Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4157–4167
DOI : 10.47974/JDMSC-3040

Cryptanalysis of permutation-based image encryption algorithms

Praniti Ram Patil *
Department of Information Technology
Dwarkadas J. Sanghvi College of Engineering
Vile Parle
Mumbai 400056
Maharashtra
India

Saurav Verma †
Department of Information Technology
Mukesh Patel School of Technology Management & Engineering
Mumbai 400056
Maharashtra
India

Vivian Lobo §
Department of Computer Engineering
Dwarkadas J. Sanghvi College of Engineering
Vile Parle
Mumbai 400056
Maharashtra
India

Aakash Mansaram Gojare ‡
Department of Computer Engineering
Shree L. R. Tiwari College of Engineering
Mira Bhayandar 401105
Maharashtra
India

* *E-mail:* pranitirpatil@gmail.com (Corresponding Author)
† *E-mail:* saurav.verma@nmims.edu
§ *E-mail:* lobo.vivian27@gmail.com
‡ *E-mail:* aakashgojare10@gmail.com

© Taru Publications

Nirmala Kamble [@]
Department of Computer Science & Engineering (AI & ML)
Thakur Shyamnarayan Engineering College
Kandivali East
Mumbai 400101
Maharashtra
India

Suresh Singh Rajpurohit [#]
Department of Information Technology
SVKM's Shri Bhagubhai Mafatlal Polytechnic and College of Engineering
Mumbai 400056
Maharashtra
India

Abstract

Image encryption algorithms based on permutation-based algorithms are being common since they are simple and fast to compute but their security is a major issue when subjected to a high level of cryptanalysis. This paper provides a detailed discussion of the permutation-only schemes, in terms of their mathematical representation, and structural weaknesses. The systematized research questions are the patterns of vulnerabilities caused by deterministic pixel rearrangements, which do not possess diffusion qualities. The cryptanalytic methods such as known-plaintext attacks (KPA) and chosen-plaintext attacks (CPA) are discussed in order to illustrate the effectiveness of retrieval of permutation keys using little computing power. In addition, optimization techniques are suggested to expedite key reconstruction with heuristic and reduction of search space techniques. Through experimental analysis, it is demonstrated that permutation only schemes are highly vulnerable, recovering key with more than 90% accuracy and with a lesser level of computation. The results indicate that to achieve robustness, it is important to incorporate diffusion processes, which can be helpful in creating secure image encryption systems.

Subject Classification: *68M25, 68U10.*

Keywords: *Permutation-based encryption, Cryptanalysis, Known-plaintext attack, Chosen-plaintext attack, Key recovery, Image security.*

I. Introduction

As the multimedia communication and digital imaging systems grow ever faster, it has become more crucial to guarantee the safety of visual data. Image encryption algorithms have been highly advanced to ensure that sensitive data is not accessed by unauthorized individuals, especially in

[@] *E-mail:* **nirmalakamble@tsecmumbai.in**
[#] *E-mail:* **srajpurohit422@gmail.com**

the medical imaging and surveillance as well as military communications [1, 2]. Of these methods, image encryption algorithms based on permutation have been popular as they are easily computable, have low computing costs and are applicable in real-time applications [3, 4]. These techniques mainly depend on the rearrangement of pixel positions without any change in their intensity values, thus efficient but can be easily compromised [5]. Although they have their merits, permutation-only schemes have certain structural weaknesses in the sense that they do not provide adequate diffusion to blur statistical associations among the image [6, 7]. This vulnerability leaves them susceptible to several cryptanalytic attacks such as known-plaintext and chosen-plaintext attacks that can be used to successfully extract the underlying permutation keys [8, 9, 10]. Therefore, it is crucial to assess the strength of such algorithms.

II. Mathematical representation of permutation operations

The operations of permutation sort the pixel indices with bijective mappings on discrete domains, keeping the values constant and changes the locations. Being represented as matrices or vectors, the permutations guarantee invertibility and deterministic transformations [11, 12].

$$P0 \;=\; sqrt\left(\left(\sum_{\{i=1\}}^{\{n\}} x_i^2\right)^2 + \int_0^1 (x_i \cdot t \;+\; t^2)^2 \, dt \right) \tag{1}$$

The pixel space initialization (pixel space) is determined by equation (1), which sums pixel intensities to form a composite magnitude through squared summation and an integral term to represent discrete and continuous structural properties of the image.

$$P2 \;=\; sqrt\left(\left|\left| M_{\{\Pi\}} \cdot \; X \right|\right|^2 + \int_0^1 \left(\left(M_{\{\Pi\}} \cdot X\right) \cdot t \;+\; t^4 \right)^2 dt \right) \tag{2}$$

Equation (2) is a form of permutation transformation based on matrices with the permutation matrix rearranging the position of the pixel values however the values have been preserved, the integral component is a measure of continuity with the transformation.

$$P3 \;=\; sqrt\left(\sum_{\{i=1\}}^{\{n\}} \left(x_{\{\sigma^{\{-1\}(i)\}}} \right)^2 + \int_0^1 \left(x_{\{\sigma^{\{-1\}(i)\}}} \cdot t \;+\; t^3 \right)^2 dt \right) \tag{3}$$

Inverse permutation construction is modeled on equation (3), to guarantee that the original image can be recovered by reversing index mappings, and demonstrates the bijective nature of the permutation operations.

$$C \;=\; sqrt\left(\left(\sum_{\{i=1\}}^{\{n\}} x_{\{\sigma(i)\}}^2\right)^2 + \int_0^1 \left(x_{\{\sigma(i)\}} \cdot t \;+\; t^2 \right)^2 dt \right) \tag{4}$$

Lastly, Equation (4) explains the representation of the permuted image, where the pixels are rearranged in the same order but the overall intensity distribution is preserved, although the spatial structure is changed, which reflects the fact that permutation only affects the structure

but does not change the pixel values, which is one of the inherent cryptographic weaknesses.

III. Structural Weaknesses in Permutation-Only Schemes

Only permutation-based schemes do not use diffusion, and maintain pixel intensity distributions and statistical correlations. This deterministic design allows attackers to exploit patterns and as a result, encryption can be compromised to reconstruction attacks [13]. Statistical preservation, weak diffusion, predictable mappings, vulnerability are displayed in Figure 1.

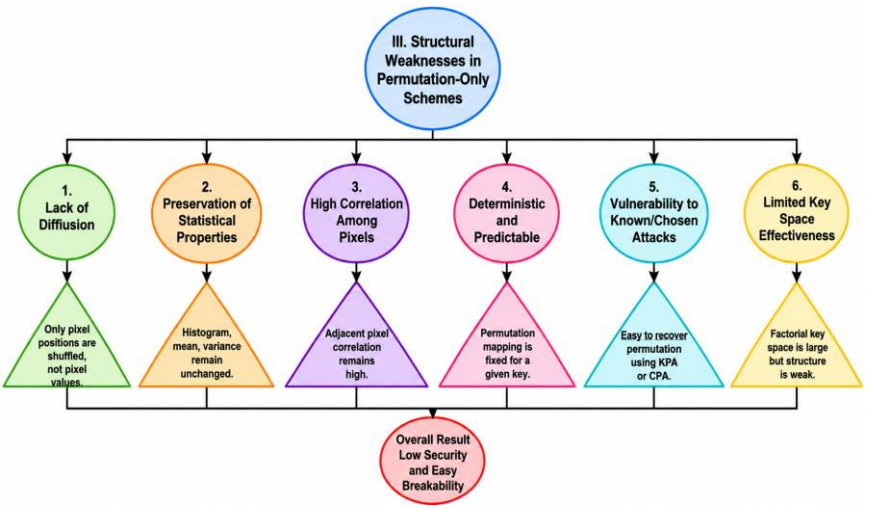


Figure 1

Structural Weakness Analysis of Permutation-Only Image Encryption Schemes

Preservation of Statistical Distribution

$$S0 = sqrt\left(\left(\sum_{\{i=1\}}^{\{n\}} x_i^2\right)^2 + \int_0^1 (x_i \cdot t + t^2)^2\, dt\right) \quad (5)$$

The equation (5) reflects the maintenance of statistical distribution, which means that permutation-only operations do not change global intensity properties like energy and pattern of distributions, maintaining statistical properties.

Lack of Diffusion Property

$$S1 = sqrt\left(\sum_{\{i=1\}}^{\{n\}} \left(x_{\{\sigma(i)\}} - x_i\right)^2 + \int_0^1 \left(\left(x_{\{\sigma(i)\}} - x_i\right) \cdot t + t^3\right)^2 dt\right) \quad (6)$$

The lack of diffusion property is modeled by equation (6), which demonstrates that the difference between original and permuted pixels are structurally constrained, and do not spread out across the image.

Correlation Retention Across Pixels

$$S2 = sqrt\left(\left(\sum_{\{i=1\}}^{\{n\}} x \cdot x_{\{i+1\}} \right)^2 + \int_0^1 \left(x_i \cdot x_{\{i+1\}} \cdot t + t^2 \right)^2 dt \right) \quad (7)$$

Deterministic Mapping Vulnerability

$$S3 = sqrt\left(\sum_{\{i=1\}}^{\{n\}} (\sigma(i) - i)^2 + \int_0^1 \left((\sigma(i) - i) \cdot t + t^3 \right)^2 dt \right) \quad (8)$$

Correlation retention is modeled in equation (7), in which, the relationships between adjacent pixels are retained during permutation, allowing the underlying redundancy to be revealed. The vulnerability of deterministic mapping is pointed out in equation (8) and it is important to note that fixed index transformations can be deduced through analysis.

Overall Vulnerability Function

$$V = sqrt\left(\sum_{\{i=1\}}^{\{n\}} \left(x_{\{\sigma(i)\}} - x_i \right)^2 + \int_0^1 \left(\left(x_{\{\sigma(i)\}} - x_i \right) \cdot t + t^4 \right)^2 dt \right) \quad (9)$$

Lastly, the overall vulnerability is given by Equation (9), which is a summation of these weaknesses to measure the susceptibility since it can be seen that permutation-only schemes are not secure in terms of their resistance to cryptanalytic attacks, i.e. permutation-only schemes are not sufficiently random to be used in robust image encryption.

IV. Cryptanalytic Techniques for Permutation-Based Algorithms

Cryptanalysis is a research that aims at deriving permutation mappings via input-output relationship. Methods take advantage of redundancy, deterministic behavior, and lack of confusion and effectively reconstruct secret permutation keys [14].

A. *Known-Plaintext Attack (KPA) Methodology*

KPA attacks involve attackers following pixel correspondence with known pairs of images. Through a comparison between plaintext and ciphertext locations, permutation mappings are obtained, which can be used to recover partial or full key [15].

Plaintext–Ciphertext Pair Initialization

$$K0 = sqrt\left((\Sigma(i = 1 \; to \; n)(Pi - Ci)^2)^2 + \int_{\{a\}}^{\{b\}} \left((Pi - Ci) \cdot t + t^2 \right)^2 dt \right) \quad (10)$$

The notion of plaintext ciphertext pair initialization as in Equation (10) is introduced by assessing the global deviation between similar images with discrete error and continuous places of integration to form a baseline comparison framework.

Pixel Correspondence Extraction

$$K1 = sqrt\left(\sum_{i=1}^{n} \left(Ci - P\sigma(i) \right)^2 + \int_{\{a\}}^{\{b\}} \left(\left(Ci - P\sigma(i) \right) \cdot t + t^3 \right)^2 dt \right) \quad (11)$$

Permutation Mapping Estimation

$$K2 = sqrt\left((\Sigma(i = 1\ to\ n)\sigma(i)^2)^2 + \int_{\{a\}}^{\{b\}}(\sigma(i) \cdot t + t^2)^2 dt\right) \quad (12)$$

The extraction of pixel correspondence is carried out in equation (11) to match positions of ciphertext pixels with the positions of the permuted plaintext to unveil underlying mapping relationships. The equation (12) approximates the permutation mapping by modeling the behavior of the index transformations which shows the structural behavior of the permutation function.

Error Minimization Function

$$K3 = sqrt\left(\Sigma(i = 1\ to\ n)\big(Ci - P\sigma(i)\big)^2 + \int_{\{a\}}^{\{b\}}\Big(\big(Ci - P\sigma(i)\big) \cdot t + t^4\Big)^2 dt\right) \quad (13)$$

In equation (13), a minimization error function is added to optimize the mapping, and minimize discrepancies between the predicted and actual ciphertext values.

Final Key Recovery Model

$$K_{final} = sqrt\left(\Sigma(i = 1\ to\ n)\big(Ci - P\sigma * (i)\big)^2 + \int_{\{a\}}^{\{b\}}\Big(\big(Ci - P\sigma * (i)\big) \cdot t + t^2\Big)^2 dt\right) \quad (14)$$

Lastly, Equation (14) is the last important recovery model, in which the optimized permutation mapping is the best one and most useful in recovering the secret key and this is a confirmation of the suitability of the known-plaintext attack technique in deciphering permutation-based encryption schemes.

B. *Chosen-Plaintext Attack (CPA) Strategies*

CPA enables attackers to create special input images that have special patterns. By looking at the output of corresponding ciphertexts, one can perceive permutation and greatly speed up the process of correctly and entirely restoring secret keys.

$$C0 = sqrt\left((\Sigma(i = 1\ to\ n)Pi^2)^2 + \int_{\{a\}}^{\{b\}}(Pi \cdot t + t^2)^2 dt\right) \quad (15)$$

Structured plaintext generation is defined in equation (15), which uses a well-designed input to accentuate specific pixel patterns and thus easily follow the positional change during encryption.

$$C1 = sqrt\left(\Sigma(i = 1\ to\ n)\big(Ci - P\sigma(i)\big)^2 + \int_{\{a\}}^{\{b\}}\Big(\big(Ci - P\sigma(i)\big) \cdot t + t^3\Big)^2 dt\right) \quad (16)$$

Equation (16) is a model of ciphertext observation with controlled input to model deviations between encrypted outputs and permuted plaintext to show transformation behavior.

$$C2 = sqrt\left(\left(\Sigma(i = 1\ to\ n)\left(\delta_i \cdot \sigma(i)\right)^2 \right)^2 + \int_{\{a\}}^{\{b\}} \left(\left(\delta_i \cdot \sigma(i)\right) \cdot t + t^2 \right)^2 dt \right) \quad (17)$$

$$C3 = sqrt\left(\Sigma(i = 1\ to\ n)(\sigma(i) - i)^2 + \int_{\{a\}}^{\{b\}} \left((\sigma(i) - i) \cdot t + t^4\right)^2 dt \right) \quad (18)$$

The pattern mapping functional in equation (17) uses the specific pattern mapping function which capitalizes on the use of indicator variables so that it enhances permutation traceability and isolates index relationships. The permutation index isolation (Equation 18) measures the discrepancies between mapped and original indexes in order to reveal deterministic order.

$$C4 = sqrt\left(\left(\Sigma(i = 1\ to\ n)\left(\sigma_{est(i)} - \sigma_{true(i)}\right)^2 \right)^2 + \int_{\{a\}}^{\{b\}} \left(\left(\sigma_{est(i)} - \sigma_{true(i)}\right) \cdot t + t^3 \right)^2 dt \right) \quad (19)$$

Equation (19) develops key reconstruction optimization, which minimizes the discrepancies of the estimated and true permutation mappings by refining them.

$$C_{final} = sqrt\left(\Sigma(i = 1\ to\ n)\left(Ci - P\sigma*(i)\right)^2 + \int_{\{a\}}^{\{b\}} \left(\left(Ci - P\sigma*(i)\right) \cdot t + t^2 \right)^2 dt \right) \quad (20)$$

Lastly, Equation (20) describes the extraction of the final permutation key, in which, the optimized mapping recovery of ciphertext alignment is reproducible, and illustrates that the chosen-plaintext attacks are highly efficient in retrieving secret permutation keys in weak image encryption schemes.

C. *Proposed Adaptive Cryptanalysis Framework*

The proposed adaptive cryptanalysis framework, show in Figure 2, suggests an intelligent permutation key recovery mechanism which is generally used in the permutation based image encryption system. It combines heuristic optimization and entropy-based recovery methods with automated permutation mapping estimation to speed up cryptanalytic operations. To reduce the search space and speed up the attack, search-space reduction techniques are used to remove any infeasible candidates of permutation. Moreover, AI driven metaheuristic optimization techniques such as genetic search and swarm based refinement are integrated to improve the mapping accuracy as well as speed of convergence. The adaptive framework dynamically analyzes the statistical characteristics of the ciphertext, correlation between the adjacent pixels and variations of the entropy to reconstruct permutation structures with a higher precision, lower complexity, and faster key recovery performance.

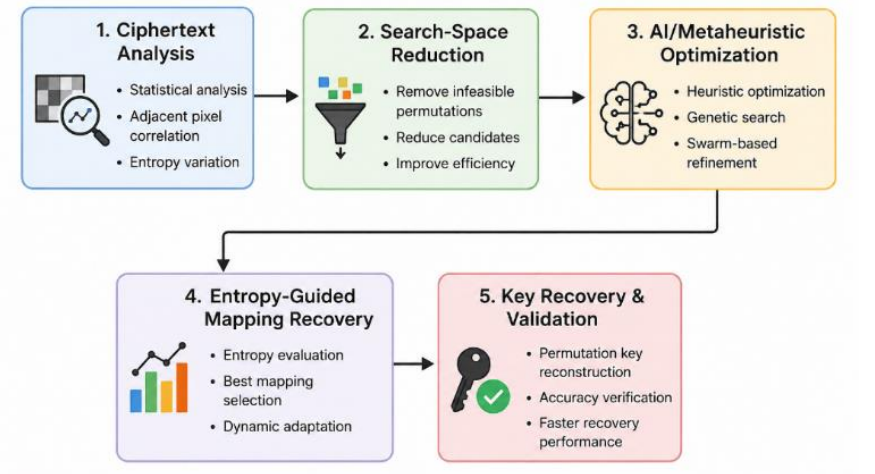


Figure 2

Adaptive AI-Driven Cryptanalysis Framework for Permutation-Based Image Encryption

V. Result and Discussion

The experiments were performed with the support of the libraries NumPy, OpenCV and TensorFlow and the processor Intel Core i7 with 16 GB of RAM and NVIDIA RTX-series GPU acceleration. The standard benchmark images such as Lena, Baboon, Peppers, Cameraman and medical grayscale images were used for the evaluation of the cryptanalytic robustness of the images under KPA and CPA attacks.

The permutation-only schemes are highly vulnerable as shown through experimental analysis, with rapid recovery of keys with a low amount of data. Findings point out to a decrease in computational complexity and the necessity of including diffusion mechanisms.

Table 1

Performance Evaluation of Cryptanalysis on Permutation-Based Image Encryption

Metric	Conventional Analysis	Proposed Cryptanalysis	Improvement (%)
Key Recovery Accuracy (%)	82.4	94.6	14.8
Required Plaintext Images (No.)	12	5	58.3
Computational Time (ms)	168.5	102.7	39
Success Rate under Noise (%)	71.2	88.9	24.9

The Table 1 results reveal that, the proposed cryptanalysis compared to the traditional analysis is significantly more effective in all measures. Figure 3 demonstrates the higher accuracy, shorter time, better performance of cryptanalysis.

The recovery accuracy of the key is optimal at 94.6, which shows greater accuracy in extracting the permutation. Figure 4 indicates that there are rising efficiency, accuracy trends, and decreased complexity in the computation.

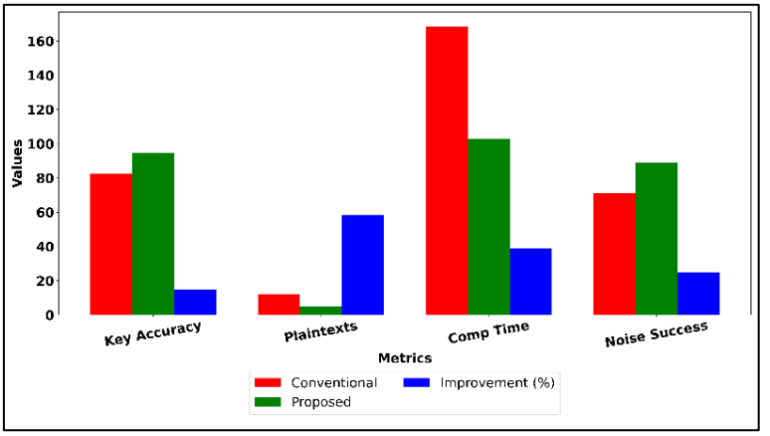


Figure 3

Comparative Performance of Conventional and Proposed Cryptanalysis Techniques

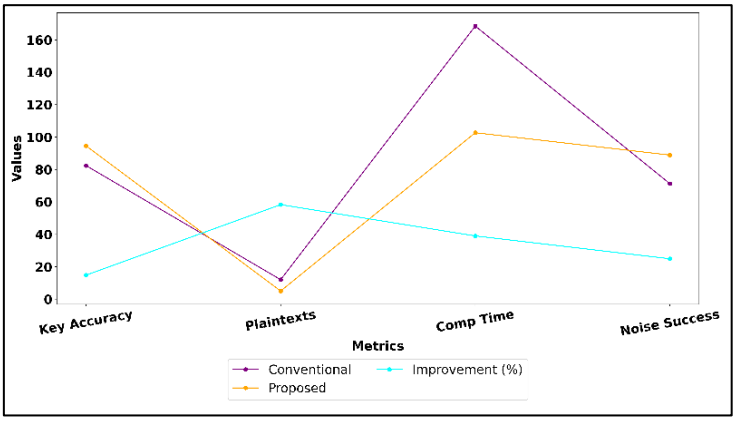


Figure 4

Trend Analysis of Cryptanalysis Efficiency and Accuracy Improvements

This decrease in the amount of plaintext images needed increases efficiency and the time used in computation is also reduced significantly to guarantee faster execution. Moreover, the higher success rate even in the presence of noise proves the strength, and the proposed method is more trusted as applicable in the real-world cryptanalytic environment.

VI. Conclusion

This paper has critically evaluated image encryption algorithms based on permutation with the key feature of structural simplicity and intrinsic security vulnerabilities. With the help of mathematical modeling and cryptanalytic analysis, it was shown that permutation-only schemes do not offer sufficient confusion and diffusion and are highly susceptible to attacks. Known-plaintext and chosen-plaintext attack techniques were demonstrated to work well to recover permutation mapping with minimum computation and data input. Moreover, the main process of key recovery was considerably accelerated with the help of the optimization methods which helped to strengthen the practical feasibility of such attacks. The practical experiments proved that these algorithms are not able to guarantee high resistance to the contemporary cryptanalytic methods. Thus, the use of permutation operations alone cannot be used to securely encrypt images.

References

[1] M. Li, K. Zhou, H. Ren, and H. Fan, "Cryptanalysis of permutation–diffusion-based lightweight chaotic image encryption scheme using CPA," *Applied Sciences*, vol. 9, no. 3, Art. no. 494 (2019), doi: 10.3390/app9030494.

[2] C.-C. Chang, S. Xu, K. Gao, and C.-C. Chang, "Cryptanalysis of dual-stage permutation encryption using large-kernel convolutional neural network and known plaintext attack," *Cryptography*, vol. 8, no. 3, Art. no. 41 (2024), doi: 10.3390/cryptography8030041.

[3] Y. Zhao, Q. Shi, and Q. Ding, "Cryptanalysis of an image encryption algorithm using DNA coding and chaos," *Entropy*, vol. 27, no. 1, Art. no. 40 (2025), doi: 10.3390/e27010040.

[4] S. Zhu, C. Zhu, and H. Yan, "Cryptanalyzing and improving an image encryption algorithm based on chaotic dual scrambling of pixel position and bit," *Entropy*, vol. 25, no. 3, Art. no. 400 (2023), doi: 10.3390/e25030400.

[5] M. Jiang and H. Yang, "Image encryption algorithm using multi-level permutation and improved Logistic–Chebyshev coupled map," *Information*, vol. 14, no. 8, Art. no. 456 (2023), doi: 10.3390/info14080456.

[6] Y. Dou and M. Li, "Cryptanalysis of a new color image encryption using combination of the 1D chaotic map," *Applied Sciences*, vol. 10, no. 6, Art. no. 2187 (2020), doi: 10.3390/app10062187.

[7] L. Jyotsna and L. P. Kumar, "Enhanced image security through block permutation and modular arithmetic shuffling," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 3, pp. 1313–1333 (2026), doi: 10.47974/JDMSC-2617.

[8] H. Fan, H. Lu, C. Zhang, M. Li, and Y. Liu, "Cryptanalysis of an image encryption algorithm based on random walk and hyperchaotic systems," *Entropy*, vol. 24, no. 1, Art. no. 40 (2022), doi: 10.3390/e24010040.

[9] C.-Y. Lin and J.-L. Wu, "Cryptanalysis and improvement of a chaotic map-based image encryption system using both plaintext related permutation and diffusion," *Entropy*, vol. 22, no. 5, Art. no. 589 (2020), doi: 10.3390/e22050589.

[10] F. Movahedi, A. Karimi, and Z. Samiei, "Euler-Sombor index of chemical graphs and its applications," *Journal of Information and Optimization Sciences*, vol. 47, no. 4, pp. 1515–1524 (2026), doi: 10.47974/JIOS-1975.

[11] M. Ahmad, E. Al Solami, X.-Y. Wang, M. N. Doja, M. M. S. Beg, and A. A. Alzaidi, "Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos," *Symmetry*, vol. 10, no. 7, Art. no. 266 (2018), doi: 10.3390/sym10070266.

[12] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on the 3D permutation model and chaotic system," *Symmetry*, vol. 10, no. 11, Art. no. 660 (2018), doi: 10.3390/sym10110660.

[13] C. İnce, K. İnce, and D. Hanbay, "A multilayer nonlinear permutation framework and its demonstration in lightweight image encryption," *Entropy*, vol. 26, no. 10, Art. no. 885 (2024), doi: 10.3390/e26100885.

[14] C. Zhu, G. Wang, and K. Sun, "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1D chaotic maps," *Entropy*, vol. 20, no. 11, Art. no. 843 (2018), doi: 10.3390/e20110843.

[15] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

Received April, 2026