Kumar and Revathi
Journal of Engineering and Applied Science (2024) 71:41
https://doi.org/10.1186/s44147-023-00349-8

Journal of Engineering and Applied Science

RESEARCH Open Access

An efficient image encryption algorithm using a discrete memory-based logistic map with deep neural network

B. Sakthi Kumar[1*] and R. Revathi[2]

*Correspondence:
b.sakthi2004@gmail.com

[1] Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India
[2] Department of ECE, KLEF, Guntur, India

Abstract

In the last few years, multimedia technology has made tremendous strides. These days, the Web is frequently used to transfer multimedia content, including audio, video, and photos. However, the Internet is a very vulnerable medium with many security holes. To ensure that multimedia content carried across unprotected channels, like the Internet, is secure and private, several encryption techniques have been proposed. New encryption strategies must be developed because multimedia data streams cannot be encrypted using traditional methods. Therefore, the main goal of the recommended system is to present an analytical research approach for introducing a sophisticated framework wherein the suggested encryption technologies' efficacy is increased through the use of deep neural networks (DNNs). The robustness of the DNN principle is coupled with a discrete memristor-based logistic chaotic map notion for enhanced security performance. In this paper, three distinct encryption algorithms—Arnie cat with an artificial neural network (ANN), Henon map with an ANN, and logistic map with a DNN—are compared for security and performance with the suggested algorithm. Correlation coefficients, information entropy, number of pixels changing rate (NPCR), encryption quality, and encryption duration are the cryptographic analysis parameters examined here. The results show that the recommended implementation enhances security performance without degrading image quality. The proposed algorithm achieves 35.9% of UACI, 99.95% of NPCR, and 7.997231 of entropy.

Keywords: Image encryption, Image decryption, Arnold map, He map, Logistic map, Artificial neural network, Deep neural network, Memristor

Introduction

Digital images have become increasingly popular as network and multimedia technology have advanced. Image data has a high correlation and high redundancy between pixels. In some cases, imaging applications must meet their requirements, such as real-time communication and evaluation. Security is one of the primary objectives of information transmission over a network. Therefore, multimedia information security has become critical in e-health, the military, e-commerce, banking transactions, and mobile applications [1, 2]. Communication information (plain text) must be protected

from unauthorized users to provide security properties to multimedia content. Multimedia content must be protected from attacks such as interception, interruption, fabrication, and modification [3, 4]. Encryption technology is a secure transmission method. This technology encrypts the data to be transmitted, converting it into cypher text that an authorized person can successfully restore. Several encryption schemes can be used to secure images [5] Fig. 1.

Encryption algorithms are classified as direct or partial encryption to provide integrity and privacy [6]. All media data is encrypted in full encryption [7]. It can encrypt large amounts of data, making it less efficient but more secure. Only a portion of the media content is encrypted during selective (partial) encryption. Because encryption operations are performed on a small amount of data, partial encryption algorithms reduce encryption and decryption time, making them more efficient but less secure [8–10]. Some researchers have created a single scheme that combines encryption and compression. Encryption and compression are implemented simultaneously in such a scheme [11].

A memristor is a fundamental circuit unit with memory that illustrates the connection between charge and magnetic flux. Furthermore, memristors have numerous applications, including neural networks [12], electrical engineering [13–15], secure communication [16], and so on. Classic chaotic maps, such as the logistic and henon maps, frequently suffer from a narrow parameter range and low complexity. To improve the dynamic behavior of two classical discrete maps, this article introduces discrete memristor models in logistic classical discrete maps inspired by previous outstanding works. Furthermore, the chaotic behavior of the chaotic map provides sufficient security. Combining deep learning and chaotic behavior may result in a more compelling image encryption method. As a result, the paper presented here presents a framework in which a deep learning logistic map is used to improve optimization for an enhanced image encryption process. This paper compares the security and performance of the proposed algorithm with three different encryption algorithms: Arnold cat with artificial neural networks (ANN), Henon map with artificial neural networks (ANN), and logistic map with deep neural networks (DNN).

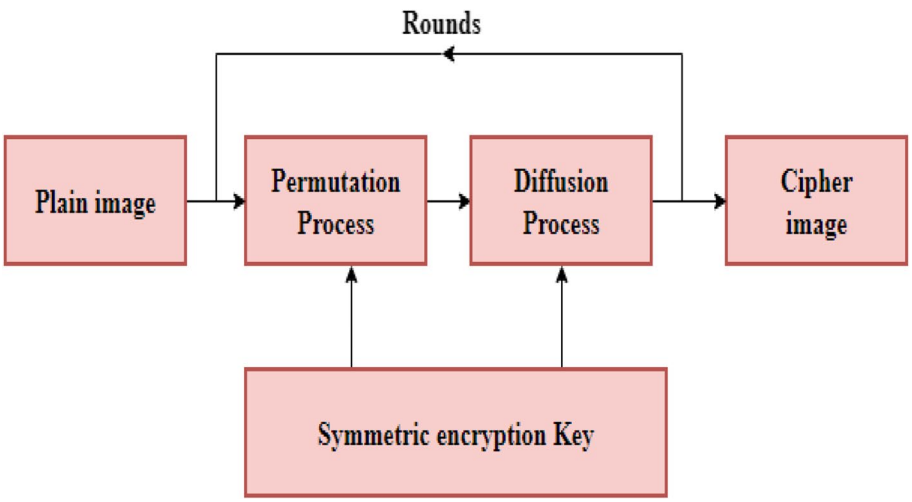


Fig. 1 Encryption architecture

We put the proposed image encryption technique through various assaults as part of our thorough security study. A variety of statistical and cryptanalysis attacks, such as known-plaintext and chosen-plaintext attacks, cropping attacks (random and selective), noise attacks (AWGN and salt-and-pepper noise), and adaptive attacks (iterative and machine learning-based) were among them. We evaluated our scheme's resilience in protecting sensitive image data by contrasting its performance with current approaches. This allowed us to confirm the scheme's effectiveness and security in various attack situations.

The rest of this article is organized as follows. Section 2 provides an overview of the most recent literature review. Section 3 discusses the proposed encryption techniques. Section 4 discusses the comparison results and security analysis of the proposed algorithms. Finally, Section 5 summarizes some final observations.

Literature survey

Sara t. Kamal et al. (2021) Presented novel cryptographic techniques for greyscale and color medical data. A new image feature extraction based on blocks is demonstrated. The image blocks are shuffled using zigzag patterns, rotations, and random structures. The encrypted image is then propagated using the key generated by the chaotic logic graph. There were comparisons with various encryption techniques. The suggested algorithm performs better than previously available encryption techniques in medical image encryption. The results demonstrate that the algorithm can encrypt color and greyscale grayscale medical images [17].

Shaimaa Abbas et al. (2020) proposed different encryptions and decryption methods using a chaotic neural network (CNN). The goal is to combine ANN and chaotic cryptography efficiently. The neural network weights are determined using the chaotic sequence. They are constantly updated based on the encryption algorithm's key generation. Matlab is used to implement the system. Because it is based on ANN, this system is complex. Matlab software saves time because it is simple and has many tools. This method encrypts the image at the sending end and then uses a decryption algorithm on the receiving end to restore the same original image as the transmitted image [18].

Shima Ramesh Maniyath et al. (2020) created a statistical research method for presenting a sophisticated framework in which DNN was used to optimize the effectiveness of simple encryption techniques. The ability of optimization concepts to improve security efficiency reinforces the Chaos Map concept. The findings reveal that the proposed application increases security while maintaining image quality. As a result, this paper examines a more effective and efficient image system security, with quantitative simulation demonstrating that it outperforms other commonly used machine learning methods [19].

N.K. Pareek et al. (2006) presented an image encryption technique with an 80-bit external key and two chaotic logic graphs is proposed. By assigning a different weight to each primary key bit, the default values for both logical mappings are obtained. Furthermore, the suggested encryption method encrypts pixels in an image using eight different types of operations, resulting in the logical mapping determining which one is used for a given pixel. Several experiments, statistical analysis, and sensitivity analysis demonstrate that the suggested algorithm provides a secure and effective method for real-time image communication and encryption [20].

Pranjali Sankhe et al. (2018) presented a proposed symmetric image encryption algorithm that employs a novel image pixel shuffling method to achieve effective and efficient image encryption. The procedure of encrypting and decrypting data that is used to keep data and images secure and private is known as cryptography. We will apply chaotic encryption and decryption to images in this article. The chaos method is a popular algorithm in real-time secure image communication systems. The henon map generates the critical value, and the Arnold cat map completes the pixel blending [21].

Otilia Cangea et al. (2018) presented a novel approach for implementing a chaotic-based color image encryption method with a particular function to improve data security. Color images can be encrypted using the chaos-based encryption system established and proposed in this paper by simultaneously encrypting their R, G, and B components. This cryptosystem was preferred after attempting several various approaches based on the same chaos principle. Still, they were demonstrated to be faster due to heavy computation or the need to save the permutation table required for the decryption stage. This also represents a significant vulnerability [22].

Sakshi Patel et al. (2020) presented an encryption method based on chaotic logistic mapping and DNA encoding. The image is broadcast using the 32-bit ASCII private key. The demonstration outcomes show that the proposed algorithms perform better than other logic map encryption methods. The proposed method also considers possible parameters such as PSNR and SSIM. Display and analyze the results of encryption and decryption algorithms using various parameter measurements [23].

Mingming Chen et al. (2020) presented an encoding algorithm that is then used to shuffle the subimage or pixel locations. After that, the encoded sub-images are composited into a single image. Finally, DRPE is used to encode the composite image. The new encryption application's security level can be enhanced by modifying the shear let transform's variables and selecting methods to encode pixels and synthesize various pictures into one image. Analytical and experimental outcomes demonstrate that the suggested optical encryption framework is practical. New encoding methods and reversible synthesis methods can be used to improve the proposed cryptographic framework [24].

Zeesha Mishra et al. (2020) presented dual-speed and small-area configurations for the SIT method in resource-constrained domains. The suggested channel is helpful for high-frequency applications, whereas the proposed serial configuration benefits applications with small area requirements, lowering hardware costs. The proposed design is implemented in the FPGA device XC5VLX50T-3ff1136, with a 287.51-MHz operating frequency in a segmented architecture and 46 segments in a serial architecture. SIT has five rounds but provides enough security for data encryption. According to security analysis, the algorithm has more entropy, good NPCR and UACI, more key space, and the best adjacent pixel correlation [25].

Methods

Image cryptographic techniques can become an essential part of the image delivery process if they strive for reliability while maintaining the highest level of security. This section details the proposed algorithm with three algorithms: the Logistic with deep neural

network (DNN), the Henon map with artificial neural network (ANN), and the Arnold map with ANN. The original and encrypted images are fed into the ANN/DNN. The encrypted and decrypted images are then provided into an artificial neural network/deep neural network. Intensity histograms for the actual and encrypted images, pixel correlation plots, key sensitivity, loss, and accuracy for the original, encrypted, and decrypted images, and structural similarity among the authentic and encrypted photos are among the metrics used to assess their quality. Figure 2 shows the system design of the proposed methodology.

Arnold cat with artificial neural network (ANN)

Arnold cat map algorithm (ACM)

ACM is one of the encryption methods used to encrypt images. The theory works mathematically by expanding and deforming a square, then snapping it together similarly. ACM works by encoding the position of a pixel without varying its value. ACM is a two-dimensional reversible chaotic graph [26]. This can be accomplished using the formula below.

$$[x_{n+1}\ y_{n+1}\ ] = [1\ c\ d\ cd + 1\ ][x_n\ y_n\ ] \bmod (\mathrm{M}) \tag{1}$$

Where c and d are both positive integers. (x_{n+1}, y_{n+1}) represents the new position of the original image, and (x_n, y_n) represents the primary position of the actual image. Where $n = 0, 1, 2$, There exist positive integers T after iterating N times, such that $(x_{n+1}, y_{n+1}) = (x, y)$.

The period T is determined by the original image's variables c, d, and size M. Because there are only linear transforms and modulation functions, using an ACM to shuffle pixel positions is highly efficient. After much iteration, the relationship between proximate pixels can be mixed entirely. On the other hand, the periodicity of the Arnold cat graph reduces the encryption's security because a potential attacker can iterate through the Arnold cat graph indefinitely to re-appear the actual image. The distinction between authentic and encrypted images is not statistically significant. Furthermore, the space available for positive integer keys is limited.

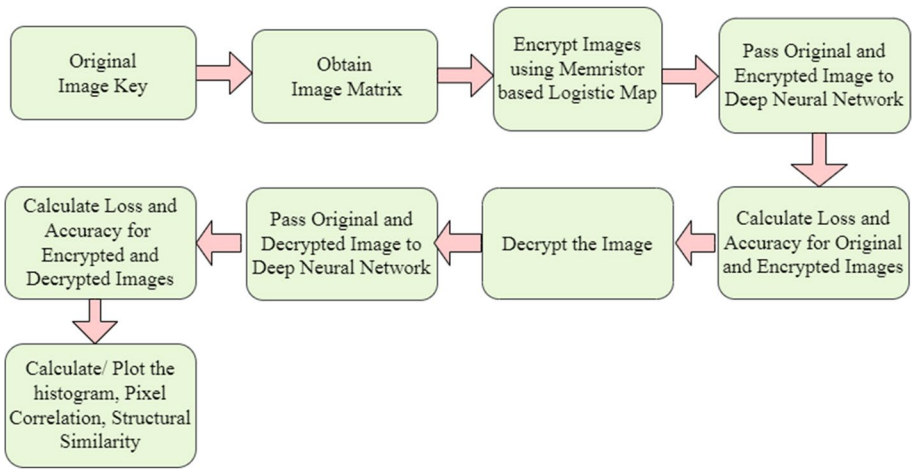


Fig. 2 System design

Artificial neural network

A neural network is a machine that depicts how the brain performs a specific task. ANN is used to create matrix codes from planes. After training, the ANN broadcasts the code that generates the bias and weight matrices for the first step. It is a computer system inspired by the human brain's learning ability. It is the only type of structure handling method. ANNs are well-known for their unique features. It has elementary processing elements, such as neurons. A large number of weighted links exist between distributed elements. These are analyzed during the e-learning process. Because of their distributed representation, massive parallelism, learning ability, and fault tolerance, artificial neural networks are more valuable. An ANN consists of processing units, topology, and learning algorithms.

ANN is widely used in a variety of fields. Some examples include clustering/classification, function approximation, prediction, pattern classification, optimization, control, and content-addressable memory. At the decryption end, a chaotic binary sequence is generated and sent to the ANN, and the ANN generates the weight to generate the key to obtain the original image. Figure 3 shows the ANN structure.

Henon map with artificial neural network (ANN)

Henon map

The Henon map is a well-studied method of chaotic discrete-time dynamical systems. It was first proposed as a simplified version of the Lorentz model. It is formed by using the following equation [27] to map a point (x_n, y_n) to the next point.

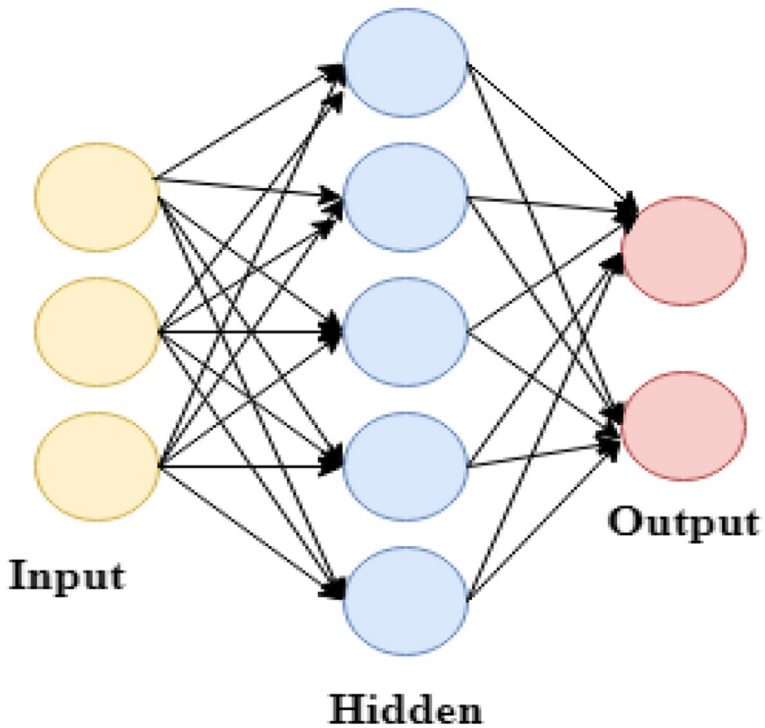


Fig. 3 Artificial neural network

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

$$x_{n+1} = \beta x_n \tag{3}$$

In Eqs. (2) and (3), x_n and y_n are the current positions, and x_{n+1} and y_{n+1} are the subsequent positions. The primary values of x_n and y_n determine the succeeding point in the initial conditions. Slight variations in the initial conditions x_n and y_n can significantly influence the final map. The traditional Henon map employs values of $\alpha = 1.4$ and $\beta = 0.3$, which distort the outcomes. A change in both values changes the characteristics of the resulting graph, which may no longer be chaotic [28, 29]. The Henon map model is frequently used in image encryption as a broadcast technique or as a keystream generator to change pixel values in an image. This chaos graph requires two initial values (x_0 and y_0). Each iteration yields new x_n and y_n values, which are then used to set the threshold. After being transformed to a bit value (0 or 1), this threshold will be converted to grayscale; the grayscale value for each pixel up to the chaos map is $m \times n$ size.

Proposed discrete memristor (D.M.)-based logistic map with DNN model

Logistic map

Logistic maps are also known as wormhole models. A logistic map is a simple, chaotic map in mathematical terms. Its mathematical expression is as follows:

$$x_{i+1} = \mu x_i (1 - x_i) \tag{4}$$

Where xϵ 0, 1 and $\mu\epsilon$ 0, 4 are logistic parameters. When xϵ 0, 1, the logistic map is chaotic. That is, the sequence produced by the logistic map's action on the initial condition x_0 is non-periodic and does not converge. Beyond this range, the generated sequence must connect to a particular value $3.5699456 < \mu \leq 4$. When the above condition is approximately 4, the values developed iteratively follow a pseudo-random distribution. After a certain number of iterations, other values are generated. The deal will then tend to converge on a single value. The sensitivity of chaotic systems to initial conditions is their defining feature. These sequences are known as chaotic sequences.

DM-based logistic map mathematical model

This section incorporates discrete memristors into logical maps and generates DM-based logistic maps. The D.M. model's input is set to the sequence x_i, and its output is shown in the formula (5).

$$output_i = x_i . Amp . \cos\left(q_0 + k \sum_{j=0}^{i-1} x_j\right), \tag{5}$$

Where the output is a sequence as well, let be the D.M. (i.e., the discrete memristor output) multiplied by the x_i term in equation (1- x_i) (4). The mathematical model for DM-based Logistics Mapping is as follows:

$$x_{i+1} = \mu . x_i . \left(1 - x_i . output_i\right) = \mu . x_i . \left(1 - x_i . x_i . Amp . \cos\left(q_0 + \mathrm{k} . \sum_{\mathrm{i}=0}^{\mathrm{n}-1} \mathrm{x_i}\right)\right) \tag{6}$$

Among them, μ is the system control parameter, k is the memristor parameter, and q_0 is the initial value of the Memristor. Set Amp to 1, then open the accumulator on the D.M. in order, and the logistic map based on D.M. can be written as follows:

$$\begin{cases} x_{i+1} = \mu . x_i . (1 - x_i . x_i . coscos\ (q_0 + k . w_i)) \\ w_{i+1} = w_i + x_i \end{cases} \tag{7}$$

Where $w_0 = 0$. The state of the DM-based logistic diagram is determined by μ, k, and q_0. If $k = 0.0001$ is set, the mapping formula (7) is modified using the discrete memristor formula (6). This article examines trajectories, Lyapunov exponents, bifurcation graphs, and complexity analysis relating to the dynamic behavior of DM-based logistic graphs. Figure 4 depicts the Simulink model based on the D.M. logistic graph. The unit delay block and unit delay one block represent x_i and w_i, respectively, and can set the sequence's initial value. The gain block represents the parameter k. The sequence x_i can be seen in the scope block. The constant block represents the initial q_0 Memristor and the system parameter μ. Driving delay blocks, gain blocks, and continuous blocks can all be used to control the map's state.

Hyperchaos in memristive logistic map

To demonstrate the dynamics of memristive logic graphs, we investigate the dynamic behavior based on control parameters in terms of bifurcation graphs, dynamic graphs, and phase-plane graphs. The internal parameters of the discrete Memristor are set to $a = -1$, $b = 1$, and the initial state of the memristor logic map is set to (x0, q0) = (0.5, 0.5). Bifurcation plots are generated on a 2D parameter plane by detecting the cycle number of a discrete map iteration sequence. Figure 5a depicts the bifurcation plot of the memristive logistic map for Fig. 5a shows the bifurcation plot of the memristive Logistic map for k∈ [1.2, 2] and μ ∈ [0.4, 0.4]. The parameter areas are colored differently based on the cycle number of iterative sequences. Mainly, white represents unbounded behavior, red denotes chaos, orange denotes multi-period, dark blue denotes stable point, and other colors denote period-2, period-3, and period-8, respectively.

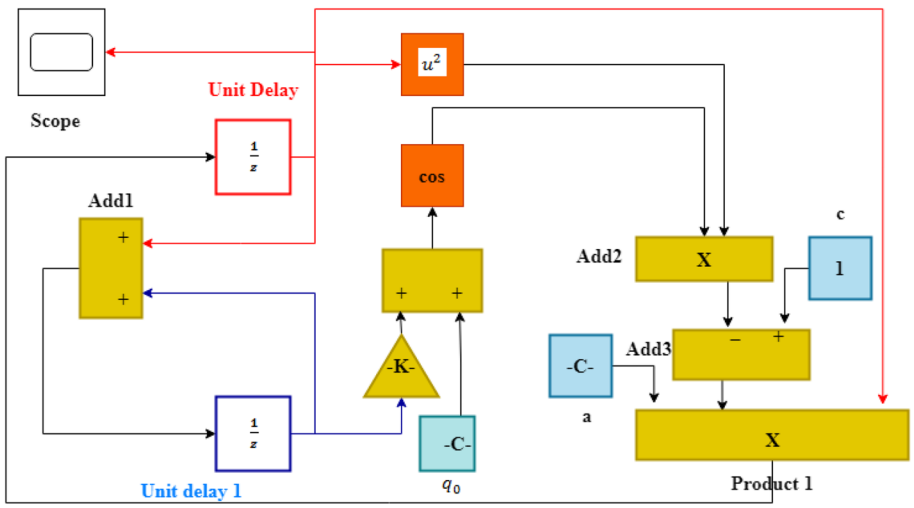


Fig. 4 Simulink model of DM-based Logistic map

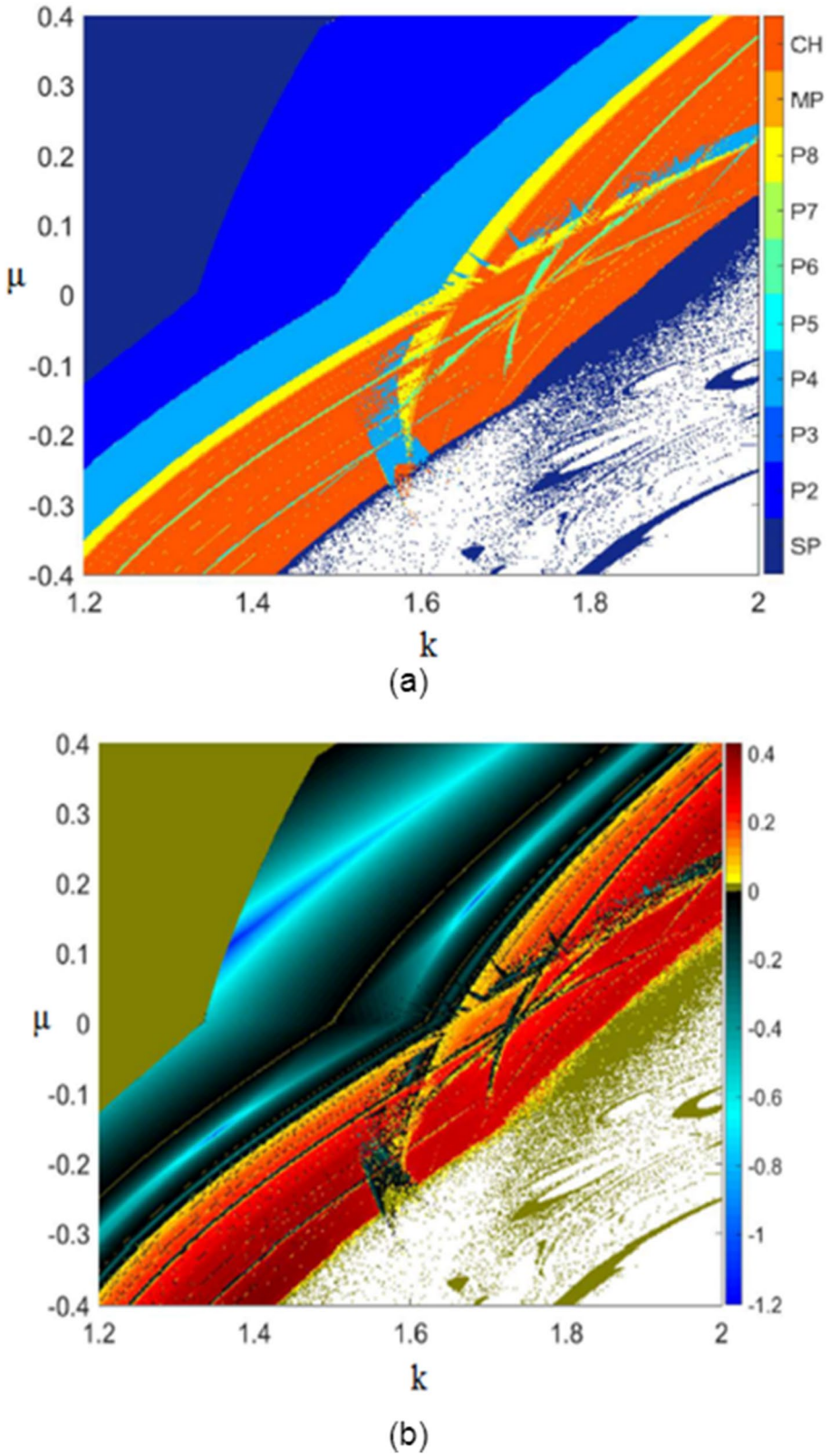


Fig. 5 **a** 2D bifurcation plot according to the cycle number of iterative sequences. **b** 2D dynamical map by computing the LLE of iterative sequences

Figure 5b shows the LLE of the memristive logistic plot of the 2D bifurcation graph in Fig. 5a under the same parameter region, with different LLEs colored differently. As a result, the dynamic graph in Fig. 5b can also be used to characterize the dynamic behavior of the memristive logic graph, which is a valuable supplement to the bifurcation graph in Fig. 5a.

It should be noted that the white areas represent unbounded behavior. In summary, the memristive logistic map can exhibit complex dynamical behaviors determined by the k and μ.

Deep neural network

A neural network is a machine that simulates how the brain performs specific tasks. DNN generates matrix code from blueprints. The DNN generates encoded weight and bias matrices for the first diffusion step at the end of this training process. Deep neural networks are used for encryption and decryption. DNNs are used in deep learning. DNNs are a type of deep neural network that is commonly used to analyze visual images. Individual neurons respond to stimuli only in a small area of the visual field known as the receptive field. The receptive fields of the neurons overlap to cover the entire field of view.

When compared to other image classification algorithms, DNNs require very little preprocessing. DNNs differ from traditional neural networks in their architecture. Ordinary N.N.s process input information using several hidden layers. Each layer contains a set of neurons, and each layer is fully connected to all of the neurons in the previous layer. In the final stage, there is a final fully connected layer, the output layer, representing the prediction.

Algorithm: Image encryption using deep neural network

Step 1: The first input sequence generates a chaotic series. The logistic map will then be used to create the messy line.

Step 2: Create a DNN output for creating a DNN network that uses chaotic sequences to calculate weights. DNN extracts features from images automatically. This effectively uses information from neighboring pixels to convolutionally down-sample the image and then use the prediction layer at the end. As a result, it is more accurate.

Step 3: At this point, the image is encrypted with the logistic map algorithm. To protect itself from plain text attacks, a logistic map generates smooth image histograms [30]. Figure 6 shows the DNN neural structure Fig. 7.

Image encryption using discrete memristor-based logistic map with DNN

As shown in Fig. 8, the suggested encryption scheme encrypts images using chaos and deep neural networks. There are two groups of images to be encrypted. 80% of the original images are used for pattern training, with the remaining 20% for pattern testing. Each pattern is normalized because the pixel values are relatively high. This can be accomplished with the MATLAB Signal Processing Toolbox's "mapminmax" function. Two chaotic logic graphs are used in the proposed algorithm to achieve image encryption. Divide the image to be encrypted $I\ m \times n$ into four non-overlapping subimages $A_{m'Xn}$. The suggested encryption method employs a diffusion and substitution

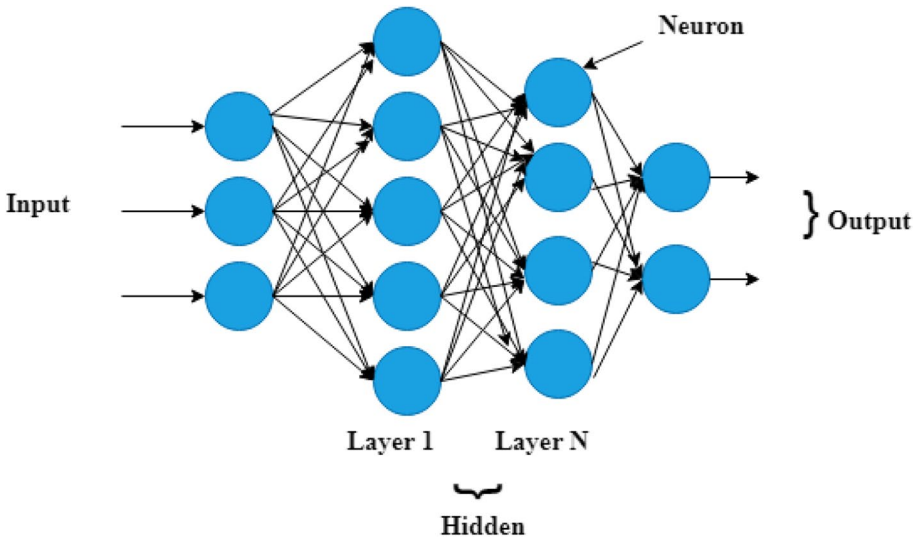


Fig. 6 Deep neural network

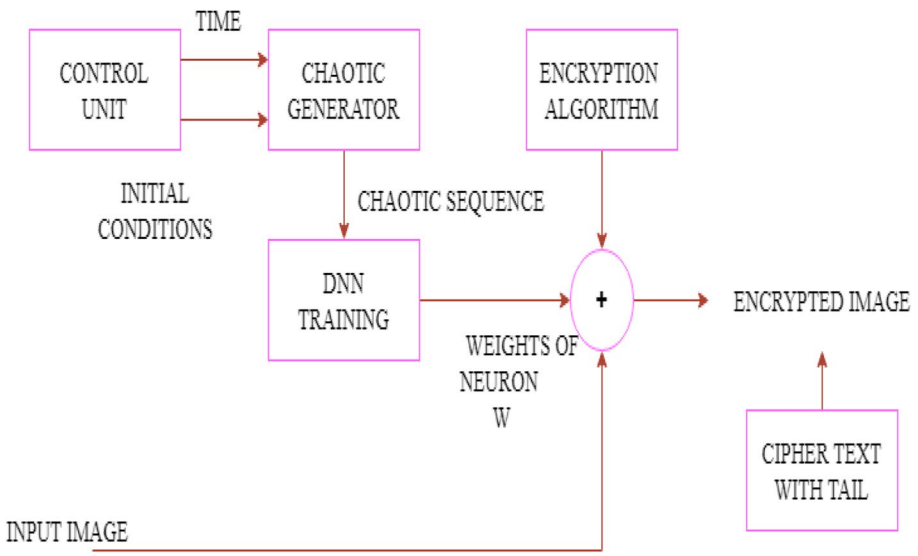


Fig. 7 Image decryption

mechanism. This section aims to generate matrix codes from ordinary images for the first step of the broadcast operation. The weights wi are added to the DNN using a discrete memristor-based logistic map generator. Chaotic systems exhibit large-scale emergence in unpredictable but deterministic ways. Common patterns can emerge when the exact location is unreliable and caused by a highly sensitive dependence on the system's initial conditions. Image encryption is appropriate for chaotic systems because of their high sensitivity to initial needs, randomness, unpredictability, and topological mixing.

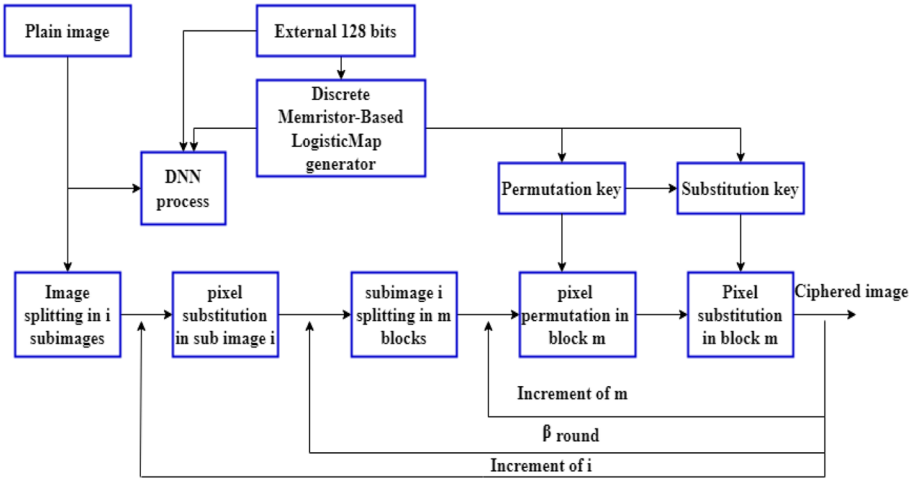


Fig. 8 Overall block diagram of the proposed method

Results and discussion

The effectiveness of the encryption schemes described in Section 3 is compared using the following metrics: correlation coefficient, histogram analysis, encryption entropy, differential measure, and encryption speed.

Figure 9 depicts the output of the color images used to evaluate the suggested encryption method. The evaluation was performed on various real-time test images with resolutions ranging from 1080 × 1080 to 4320 × 4320.

Histogram analysis

Histogram analysis demonstrates encryption algorithms' superior substitution and diffusion properties. We examine the histograms of several simple images and the ciphertext images obtained using the abovementioned method. Figure 10a, b depicts a histogram analysis of the proposed image encryption method. The encrypted image histogram's uniform distribution indicates the method's high quality.

Correlation coefficient

Statistical analyses, such as correlation coefficients, quantify the relation among adjacent pixels in an image. The correlation between two adjacent pixels in a standard image is always high in the horizontal, vertical, or diagonal direction, as calculated by the equation

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{8}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} x_i - E(x_i)^2 \tag{9}$$

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - Ex_i)(y_i - E(y_i) \tag{10}$$

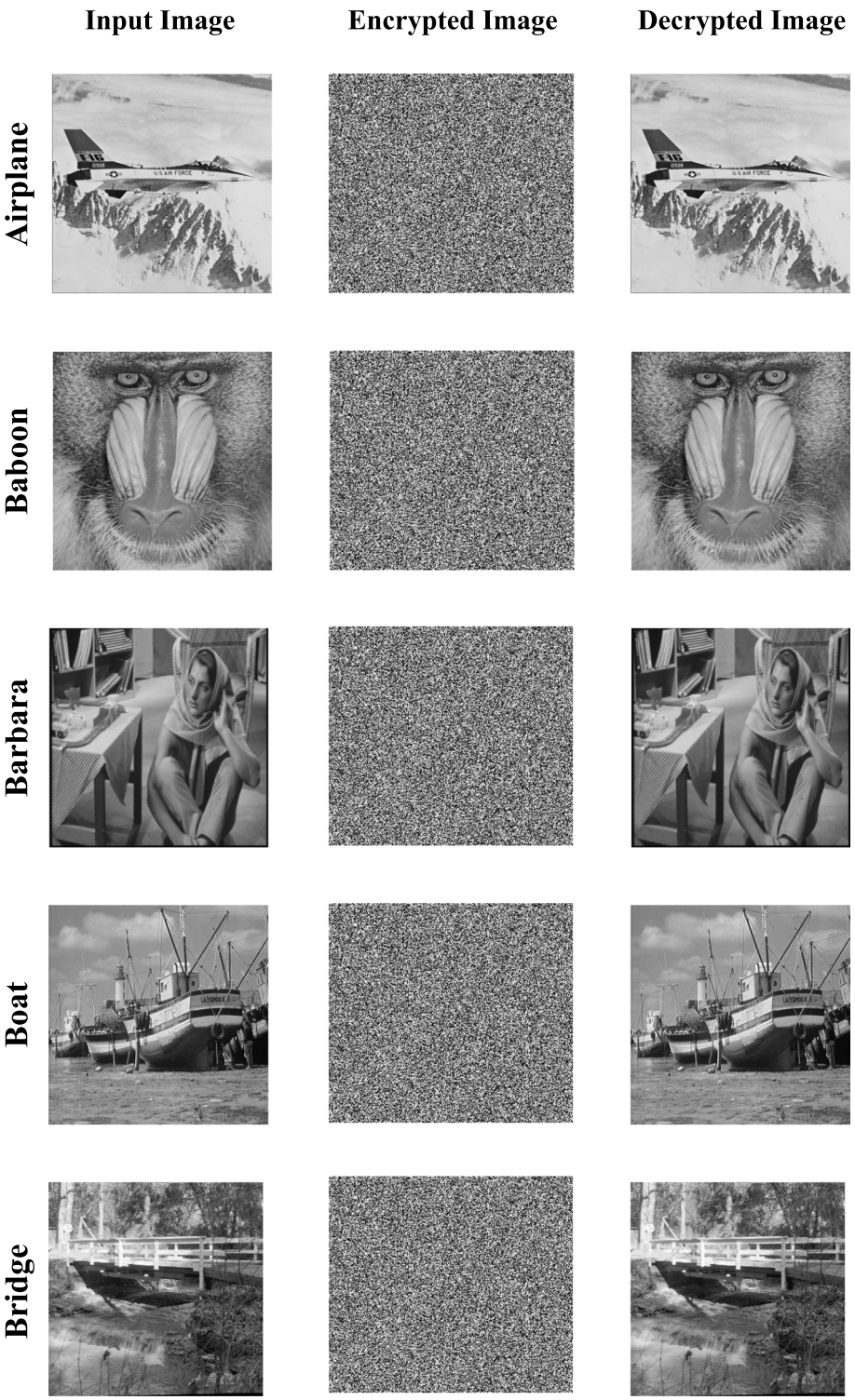


Fig. 9 Visual outcomes for sample real-time image

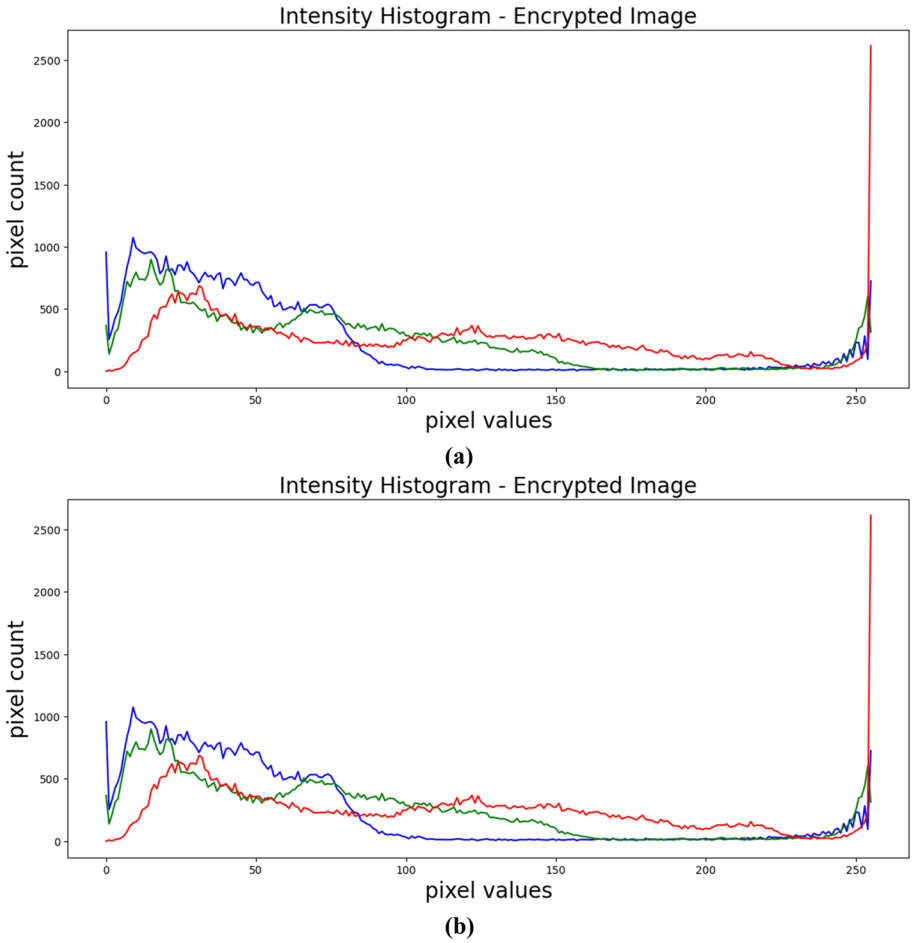


Fig. 10 **a** histogram analysis of the plain image. **b** Histogram analysis of the encrypted image

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{11}$$

Where x and y are two adjacent grayscale values in the image, $E(x)$ and $D(x)$ are the desired intensity and variance, respectively. The plain image's correlation coefficient is typically high (almost 1). Table 1 displays the results of the proposed methods discussed above using real-time standard grayscale grayscale images. The logistics generated by the DNN method generate more variations compared to the other two methodologies, as shown in the table. Figure 11 depicts the correlation graphs of the original and encrypted images.

Differential measures

To defend against differential attacks, any change to the plaintext image causes the encrypted image to change significantly. This is accomplished through the use of two commonly used measures. NPCR and UACI, to be specific. When only one-pixel changes in the raw image, NPCR represents the rate of change in the number of pixels in the ciphertext. Uniform average variation intensity (UACI) calculates the average intensity of the difference between standard and encrypted images. The NPCR value must

Table 1 Correlation coefficient factor

Algorithm	Horizontal	Vertical	Diagonal
Chaotic map	0.0007	0.00271	0.03861
DNN	− 0.00094	0.0041	0.00043
Arnold cat map with artificial neural network(ACM-ANN)	− 0.08044	− 0.0422	0.085674
Henon map with artificial neural network (HM-ANN)	0.000177	− 0.00045	− 0.00103
logistic map with deep neural network (LM-DNN)	− 0.003678	− 0.00011	− 0.00044
Proposed discrete memristor-based logistic map with deep neural network	− 0.00236	− 0.00008	− 0.00032

always be in the 99% range, and the UACI value must always be in the 33% range, indicating the algorithm's sensitivity.

$$\mathrm{NPCR} = \sum_{\mathrm{i,j}} \frac{\mathrm{D(i,j)}}{\mathrm{M} \times \mathrm{N}} \tag{12}$$

$$\mathrm{UACI} = \frac{1}{\mathrm{M} \times \mathrm{N}} \left[\sum_{\mathrm{i,j}} \frac{\mathrm{D(i,j)}}{255} \right] \times 100\% \tag{13}$$

When simple variations to the plaintext image can significantly alter the cypher image, differential attacks become ineffective. Significantly greater NPCR values are needed for a perfect encryption scheme. NPCR plots for various encryption methods are shown in Fig. 12. These values are compared in Tables 2 and 3. As these tables show, all the compared techniques are up to date and thus resistant to various differential attacks. Figure 13 depicts the UACI graph for different encryption methods.

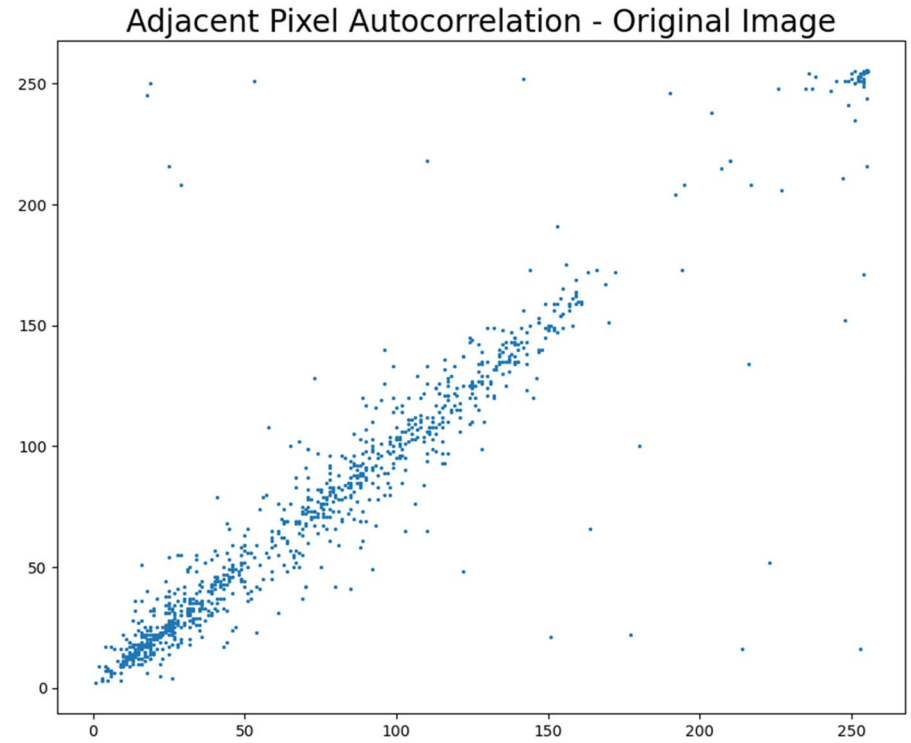
Encryption entropy

Shannon developed the concept of information entropy. It has numerous applications, including lossless compression, statistical inference, and encryption algorithms. It has recently been used in many subfields, such as machine learning, physics, and biology. Information entropy is a measure of ambiguity related to a random event that describes how much information is in the event. The greater the uncertainty or randomness of an event, the greater its information entropy. The information source X has a length of L.

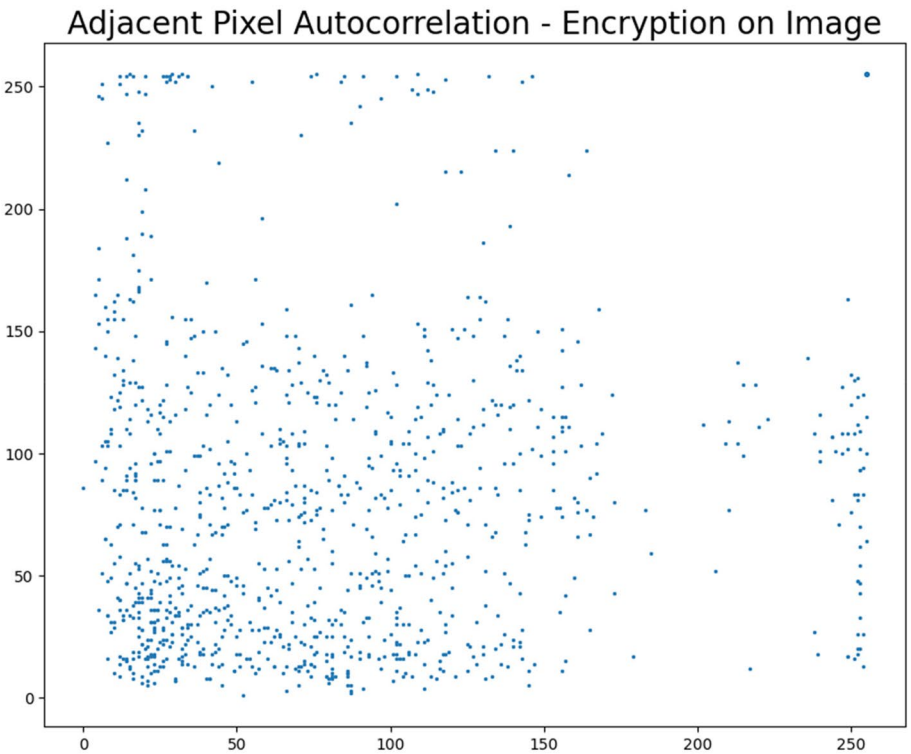
$$H(x) = -\sum_{i=0}^{i=l-} p(x_i) \log_2(p(x_i)) \tag{14}$$

Where $p(x_i)$ is the probability that it will occur, x emits 2^8 symbols with the same chance for a truly random data source, $p(x_i) = \frac{1}{2^8}$, i.e., $X = (x0, x1, \ldots, x2^8)$. i.e., $X =$ (x0, x1,..., x28).

Using Eq. (14), we calculate the information entropy and get H.X. = 8. Because the database rarely produces random messages, its entropy value is usually less than 8. When data are encrypted, they should ideally have an entropy of 8. If the data entropy of the symbols generated by the image encryption system is less than 8, there is predictability, which poses a security risk to the system.



(a)



(b)

Fig. 11 **a** Correlation plot of the original image. **b** Correlation plot of the encrypted image

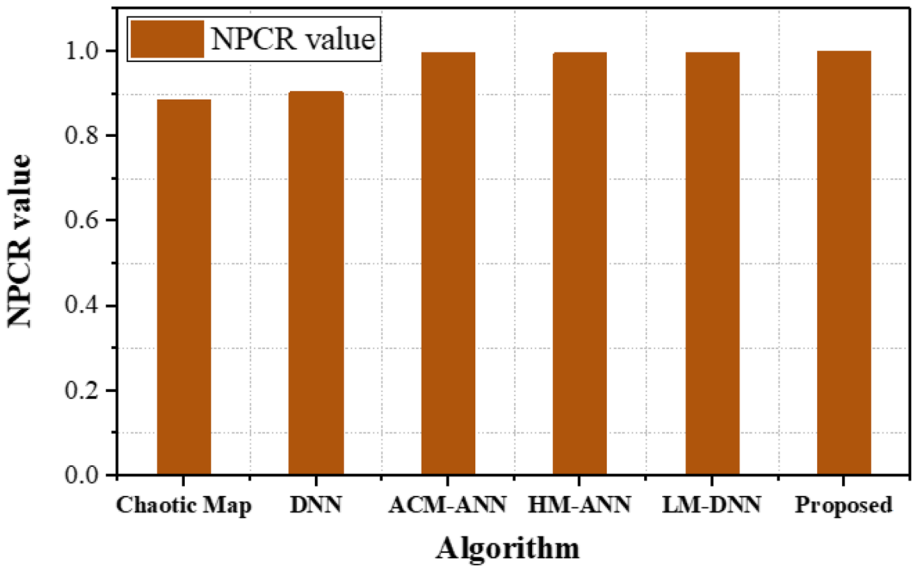


Fig. 12 NPCR plot of the different encryption methods

Table 2 NPCR (%)

Algorithm	NPCR value
Chaotic map	0.8867
DNN	0.9036
Arnold cat with artificial neural network(ACM-ANN)	0.9952
Henon map with artificial neural network(HM-ANN)	0.9964
logistic map with deep neural network(LM-DNN)	0.9977
Proposed discrete memristor-based logistic map with deep neural network	0.9995

Table 3 UACI (%)

Algorithm	UACI value
Chaotic map	0.3267
DNN	0.3301
Arnold cat with artificial neural network(ACM-ANN)	0.3345
Henon map with artificial neural network(HM-ANN)	0.3356
logistic map with deep neural network(LM-DNN)	0.3367
Proposed discrete memristor-based logistic map with deep neural network	0.3598

The entropy values for the algorithms in the discussion are shown in Table 4. The theoretical entropy for a 256-level grayscale grayscale image is 8 bits. However, in practice, achieving this ideal value is impossible. Encryption algorithms are acceptable up to the nearest value of 8. Table 4 shows that the DNN method's discrete Memristor-based logistic map outperforms the other methods. Figure 14 shows the entropy analysis of the three different encryption methods.

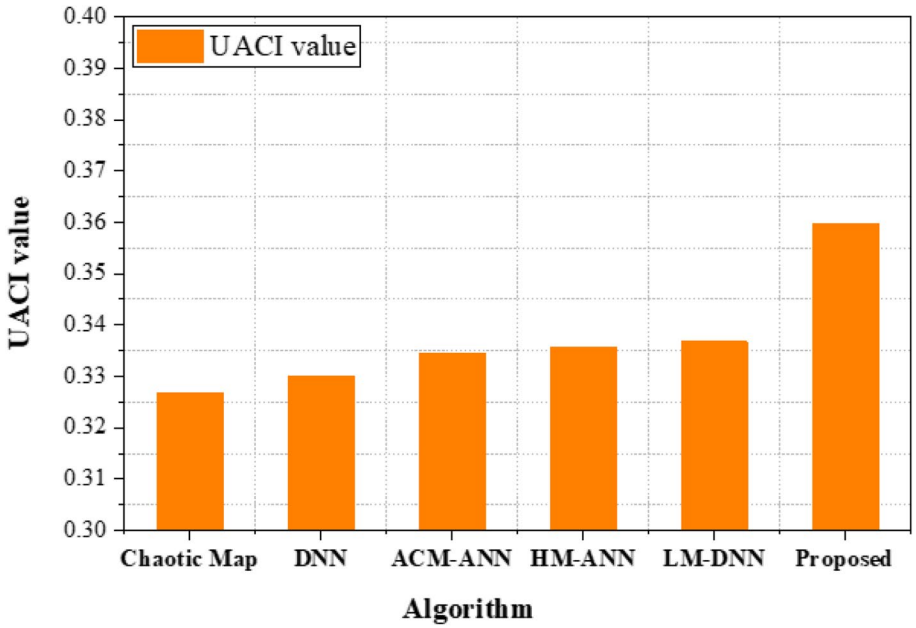


Fig. 13 UACI plot of the different encryption methods

Encryption speed

The time it takes to encrypt an image is another helpful tool for evaluating an algorithm's efficiency. The execution time in this survey will be measured in real-time in CPU cycles. Table 5 shows the algorithm's execution time for comparing standard Lena images of size 512 × 512. The discrete memristor-based logistic map using the DNN method requires less processing time. Figure 15 depicts the encryption speed graph for various encryption methods.

Error metric analysis

A set of test photos is subjected to the technique, which produces encrypted versions, which are subsequently decrypted, as part of an error matrix study for the "an efficient image encryption algorithm using discrete memristor-based logistic map with deep neural network". to evaluate true positives, true negatives, false positives, and false negatives—a measure of algorithm performance—a confusion matrix is made. In addition to

Table 4 Entropy

Algorithm	Original image	Cypher
Chaotic map	6.914667	7.892310
DNN	6.914667	7.923642
Arnold cat with artificial neural network(ACM-ANN)	6.914667	7.901581
Henon map with artificial neural network(HM-ANN)	6.914667	7.980477
logistic map with deep neural network(LM-DNN)	6.914667	7.990304
Proposed discrete memristor-based logistic map with deep neural network	6.914667	7.997231

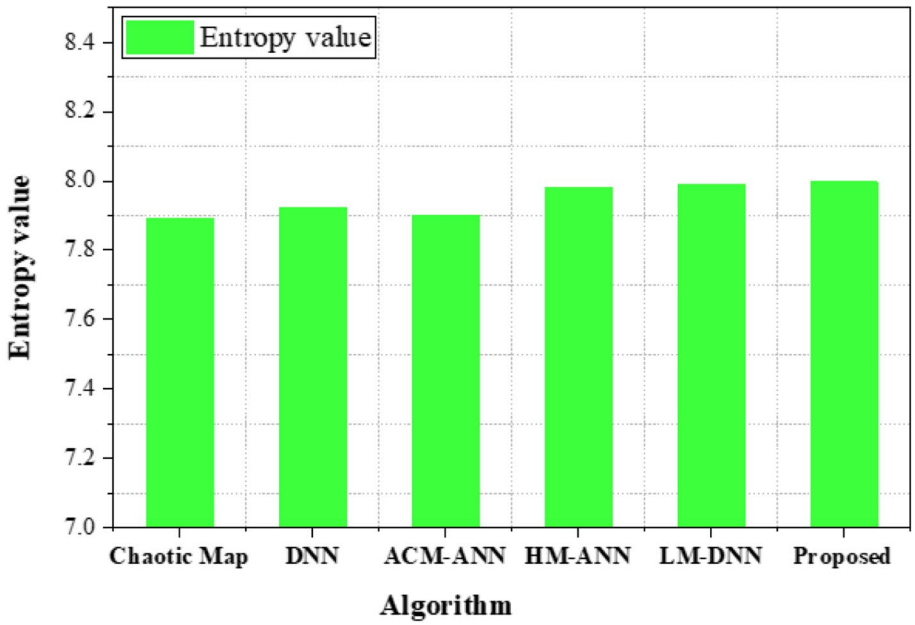


Fig. 14 Entropy analysis of the different encryption methods

Table 5 Encryption speed

Algorithm	Encryption speed (seconds)
Chaotic map	0.5870
DNN	0.6033
Arnold cat with artificial neural network (ACM-ANN)	0.6421
Henon map with artificial neural network (HM-ANN)	1.06
logistic map with deep neural network (LM-DNN)	0.3023
Proposed discrete memristor-based logistic map with deep neural network	0.2576

the visual evaluation of decrypted images, performance metrics like accuracy, precision, recall, and F1-score are measured. Through this process, the encryption and decryption capabilities of the method are assessed and could result in more optimization Table 6.

Performance comparison analysis

The entropy, NPCR, and UACI values of the suggested encryption method are compared with those of other current algorithms available in the literature [31–38]. Table 7 lists the estimated values. It is clear from the evaluated values that the suggested encryption scheme is resistant to both statistical and differential assaults.

Randomness validation

The unique way our performance analysis assesses the effectiveness and security of our suggested picture encryption technique makes it stand out. We understand how critical it is to place our findings in the perspective of the most recent developments in the area.

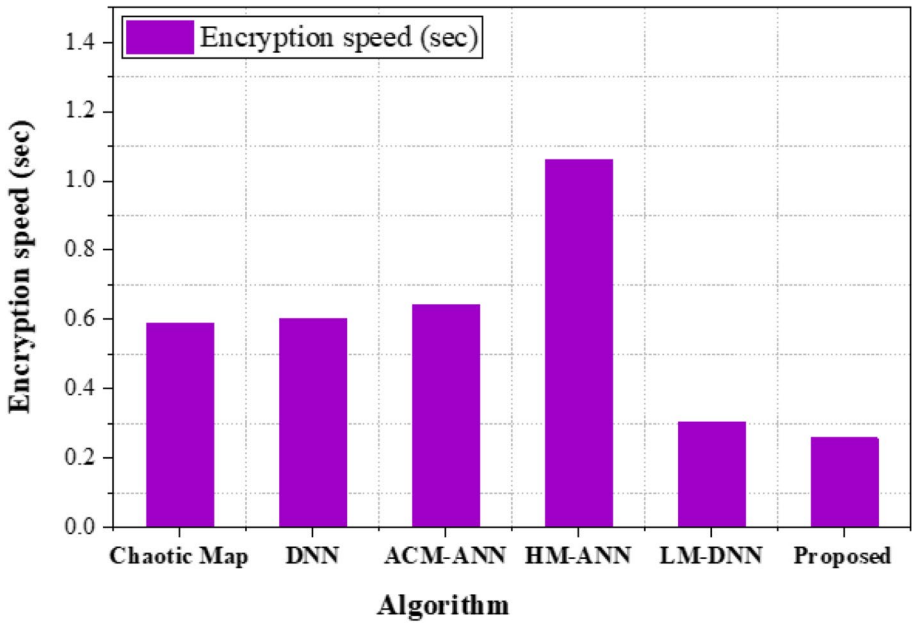


Fig. 15 Encryption speed plot of the different encryption methods

Table 6 MSE, PSNR, and SSIM values for the encrypted images

S.No	Image	MAP	PSNR (in dB)	SSIM
1.	Airplane	7654.84	8.9180	0.0132
2.	Baboon	7781.23	8.9828	0.0123
3.	Barbara	8243.78	8.6968	0.0078
4.	Boat	8090.04	7.5766	0.0154
5.	Bridge	6998.87	8.2344	0.0104

Our method is unique in that it uses a deep neural network (DNN) for picture encryption along with a discrete memristor-based logistic map (DMLM). We are sure that this combination offers unique advantages in terms of security, adaptability, and computational efficiency—strengths that our comparative analysis will make clear. We want to highlight our approach's amazing benefits and contributions by comparing it to these recent articles and proving how effective it is at protecting sensitive image data in a range of application scenarios (Table 8).

Discussion

In this study, we have presented an efficient image encryption algorithm that combines a discrete memristor-based logistic map with a deep neural network (DNN). Our research addresses the pressing need for robust image encryption methods in an era where data security is paramount. The algorithm's core methodology involves the discrete memristor-based logistic map, which introduces a unique chaotic element to the encryption process and the integration of a DNN to enhance its capabilities. Our experimental results have demonstrated the algorithm's effectiveness, emphasizing its robust security,

Table 7 Performance comparison table

S.NO	Method	UACI	NPCR	Entropy
1.	Proposed method	35.9832	99.9541	7.997231
2.	[31]	33.4935	99.6230	7.997214
3.	[32]	33.4352	99.6543	7.997216
4.	[33]	33.4597	99.7213	7.997226
5.	[34]	33.7436	99.6981	7.997229
6.	[35]	34.5678	99.8735	7.997227
7.	[36]	34.5871	99.7986	7.997219
8.	[37]	33.4294	99.5972	7.997203
9.	[38]	33.4364	99.6092	7.997223

high-quality image preservation, and computational efficiency. We have rigorously evaluated its performance, utilizing statistical analyses such as entropy, correlation coefficients, and error metrics like MSE and PSNR. Notably, this algorithm showcases resistance to various attack scenarios, which is a pivotal characteristic in protecting sensitive image data.

Moreover, our algorithm's distinctive feature lies in the fusion of the discrete memristor-based logistic map and the deep neural network, significantly enhancing its efficiency and security. This amalgamation of innovative technologies underscores its unique contribution to image encryption. Our work has practical implications for securing various applications, including medical image transmission, confidential data storage, and secure communication channels. However, we acknowledge that there may be further areas for refinement and improvement, which opens doors to future research avenues. In conclusion, our research underscores the importance of image encryption and offers a novel and efficient solution that holds promise in safeguarding digital images across various domains.

Table 8 Randomness evaluation of encrypted image by NIST test suite

Statistical test	Generated key		
	Pr	*P* value	Results
Frequency	0.275709	10	Pass
Block frequency	0.249284	9	Pass
Cumulative sums	0.867692	9	Pass
Runs	0.275709	9	Pass
Longest run	0.368150	10	Pass
Rank	0.262249	10	Pass
FFT	0.062821	10	Pass
Non-overlapping template	0.348970	10	Pass
Overlapping template	0.249298	9	Pass
Universal	0.759756	9	Pass
Approximate entropy	0.739918	10	Pass
Random excursions	0.350485	9	Pass
Random excursions variant	0.055361	9	Pass
Serial	0.071177	10	Pass

Several limitations should be noted in our paper on the "efficient image encryption algorithm using discrete memristor-based logistic map with deep neural network." Utilizing a deep neural network adds computational overhead, and our method might require hardware. More research is needed to determine the algorithm's resilience to future assaults, key distribution and administration, flexibility to handle various data kinds, and applicability for contexts with limited resources. Furthermore, in real-world applications, user-friendliness, legal compliance, and generalizability to different image kinds should be given consideration.

Conclusions

The suggested system employs a novel algorithm to perform image security using DNNs. The objective is to obligate the encryption technique to manipulate the trapdoor function in the cryptosystem. Discrete memristor-based logic maps are designed as an application based on primitive, chaotic maps and discrete memristors. This paper compares the proposed algorithm's performance to three other image encryption algorithms. Performance metrics such as NPCR, UACI, correlation coefficient, differential metrics, entropy, and encryption speed are evaluated using standard test images. By combining these properties, the proposed cryptosystem avoids all of the cryptographic weaknesses of previous chaos-based cryptosystems. Various security analyses are performed on the new algorithm, and the simulation results show that the encryption and decryption effects are excellent and the algorithm has good security and robustness.

Abbreviations

DNN	Deep neural networks
ANN	Artificial neural network
NPCR	Number of pixels changing rate
ACM	Arnold cat map algorithm
DM	Discrete memristor

Acknowledgements
Not applicable.

Authors' contributions
BSK wrote the original draft and worked on the software. RR worked on the software. BSK defined the methodology, and reviewed and edited the manuscript. RR supervised the work. All authors read and approved the final manuscript.

Funding
No funding was received by any government or private concern.

Availability of data and materials
Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 4 September 2023 Accepted: 21 December 2023
Published online: 12 February 2024

References

1. Kalpana V, Vijaya Kishore V, Satyanarayana RVS (2023) MRI and SPECT brain image analysis using image fusion. In: Marriwala, N., Tripathi, C., Jain, S., Kumar, D. (eds) Mobile radio communications and 5G networks. Lecture notes in networks and systems, vol 588. Springer, Singapore. https://doi.org/10.1007/978-981-19-7982-8_48

2. Vijaya Kishore V, Kalpana V (2020) Effect of Noise on Segmentation Evaluation Parameters. In: Pant, M., Kumar Sharma, T., Arya, R., Sahana, B., Zolfagharinia, H. (eds) Soft computing: Theories and applications. Advances in intelligent systems and computing, vol 1154. Springer, Singapore. https://doi.org/10.1007/978-981-15-4032-5_41
3. Vijaya Kishore V, Kalpana V (2020) ROI segmentation and detection of neoplasm based on morphology using segmentation operators. In: Hitendra Sarma, T., Sankar, V., Shaik, R. (eds) Emerging trends in electrical, communications, and information technologies. Lecture notes in electrical engineering, vol 569. Springer, Singapore. https://doi.org/10.1007/978-981-13-8942-9_41
4. Stallings W (2010) Cryptography and network security: principles and practice, vol 998. Prentice Hall
5. David VARS, Govinda E, Ganapriya K, Dhanapal R, Manikandan A (2023) An automatic brain tumors detection and classification using deep convolutional neural network with VGG-19," 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). Coimbatore, India. pp. 1–5. https://doi.org/10.1109/ICAECA56562.2023.10200949
6. Lian S, Liu Z, Ren Z, Wang H (2006) Secure advanced video coding based on selective encryption algorithms. IEEE Trans Consum Electron 52(2):621–629
7. Xue X, Palanisamy S, A M, Selvaraj D, Khalaf OI, Abdulsahib GM (2023) A Novel partial sequence technique based Chaotic biogeography optimization for PAPR reduction in eneralized frequency division multiplexing waveform. Heliyon 9(9):e19451. https://doi.org/10.1016/j.heliyon.2023.e19451
8. Cheng H, Li X (2000) Partial encryption of compressed images and videos. EEE Trans Signal Process 48(8):2439–2451
9. Lian S (2008) Multimedia content encryption: techniques and applications. Auerbach Publications
10. Rodrigues J, Puech W, Bors A (2006) Selective encryption of human skin in jpeg images. In: In *2006 International conference on image processing*. IEEE, pp 1981–1984
11. Ali R, Manikandan A, Xu J (2023) A novel framework of adaptive fuzzy-GLCM segmentation and Fuzzy with capsules network (F-CapsNet) classification. Neural Comput Applic. https://doi.org/10.1007/s00521-023-08666-y
12. Karpagalakshmi R, Tensing D, Kalpana A (2016) Image localization using deformable model and its application in healthinformatics. J Med Imaging Health Inform 6:1972-1976. https://doi.org/10.1166/jmihi.2016.1959
13. Balasubramani A, Kalaivanan K, Karpagalakshmi RC, Monikandan R (2008) Automatic facial expression recognition system. 2008 International Conference on Computing, Communication and Networking, Karur, India. pp. 1-5. https://doi.org/10.1109/ICCCNET.2008.4787749
14. Yoon JH, Zhang J, Lin P, Upadhyay N, Yan P, Liu Y, Xia Q, Yang JJ (2020) A low-current and analog memristor with Ru as mobile species. Adv Mater 32:e1904599
15. Zhang Y, Ping Y, Zhang Z, Zhao G (2021) Recent advances in dimensionality reduction modeling and multistability reconstitution of memristive circuit. Complex 2021:1–18
16. Dai W, Xu X, Song X, Li G (2022) Audio encryption algorithm based on chen memristor chaotic system. Symmetry 14:17
17. Kalaiarasan D, Ahilan A, Ramalingam S (2023) A Harris Hawk optimization with chaotic map based image encryption for multimedia application. 11035 – 11057
18. Manikandan A, Ponni M (2022) An early prediction of tumor in heart by cardiac masses classification in echocardiogram images using robust back propagation neural network classifier. Braz Arch Biol Tech 65. https://doi.org/10.1590/1678-4324-2022210316
19. Maniyath SR, Thanikaiselvan V (2020) An efficient image encryption using deep neural network and chaotic map. Microprocess Microsyst 77:103134. https://doi.org/10.1016/j.micpro.2020.103134
20. Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. Image Vis Comput. 24(9):926–934
21. Annamalai M, Ponni Bala M (2023) Intracardiac mass detection and classification using double convolutional neural network classifier. J Eng Res 11(2A):272–280. https://doi.org/10.36909/jer.12237
22. Cangea O, Paraschiv N (2018) Chaos-based cryptography for color images. In: *2018 22nd International Conference on System Theory, Control and Computing (ICSTCC)*, pp 510–515. https://doi.org/10.1109/ICSTCC.2018.8540650
23. Balamurugan D, Seshadri A, Reddy P, Rupani A, Manikandan A (2022) Multiview objects recognition using deep learning-based wrap-CNN with voting scheme. Neural Process Lett 54:1-27. https://doi.org/10.1007/s11063-021-10679-4
24. Chen M, Ma G, Tang C, Lei Z (2020) Generalized optical encryption framework based on shearlets for medical image. Opt Lasers Eng 128:106026
25. Mishra Z, Acharya B (2020) High throughput and low area architectures of secure IoT algorithm for medical image encryption. J Inf Secure Appl 53:102533
26. Manikandan A, Madhu GC, Flora GD et al (2023) Hybrid advisory weight based dynamic scheduling framework to ensure effective communication using acknowledgement during encounter strategy in Ad-hoc network. Int J Inf. tecnol. https://doi.org/10.1007/s41870-023-01421-5
27. Chandramohan K, Manikandan A, Ramalingam S, Dhanapal R (2023) Performance evaluation of VANET using directional location aided routing (D-LAR) protocol with sleep scheduling algorithm. Ain Shams Eng J 102458. https://doi.org/10.1016/j.asej.2023.102458
28. Gopalan SH, Ashok J, Manikandan A et al (2023) Data dissemination protocol for VANETs to optimize the routing path using hybrid particle swarm optimization with sequential variable neighbourhood search. Telecommun Syst. https://doi.org/10.1007/s11235-023-01040-2
29. Reka R, Manikandan A, Venkataramanan C et al (2023) An energy efficient clustering with enhanced chicken swarm optimization algorithm with adaptive position routing protocol in mobile adhoc network. Telecommun Syst. https://doi.org/10.1007/s11235-023-01041-1
30. Venkataramanan C, Ramalingam S, Manikandan A (2021) LWBA: Lévy-walk bat algorithm based data prediction for precision agriculture in wireless sensor networks. J Intell Fuzzy Syst 41:2891–2904. https://doi.org/10.3233/JIFS-202953

31. Venkataramanan C, Sarojini R, Porchelvi N, VMSN PK, Ramalingam S (2022) Dual-band Micro-Strip Antenna using Split Ring Resonators for ISM Bands," 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS). Trichy, India. pp. 1424–1429. https://doi.org/10.1109/ICAISS55157.2022.10010915
32. Karpagalakshmi RC, Vijayalakshmi P, Gowsic K et al (2021) An effective traffic management system using connected dominating set forwarding (CDSF) framework for reducing traffic congestion in high density VANETs. Wireless Pers Commun 119:2725–2754. https://doi.org/10.1007/s11277-021-08361-y
33. Banu SA, Al-Alawi AI, Padmaa M, Priya PS, Thanikaiselvan V, Amirtharajan R (2023) Healthcare with datacare—a triangular DNA security. Multimed Tools Appl:1–18
34. Nilabar Nisha U, Manikandan A, Venkataramanan C, Dhanapal R (2023) A score based link delay aware routing protocol to improve energy optimization in wireless sensor network. J Eng Res. https://doi.org/10.1016/j.jer.2023.100115
35. Mahalingam H, Velupillai Meikandan P, Thenmozhi K, Moria KM, Lakshmi C, Chidambaram N, Amirtharajan R (2023) Neural attractor-based adaptive key generator with DNA-coded security and privacy framework for multimedia data in cloud environments. Mathematics 11(8):1769
36. Manikandan V, Amirtharajan R (2022) A simple embed-over encryption scheme for DICOM images using Bülban Map. Med Biol Eng Comput 60(3):701–717
37. Thenmozhi K, Rayappan JBB, Amirtharajan R, Praveenkumar P (2021) MUX induced ring oscillators for encrypted nano communication via quantum dot cellular automata. Nano Commun Netw 27:100338
38. Devi RS, Thenmozhi K, Rayappan JBB, Amirtharajan R, Praveenkumar P (2019) Entropy-influenced RNA diffused quantum chaos to conserve medical data privacy. Int J Theor Phys 58:1937–1956

Publisher's Note