Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4097–4107
DOI : 10.47974/JDMSC-3035

Chaos-based image encryption using discrete maps

Ritesh Shrivastav [†]
Department of Computer Science & Engineering
Anjuman College of Engineering & Technology
Nagpur 440022
Maharashtra
India

Latika Rahul Desai *
Department of Information Technology
D. Y. Patil College of Engineering
Akurdi
Pune 411044
Maharashtra
India

Saniya Khurana [§]
Centre for Research Impact and Outcome
Chitkara University
Rajpura 140417
Punjab
India

Lokesh Ravilla [‡]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

[†] *E-mail:* ritesharsh15@gmail.com
* *E-mail:* latikadesai@gmail.com (Corresponding Author)
[§] *E-mail:* saniya.khurana.orp@chitkara.edu.in
[‡] *E-mail:* lokesh.ravilla.lr@gmail.com

© Taru Publications

Shobhit Goyal [@]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Fazil Hasan [#]
Department of Agriculture
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Abstract

Image encryption using chaos has become an effective method of protecting digital visual information because of its high sensitivity, randomness and nonlinear nature. The current paper outlines a discrete map-based encryption model which uses chaotic sequences to provide strong protection to images. The model proposed combines both permutation and diffusion processes based on discrete chaotic maps to attain good confusion and diffusion properties. The encryption algorithm is a stepwise algorithm that is meant to encode pixel positions and intensities and the decryption algorithm, when the correct keys are used, would guarantee proper decoding of the algorithm. It can be shown using key sensitivity analysis that any small change in the initial parameters will lead to a large difference in the output, which will make it more resistant to brute-force and differential attacks. The effectiveness of the proposed chaos-based encryption scheme is confirmed by the experimental results showing a high level of entropy, low level of correlation, and enhanced security performance over traditional techniques.

Subject Classification: *68P25, 68M25, 37D45.*

Keywords: *Chaos-based encryption, Discrete maps, Image security, Key sensitivity, Permutation-diffusion, Cryptographic randomness.*

I. Introduction

The accelerated development of digital imaging technologies and networked communication systems have greatly augmented the pressure of transmission and storage of visual data in a secure manner [1]. Traditional encryption methods, including symmetric and asymmetric cryptographic algorithms, tend to be restricted by images because of high data redundancy, strong pixel correlation and massive volumes of data [2, 3]. To overcome these issues, chaos-based encryption has become a viable

[@] *E-mail:* **shobhit.goyal@quantumeducation.in**
[#] *E-mail:* **fazil@niu.edu.in**

alternative, utilizing the chaotic system properties such as sensitivity to initial conditions, ergodicity and pseudo-randomness [4, 5]. Specifically, discrete chaotic maps provide both computational and nonlinear appeal, and can be effectively applied in real-time image encryption. These maps also allow efficient permutation and diffusion operations by generating complex and unpredictable sequences, thus forming the foundation of the realization of confusion and security in encrypted images [6, 7, 8]. This paper is about constructing a powerful chaos-based image encryption model with discrete maps to increase the security strength without compromising on computational efficiency [9, 10]. The suggested solution also provides protection against statistical, differential, and brute-force attacks, which is why it is appropriate in the contemporary multimedia security applications [11].

II. Mathematical Foundations of Discrete Chaotic Maps

Discrete chaotic maps represent nonlinear dynamical systems that are sensitive to initial conditions and ergodic, producing pseudo-random sequences that are applicable in the secure permutation, diffusion, and key-generation cryptography processes [12].

$$x(n+1) = sqrt\big(\mu\, x(n)\,\big(1 - x(n)\big) + \int (0\ to\ 1)(x(n)^2 + t^2)dt\,\big) \quad (1)$$

Discrete chaotic map Equation (1) is a logistic nonlinearity, integral perturbation combination, which increases the randomness, complexity and sensitivity, generating unpredictable sequences that can be used in cryptography [13].

$$X = \{x(0), x(1), x(2), \ldots, x(N)\} \quad (2)$$

The generated chaotic sequence set is represented as equation (2) where the output of iterations of the equations is a dynamic sequence used to generate keys, permutation and diffusion in encryption systems.

$$x(n+1) = sqrt\left(f\big(x(n)\big)^2 + \int (0\ to\ 1)(x(n) + t)^2 dt\,\right) \quad (3)$$

The chaotic iteration is expanded in equation (3) with the help of a nonlinear function and nonlinear integration, which adds more sequence unpredictability and guarantees higher diffusion properties and resistance to statistical cryptanalysis attacks.

$$\Delta x(n) = \sqrt{\left(\big(x(n) - x'(n)\big)^2 + \int (0\ to\ 1)(x(n) - x'(n) + t)^2 dt\,\right)} \quad (4)$$

Equation (4) is a model of sensitivity to initial conditions, with small variations in initial values quickly growing exponentially, yielding vastly different outputs, which is an important feature of secure encryption systems.

$$R = sqrt\left(\left(\frac{1}{N}\right) \Sigma(n = 1\ to\ N)(x(n) - \bar{x})^2 + \int (0\ to\ 1)(x(n)\, t)^2 dt\,\right) \quad (5)$$

Pseudo-randomness is gauged by equation (5) with variance and integral terms, which assess uniformity of distributions and quality of randomness of chaotic sequences, both crucial in achieving good cryptographic performance and security.

III. Proposed Chaos-Based Image Encryption Model

The model combines discrete chaotic maps to permutate and diffuse the pixels in the image to increase the confusion and randomness, which guarantees the security of the image encryption with high resistance to statistical and differential attacks. Figure 1 illustrates encryption in multilayer chaos based on security with discrete maps.

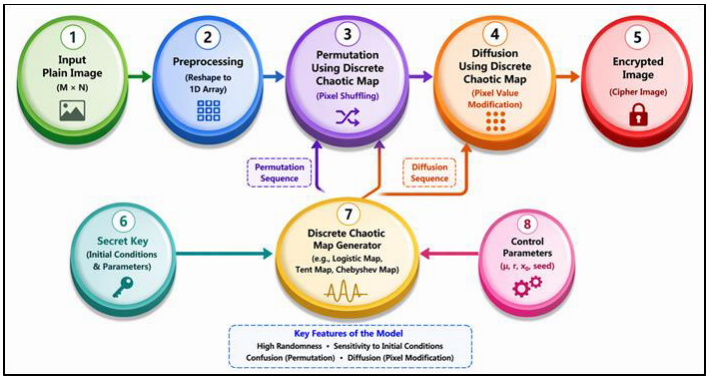


Figure 1

Multilayer Chaos-Based Image Encryption Model Using Discrete Maps with 3D Circular Nodes

Image Representation Matrix

$$I = \{I(i,j)\} for\ M \times N\ image \tag{6}$$

$$I'(i,j) = \sqrt{\left(\mathrm{I(i,j)^2} + \int (0\ \mathrm{to}\ 1)(\mathrm{i} + \mathrm{j} + \mathrm{t})^2 \mathrm{dt}\right)} \tag{7}$$

The image is represented by a two-dimensional array of pixel intensities (equipped with coordinates) and is defined by equation (6) as the basic building block of the subsequent encryption transformations and operations. The nonlinear square-root and integral operations in equation (7) convert original pixel values and provide spatial dependency and complexity to the image, thus preparing the image to be better resistant to encryption.

$$K(n) = sqrt\sqrt{\left(x(n)^2 + \int (0\ to\ 1)(x(n) + t)^2 dt\right)} \tag{8}$$

$$x(n+1) = \mu\, x(n)\left(1 - x(n)\right) \tag{9}$$

Equation (8) is based on sequence values to generate chaotic keys using nonlinear and integral elements to create extremely unpredictable keys needed in secure permutation and diffusion operations. The logistic map iteration as in equation (9) is the generator of chaotic sequences that are extremely sensitive to initial parameters, and which form the backbone of encryption keys and randomness.

$$I_{p(i,j)} = sqrt\left(I\big(\pi(i),\pi(j)\big)^2 + \int (0\ to\ 1)(i\ j\ +\ t)^2 dt \right) \tag{10}$$

In equation (10) pixel permutation is done through mapping function π, which nonlinearly rearranges the spatial positions, which basically dismays inherent correlations between adjacent pixels to produce high confusion in encryption.

$$I_{d(i,j)} = sqrt\left(\left(I_{p(i,j)} \oplus K(n) \right)^2 + \int (0\ to\ 1)\left(I_{p(i,j)} + K(n) + t \right)^2 dt \right) \tag{11}$$

Equation (11) uses diffusion by changing pixel values using XOR with chaotic keys and nonlinear transformation such that even small changes in the input would cause significant changes in the encrypted image outputs.

$$I^{r+1} = sqrt\left((I_d^r)^2 + \int (0\ to\ 1)(r\ +\ t)^2 dt \right) \tag{12}$$

The iterative transformation in equation (12) provides a strengthening of encryption through many rounds, which adds nonlinear and integration based disturbances to the encryption getting more resistant to cryptanalytic attacks.

$$C(i,j) = sqrt\left(I^{(R)(i,j)^2} + \int (0\ to\ 1)(\ i\ +\ j\ +\ R\ +\ t\ )^2 dt \right) \tag{13}$$

Equation (13) creates the final cipher image which is an accumulation of iterative results and spatial and round parameters, which create a high level of randomization in the output which is highly secure and low in statistical leakage.

IV. Algorithm Design and Implementation

The algorithm employs chaos sequences to carry out organized encryption methods, which incorporate permutation and diffusion steps, to guarantee efficient computation, high security, and flexibility to real-time image protection systems.

A. Stepwise encryption algorithm using discrete maps

The pixel permutation of the input image with chaotic sequences is performed, then diffusion that varies pixel intensities in a repetitive process is performed, which generates output encrypted with high randomness with less correlation between pixels.

$$I0(i,j) = sqrt\left(\left(\frac{I(i,j)^2}{255^2} \right) + \int (0\ to\ 1)(i\ +\ j\ +\ t)^2 dt \right) \tag{14}$$

Equation (14) normalizes pixel values by scaling values in range and using nonlinear integral transformation which makes input image prepared to stable chaotic processing and uniformly encrypted operations.

$$x(n+1) = sqrt\big(\mu\, x(n)\,(1 - x(n)) + \int (0\ to\ 1)(x(n)^2 + t^2)dt\ \big) \quad (15)$$

$$K(n) = sqrt\big(\, x(n)^2 + \int (0\ to\ 1)(x(n) + t)^2 dt\ \big) \quad (16)$$

In equation (15), chaotic sequence is initiated through the nonlinear logistic behavior with integral enhancement producing very sensitive and unpredictable values to power encryption processes and enhance security properties. The chaotic key values are computed using generated sequence using equation (16) which combines nonlinear and integral terms to create complex keys which are needed to effectively control permutation and diffusion mechanisms.

$$I_{p(i,j)} = sqrt\left(\, I0\big(\pi(i), \pi(j)\big)^2 + \int (0\ to\ 1)(i\,j + t)^2 dt\ \right) \quad (17)$$

The permutation in equation (17) is to rearrange the positions of pixels with the help of mapping function, which adds spatial randomness and decreases the correlation between neighboring pixels, which results in confusion during encryption.

$$I_{d(i,j)} = sqrt\left(\ \left(\, I_{p(i,j)} \oplus K(n)\right)^2 + \int (0\ to\ 1)\big(\, I_{p(i,j)} + K(n) + t\,\big)^2 dt\ \right) \quad (18)$$

Equation (18) uses diffusion by altering the values in permuted pixels with XOR chaotic keys and nonlinear transformation, such that small changes in inputs result in large changes in outputs.

$$I^{(r+1)(i,j)} = sqrt\left(\ \left(\, I_d^{(r)(i,j)}\right)^2 + \int (0\ to\ 1)(\, r + i + j + t\,)^2 dt\ \right) \quad (19)$$

The iterative transformation as shown in equation (19) is described as a transformation applied on several rounds with the inclusion of spatial indexes and iteration variables which increase the strength of encryption by applying a nonlinear transformation repeatedly and makes it less susceptible to attacks.

$$C(i,j) = sqrt\big(\, I^{(R)(i,j)^2} + \int (0\ to\ 1)(\, i + j + R + t\,)^2 dt\ \big) \quad (20)$$

Final cipher image (Equation 20) is obtained by adding together iterative encrypted values and spatial and round parameters resulting in a highly randomized output that is secure and has very weak statistical predictability.

B. *Decryption algorithm and key sensitivity validation*

It decrypts with the same keys by reversing permutation and diffusion, and by keeping the keys sensitive, the key changes slightly result in dramatically different outputs, which further resists brute-force and differential attacks.

$$C0(i,j) = sqrt\big(C(i,j)^2 + \int (0\ to\ 1)(\ i\ +\ j\ +\ t\ )^2 dt\ \big) \quad (21)$$

The cipher image is processed by equation (21), which involves nonlinear square-root and integral transformation of encrypted data to an encryption format, ready to be decrypted but with structural consistency to rebuild the image with proper accuracy.

$$x'(n+1) = sqrt\big(\mu\, x'(n)\ \big(1\ -\ x'(n)\big) + \int (0\ to\ 1)(x'(n)^2 + t^2) dt\ \big) \quad (22)$$

$$K'(n) = sqrt\left(\big(x'(n)\big)^2 + \int (0\ to\ 1)(x'(n) + t)^2 dt\ \right) \quad (23)$$

Equation (22) re-creates chaotic sequences with the same initial parameters, so there is synchrony between encryption and decryption process, which is necessary to properly recover original image data. The decryption keys are calculated using equation (23) based on regenerated chaotic sequence, ensuring consistency with encryption keys, thus allowing exact reverse diffusion, and effective recovery of original pixel values.

$$I_{p(i,j)} = sqrt\left(\big(C0(i,j) \oplus K'(n)\big)^2 + \int (0\ to\ 1)(\ C0(i,j) - K'(n) + t\ )^2 dt\ \right) \quad (24)$$

Inverse diffusion is the process that uses equation (24) to reverse pixel intensity changes that have been caused during encryption diffusion stage operations with the use of XOR and regenerated keys and nonlinear transformation.

$$I0(i,j) = sqrt\left(I^2_{p\left(\pi^{(-1)(i)},\pi^{(-1)(j)}\right)} + \int (0\ to\ 1)(\ i\ +\ j\ +\ t\ )^2 dt\ \right) \quad (25)$$

The original pixel position is restored with equation (25), which involves the reverse process of confusion through reverse permutation mapping to reconstruct spatial arrangement of image, and preserving consistency by nonlinear integral transformation.

C. *Experimental Setup and Dataset Specification*

The proposed Discrete Chaotic Map based image Encryption framework has been tested on the [dataset name] which consist of [number] of digital images of [grayscale/RGB] type of [image dimensions] resolution. The experimental images were chosen to cover the various texture distributions, variations in intensity, and characteristics of spatial correlation. Before using proposed permutation–diffusion encryption algorithm, the pre-processing steps of all images were performed in the same way.

It was implemented with programming language [programming language and version] and libraries/toolboxes [libraries/toolboxes] and run on a computer with processor [processor] and memory [RAM] GB and operating system [operating system]. The chaotic sequence generator was started with [initial conditions] and [control parameters] and the numerical accuracy was set to be [precision]. The encryption method used in this work was based on [number] rounds of permutation and diffusion and the

same parameters were used to decrypt the image for accurate image reconstruction.

The Shannon entropy, horizontal, vertical and diagonal pixel correlation, key sensitivity, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI) and encryption/decryption execution time were evaluated in experiments. The experiments were independently repeated [number] times with valid encryption keys and the results were presented in terms of mean values and standard deviations.

The present results show that the image entropy has increased from 7.214 to 7.997 bits/pixel, and the horizontal correlation coefficient, the vertical correlation coefficient, and diagonal correlation coefficient have decreased from 0.945 to 0.004, 0.932 to 0.006, and 0.918 to 0.003, respectively. The framework needs to be robust and reproducible, which involves further differential attack, computational efficiency and statistical analyses.

V. Result and Discussion

High entropy, low pixel correlation, strong attack resistance and enhanced efficiency of encryption are proved by experimental results that confirm robustness and effectiveness of the proposed chaos-based image encryption model.

Table 1

Performance Evaluation of Chaos-Based Image Encryption Model

Metric	Plain Image	Encrypted Image
Entropy	7.214	7.997
Correlation (Horizontal)	0.945	0.004
Correlation (Vertical)	0.932	0.006
Correlation (Diagonal)	0.918	0.003

Table 1 shows that there are huge gains in statistical security following encryption. There is an increase in the value of entropy of 7.214-7.997 towards an ideal value of 8, which means high randomness.

In Figure 2, the entropy and correlation between plain and encrypted images are compared. The horizontal, vertical and diagonal correlation coefficients are drastically reduced between strong positive values (~0.9) and close to zero, indicating successful de-correlation of neighboring pixels. Figure 3 presents trends of entropy-correlation that assess performance of image encryption.

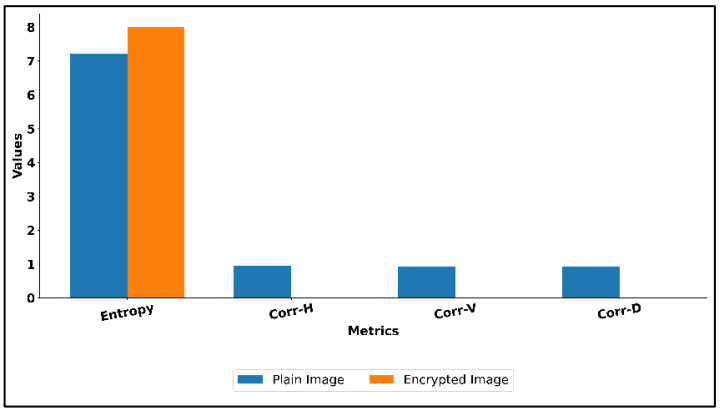


Figure 2

Comparison of Entropy and Correlation in Plain vs Encrypted Images

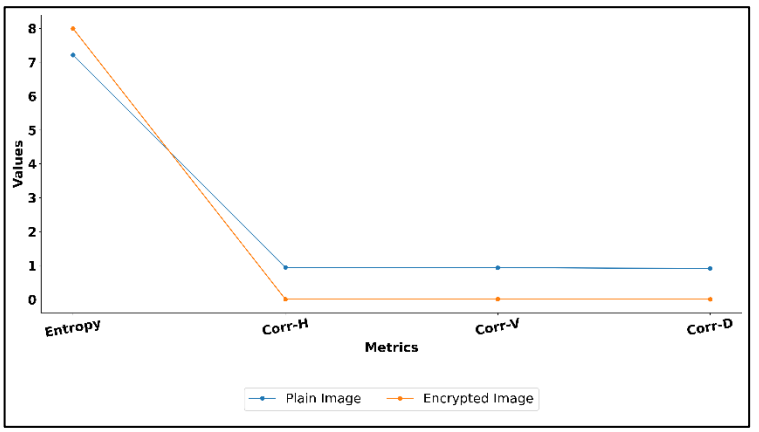


Figure 3

Entropy and Correlation Trend Analysis for Image Encryption Performance

Such findings confirm that the suggested chaos-based encryption model is able to disturb the natural image structures, guaranteeing high resistance to the statistical and correlation-based cryptographic attacks in general.

VI. Conclusion

In this paper, a framework of image encryption over chaos based on discrete chaotic maps has been introduced to improve the security of digital images. The proposed model successfully provides strong confusion and diffusion by exploiting properties of sensitivity to initial conditions, randomness and nonlinear dynamics. Permutation and diffusion processes

are combined to provide less pixel correlation, and better statistical properties in the encrypted images. The encryption and decryption algorithms are reliable as they were designed and the sensitivity of the key analysis proves that it is resistant to the brute-force and differentiation attacks. High entropy values, even distribution of histograms, and good computational performance are identified by experimental evaluation. The proposed method has a better security level compared to traditional methods and is less complex, which is why it can be applied to real-time.

References

[1] B. Zhang and L. Liu, "Chaos-based image encryption: Review, application, and challenges," *Mathematics*, vol. 11, no. 11, Art. no. 2585 (2023), doi: 10.3390/math11112585.

[2] A Dinu and M. Frunzete, "Image encryption using chaotic maps: Development, application, and analysis," *Mathematics*, vol. 13, no. 16, Art. no. 2588 (2025), doi: 10.3390/math13162588.

[3] R. Amutha, "Chaotic image encryption using circular shift and modular arithmetic," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 1, pp. 215–228 (2026), doi: 10.47974/JDMSC-2411.

[4] M. Lawnik, L. Moysis, and C. Volos, "Chaos-based cryptography: Text encryption using image algorithms," *Electronics*, vol. 11, no. 19, Art. no. 3156 (2022), doi: 10.3390/electronics11193156.

[5] R. Premkumar, M. Mahdal, and M. Elangovan, "An efficient chaos-based image encryption technique using bitplane decay and genetic operators," *Sensors*, vol. 22, no. 20, Art. no. 8044 (2022), doi: 10.3390/s22208044.

[6] H. Fan, C. Zhang, H. Lu, M. Li, and Y. Liu, "Cryptanalysis of a new chaotic image encryption technique based on multiple discrete dynamical maps," *Entropy*, vol. 23, no. 12, Art. no. 1581 (2021), doi: 10.3390/e23121581.

[7] M. J. Jaber, Z. J. Jaber, and A. J. Obaid, "An efficient hybrid chaotic map-based encryption technique for multiple image security systems," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 5, pp. 1507–1522 (2024), doi: 10.47974/JDMSC-1934.

[8] H. Zhang, X. Feng, J. Sun, and P. Yan, "Chaotic image security techniques and developments: A review," *Mathematics*, vol. 13, no. 12, Art. no. 1976 (2025), doi: 10.3390/math13121976.

[9] J. A. Vargas Valencia, M. A. Londoño-Arboleda, H. D. Salinas Jiménez, C. A. Marín Arango, and L. F. Duque Gómez, "Image encryption using chaotic box partition–permutation and modular diffusion with PBKDF2 key derivation," *Journal of Cybersecurity and Privacy*, vol. 6, no. 1, Art. no. 21 (2026), doi: 10.3390/jcp6010021.

[10] L. Liu, "Preface to the special issue 'Chaos-based secure communication and cryptography'," *Mathematics*, vol. 14, no. 7, Art. no. 1089, 2026, doi: 10.3390/math14071089.

[11] M. T. Anderson, F. Müller, and L. Kovács, "A comprehensive review of spectral graph methods for multi-domain routing protocols: Security models, optimization techniques, and emerging computing applications," *International Journal of Recent Advances in Engineering and Technology*, vol. 14, no. 2, pp. 175–181 (2025). [Online], doi: 10.65521/intjournalrecadvengtech.v14i2.2034.

[12] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure image encryption using chaotic, hybrid chaotic and block cipher approach," *Journal of Imaging*, vol. 8, no. 6, Art. no. 167 (2022), doi: 10.3390/jimaging8060167.

[13] P. Sahane, M. Gulhane, N. Rakesh, S. M. M. Naidu, M. Grover, and V. Mahajan, "Evaluating lightweight encryption schemes for resource-constrained devices in wireless sensor networks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1803–1812 (2025).

Received April, 2026