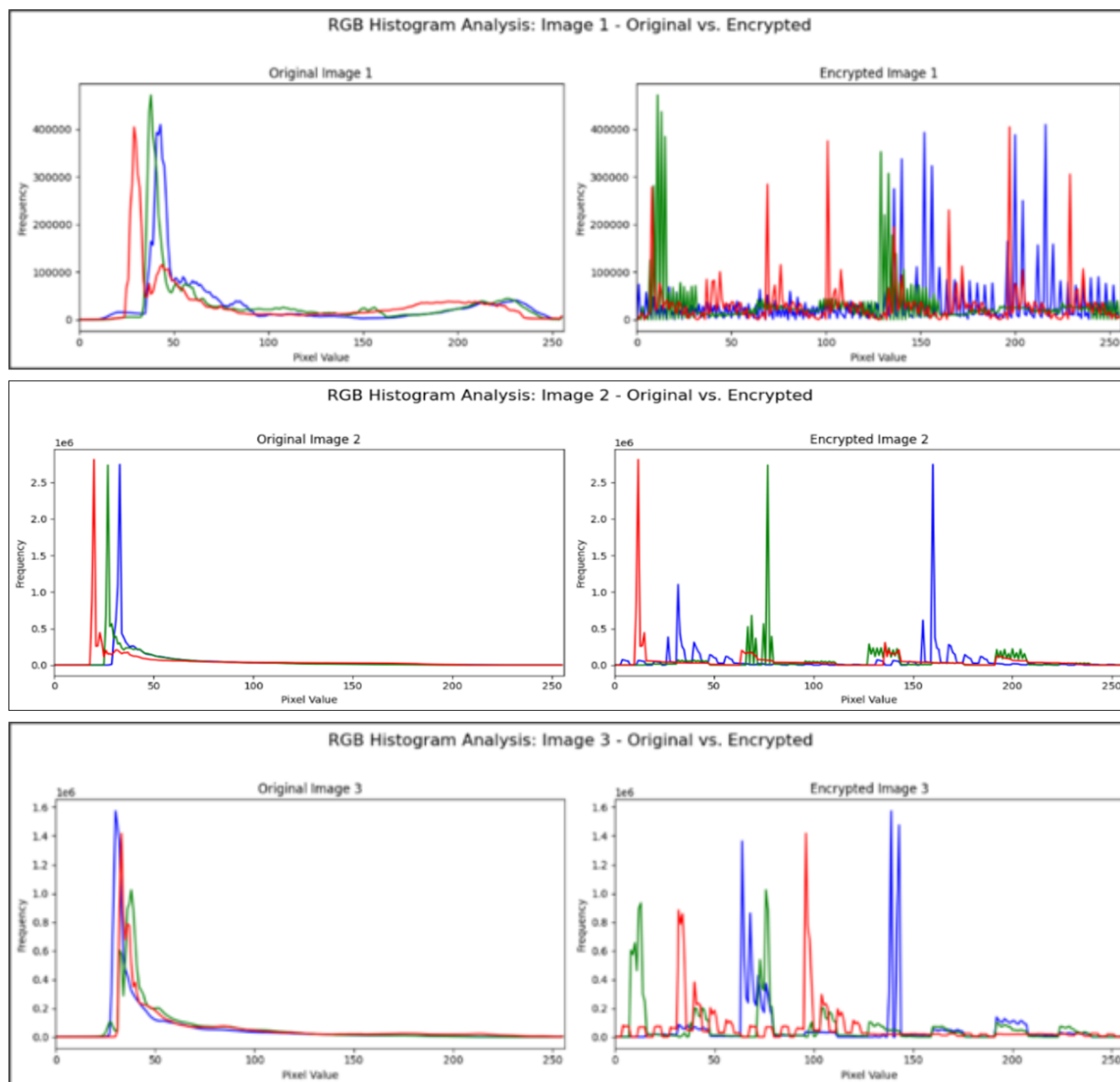


Fig 6. Histogram comparison between original and encrypted images (grayscale).

Table 3. Comparative performance of the proposed hybrid architecture and baseline methods

Algorithm	Entropy	Correlation	NPCR (%)	UACI (%)	PSNR (dB)	Time (ms)
AES-only	7.85	0.012	99.3	32.1	54.5	8.7
Rubik's Cube-only	7.72	0.028	99.5	33.0	55.2	6.5
GA-only	7.85	0.015	99.3	32.8	53.8	18.2
ICA	7.92	0.014	99.5	33.4	42.0	14.5
DHS	7.74	0.018	99.1	32.5	50.1	20 – 30
Proposed Hybrid	7.998	0.0015	99.67	33.5	56.7	12.4

The comparative results highlight the benefits of combining the three principal components. Rubik's Cube scrambling alters the spatial organization of the image, GA-based candidate-key selection optimizes the defined image-encryption objective, and AES-128 provides a standardized cryptographic transformation.

3.5 Computational Performance

The proposed method requires 12.4 ms for encryption according to the comparative evaluation. In contrast, the Rubik's Cube-only and AES-only approaches take 6.5 ms and 8.7 ms, respectively. The GA-only and ICA methods require 18.2 ms and 14.5 ms, respectively, whereas DHS is reported to take 20-30 ms.

Consequently, the proposed method exhibits an intermediate computational cost compared with the approaches considered. Its encryption time is longer than that of both the AES-only and Rubik's Cube-only methods because it incorporates multiple processing stages. However, this additional computational expense is justified by the improved values observed for entropy, correlation, NPCR, UACI, and PSNR in the comparative evaluation. The results indicate a favorable trade-off between the assessed image-encryption characteristics and computational cost.

3.6 Comparison with Published Studies

The performance of the proposed architecture was compared with several notable published studies on image encryption. Liang et al.⁽¹⁾ reported an entropy of approximately 7.85 and an NPCR of around 99.3% for their method utilizing GA and a Fibonacci Q-matrix. Nair et al.⁽⁷⁾ achieved an entropy of approximately 7.96 and a UACI of about 33.0% with their Rubik's Cube-based approach. Zhu et al.⁽⁸⁾ recorded an entropy of around 7.99 using their three-dimensional bit-level Rubik's Cube method. Chai et al.⁽²⁾ reported an entropy of approximately 7.99 and an NPCR exceeding 99.6% for their GA-STP color-image method.

In contrast, the proposed architecture achieves an entropy of 7.998 and an NPCR of 99.67%, indicating better performance than these established results. Shafique et al.⁽¹⁹⁾ reported a processing time of approximately 15 ms for their quantum-classical medical image encryption framework. The proposed architecture reports a timing result of 12.4 ms, which is lower than the reported value, despite the two approaches utilizing different architectures and application contexts.

These comparisons provide contextual evidence of the proposed architecture's measurable performance and highlight the effectiveness of integrating Rubik's Cube scrambling, GA-based candidate key selection, and AES-128.

3.7 Discussion

The measured results can be interpreted through the complementary functions of the three principal components of the proposed architecture.

Rubik's Cube scrambling acts as a spatial permutation mechanism, altering the arrangement of neighboring pixels prior to AES processing. This transformation contributes to the low correlation values observed between adjacent pixels in the encrypted images.

The Genetic Algorithm (GA) offers an evolutionary search mechanism for selecting candidate AES keys. By incorporating metrics such as entropy, NPCR, and UACI into the fitness function, this process evaluates multiple image-encryption metrics during optimization, thereby enhancing candidate key selection.

AES-128 delivers the cryptographic transformation in the second layer. The sequential application of spatial scrambling, candidate-key optimization, and AES encryption yields a combination with high entropy, low correlation, high NPCR, and favorable UACI values.

Comparative evaluations further demonstrate improved metrics across several assessed aspects when compared to individual approaches. Thus, the findings support the effectiveness of integrating spatial scrambling and evolutionary candidate-key selection with AES-128 for image encryption applications.

The reported metrics provide insight into the empirical encryption performance of the proposed architecture and should be interpreted as measures of image-encryption behavior rather than results of inferential statistical testing.

4 Future Direction

The proposed architecture presents several avenues for further exploration. Future research could involve assessing the framework with larger image collections and incorporating a variety of image types, including color images and application-specific datasets.

Additionally, the GA component can be enhanced through adaptive population strategies, alternative evolutionary operators, and multi-objective optimization formulations. These enhancements may reveal opportunities for improving the balance among entropy, correlation, NPCR, UACI, and computational cost.

Further experiments could also investigate additional cryptanalytic and robustness-oriented characteristics to provide a more comprehensive characterization of the proposed architecture. This could include analyses such as key sensitivity, chosen plaintext, known plaintext, local entropy, directional correlation, randomness testing, and robustness against noise and image modifications.

Moreover, the computational efficiency of the framework can be significantly improved through parallel processing and GPU acceleration, which would be particularly beneficial for real-time image encryption applications and large-scale image processing environments.

5 Conclusion

This study presents a two-layer hybrid image-encryption architecture that integrates spatial scrambling based on the Rubik's Cube, candidate-key selection through Genetic Algorithms, and AES-128 encryption. This architecture effectively combines spatial permutation, evolutionary optimization, and standardized symmetric encryption within a cohesive framework for image encryption.

Quantitative results indicate strong performance across the evaluated image-encryption metrics. The entropy values range from 7.995 to 7.998, the NPCR values range from 99.58% to 99.67%, and the UACI values fall between 33.28% and 33.89%. The adjacent-pixel correlation coefficients are close to zero, suggesting minimal local pixel dependence on the encrypted images.

In comparative evaluations, the proposed hybrid method achieves an entropy of 7.998, a correlation coefficient of 0.0015, an NPCR of 99.67%, a UACI of 33.5%, and a PSNR of 56.7 dB. These metrics reflect notable improvements over several individual and hybrid approaches previously analyzed. Furthermore, the encryption time of 12.4 ms indicates that the proposed architecture attains these characteristics with a reasonable computational cost.

Overall, the results underscore the efficacy of integrating Rubik's Cube spatial scrambling, Genetic Algorithm-based candidate-key selection, and AES-128 encryption for hybrid image-encryption applications. This architecture provides a framework for integrating spatial transformation and evolutionary optimization with standardized symmetric cryptography, laying the groundwork for further developments in efficient image security solutions.

6 Acknowledgements

The authors declare that no funding or grants were received for this experimental research work.

Author details: Naresh Singh is a Research Scholar; Dr. Yashpal Singh and Dr. Sumit Sangwan are Associate Professors; Dr. Bhupesh Kumar Singh is a Professor.

References

- 1) Liang Z, Qin Q, Zhou C. An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm. *Neural Computing & Applications*. 2022;34:19313–19341. <https://doi.org/10.1007/s00521-022-07493-x>.
- 2) Chai X, Zhi X, Gan Z, Zhang Y, Chen Y, Fu J. Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption. *Signal Processing*. 2021;183:108041. <https://doi.org/10.1016/j.sigpro.2021.108041>.
- 3) Sreelaja NK, Pai GAV. Stream cipher for binary image encryption using Ant Colony Optimization based key generation. *Applied Soft Computing*. 2012;12:2879–2895. <https://doi.org/10.1016/j.asoc.2012.04.002>.
- 4) Damghani H, Mofrad FB, Damghani L. Medical JPEG image steganography method according to the distortion reduction criterion based on an imperialist competitive algorithm. *IET Image Processing*. 2021;15:705–714. <https://doi.org/10.1049/ipr2.12055>.
- 5) Golalipour K. A novel permutation-diffusion technique for image encryption based on the Imperialist Competitive Algorithm. *Multimedia Tools and Applications*. 2023;82:725–746. <https://doi.org/10.1007/s11042-022-12883-3>.
- 6) Qin F, Zain AM, Zhou KQ. Harmony search algorithm and related variants: A systematic review. *Swarm and Evolutionary Computation*. 2022;74:101126. <https://doi.org/10.1016/j.swevo.2022.101126>.
- 7) Nair A, Dalal D, Mangrulkar R. Colour image encryption algorithm using Rubik's cube scrambling with bitmap shuffling and frame rotation. *Cyber Security and Applications*. 2024;2:100030. <https://doi.org/10.1016/j.csa.2023.100030>.
- 8) Zhu H, Dai L, Liu Y, Wu L. A three-dimensional bit-level image encryption algorithm with Rubik's cube method. *Mathematics and Computers in Simulation*. 2021;185:754–770. <https://doi.org/10.1016/j.matcom.2021.02.009>.
- 9) Sharmila S, Bhuvaneshwaran RS, Vaithiyanathan D. Secure image encryption using Rubik's Cube-based scrambling with chaos-driven diffusion and circular shifts. *Optik*. 2025;339:172533. <https://doi.org/10.1016/j.ijleo.2025.172533>.
- 10) Fang J, Guo N, Liang S, Xiang Y. Application of three-dimensional Rubik's cube scrambling and genetic information diffusion in multiple-color image encryption. *Journal of Supercomputing*. 2025;81:982. <https://doi.org/10.1007/s11227-025-07363-y>.

- 11) Chen WH, Zhou XF, Zheng N, Li MJ, Hu M. Image encryption scheme based on optical chaos and DNA Rubik's cube algorithm. *Physica Scripta*. 2023;98:115507. <https://doi.org/10.1088/1402-4896/acfe48>.
- 12) Fu R, Li C, Zhuang J. Robust 3D Multi-Image Encryption Scheme Based on Rubik's Cube-Poker Model. *Symmetry*. 2025;17:816. <https://doi.org/10.3390/sym17060816>.
- 13) Zhou X, Sun L, Zheng N, Chen W. Image encryption algorithm based on optical chaos and Rubik's cube matrix conversion. *AIP Advances*. 2024;14:085101. <https://doi.org/10.1063/5.0199028>.
- 14) Zhu S, Deng X, Zhang W, Zhu C. Image Encryption Scheme Based on Newly Designed Chaotic Map and Parallel DNA Coding. *Mathematics*. 2023;11:231. <https://doi.org/10.3390/math11010231>.
- 15) Gao X. Image encryption algorithm based on 2D hyperchaotic map. *Optics & Laser Technology*. 2021;142:107252. <https://doi.org/10.1016/j.optlastec.2021.107252>.
- 16) Ahmed ST, Hammood DA, Chisab RF, Al-Naji A, Chahl J. Medical Image Encryption: A Comprehensive Review. *Computers*. 2023;12:160. <https://doi.org/10.3390/computers12080160>.
- 17) Alawida M, Teh JS, Alshoura WH. A New Image Encryption Algorithm Based on DNA State Machine for UAV Data Encryption. *Drones*. 2023;7:38. <https://doi.org/10.3390/drones7010038>.
- 18) El-Khamy SE, Korany NO, Mohamed AG. A New Fuzzy-DNA Image Encryption and Steganography Technique. *IEEE Access*. 2020;8:148935–148951. <https://doi.org/10.1109/ACCESS.2020.3015687>.
- 19) Shafique A, Naqvi SAA, Raza A, Ghalaii M, Papanastasiou P, McCann J, et al. A hybrid encryption framework leveraging quantum and classical cryptography for secure transmission of medical images in IoT-based telemedicine networks. *Scientific Reports*. 2024;14:31054. <https://doi.org/10.1038/s41598-024-82256-3>.
- 20) of Standards NI, (US) T. Advanced Encryption Standard (AES). Washington, D.C.. National Institute of Standards and Technology (U.S.). 2023. <https://doi.org/10.6028/NIST.FIPS.197-upd1>.