IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 January 2024, accepted 8 January 2024, date of publication 12 January 2024, date of current version 24 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3353294

RESEARCH ARTICLE

A Faster and Robust Artificial Neural Network Based Image Encryption Technique With Improved SSIM

ASISA KUMAR PANIGRAHY[1,*], **SHIMA RAMESH MANIYATH**[2,*], **(Member, IEEE), MITHILEYSH SATHIYANARAYANAN**[3], **(Member, IEEE), MOHAN DHOLVAN**[4], **T. RAMASWAMY**[4], **SUDHEER HANUMANTHAKARI**[1], **(Member, IEEE), N. ARUN VIGNESH**[5], **S. KANITHAN**[6], **AND RAGHUNANDAN SWAIN**[7], **(Senior Member, IEEE)**

[1]Department of ECE, Faculty of Science and Technology (Icfaitech), ICFAI Foundation for Higher Education Hyderabad, Hyderabad, Telangana 501203, India
[2]Department of ECE, MVJ College of Engineering, Bengaluru, Karnataka 560067, India
[3]Research & Innovation Centre, MIT Square, SW14 8JZ London, U.K.
[4]Department of ECE, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana 501301, India
[5]Department of ECE, Gokaraju Rangaraju Institute of Engineering and Technology (GRIET), Hyderabad, Telangana 500090, India
[6]Department of CSE, Jain University, Bengaluru, Karnataka 562112, India
[7]Department of ETC, Parala Maharaja Engineering College, Berhampur 761003, India

Corresponding author: Asisa Kumar Panigrahy (asisa@ifheindia.org)

The Authors would like to acknowledge ICFAI Foundation for Higher Education Hyderabad (IcfaiTech), Hyderabad, India for the financial support and the access of the MATLAB tool for conduction of the research work. This work was supported in part by the MIT Square and Raj Square Charity Foundation, Department of Computer Science, University of Beira Interior, Covilhã, Portugal.

*Asisa Kumar Panigrahy and Shima Ramesh Maniyath contributed equally to this work.

ABSTRACT A robust image encryption process is still one of the most challenging tasks in image security owing to massive degree and sensitivity nature of information in the form of pixels. The hurdles include greater computational difficulty, information loss during encryption, universality, applicability of the approach, and less scalability. Many image encryption methods existing in literature merely encrypt a portion of the data. Therefore, we propose a robust, dynamic, and sophisticated technique to enhance the encryption process to make it difficult for an attacker to gain unauthorized access to the pixel data. The proposed system uses a novel analytical research methodology through dynamically harnessing the potential of neural network that offers better forward and backward secrecy, dynamic control, and automatic management unlike any existing system. The encryption procedure comprises of two levels, first level is confusion- permutation of input image and second level is diffusion by Bit XOR operation for secure transmission and storage of images. Finally, the encrypted image is used as a target for training the Artificial Neural Network (ANN) model. ANN trained values are used for final level of encryption to develop a Neural Network (NN)-based cryptosystem, where the crypto analyst or the cracker need to know the number of adaptive iterations and the final weights for the encryption and decryption systems to crack the system which offers higher degree of resiliency towards potential threats. Results and security analysis show that our algorithm has good encryption effect, ability of resisting exhaustive attack, statistical attack, and differential attack. The system performance after implementing the proposed method is compared with existing methods present in literature with respect to processing time and Structural Similarity Index Measure (SSIM). Our proposed method offers significant reduction in encryption time and is approximately 10-15% faster than others with SSIM of 0.002165, close to zero after encryption. It also successfully balances the image quality with higher image security and lower computational complexity.

INDEX TERMS Artificial neural network, encryption, image security, SSIM, NPCR, UACI, entropy, PSNR.

I. INTRODUCTION

Images are one of the categories of communication evidence that are regularly used and incorporated by many company

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Sharif.

management systems. Image data has the benefit of covering more multimedia data content with less memory, making information dissemination simpler. However, very often such important/private images are transferred over an unsecured communication channel [1]. In many fields, including video conferencing, medical imaging, industrial and military systems data security is crucial. Such applications demand a potential access to the signal to offer validation for the degree of vulnerability of images [2]. However, threats to such application will mean direct illegitimate access to the confidential and private information of the user as well as the data [3] [4]. Therefore, adequate image security is required to prevent unwanted access to crucial information. Data encryption is quite successful for upholding the integrity, confidentiality, and validity of the image [5]. It is a mechanism where simple and plain information is secured by using specific form of cryptographic approach. The original file after encryption can be accessed only if a specific decryption mechanism is applied. At present, various commercial applications over small and large scaled network make use of data encryption [6]. However, there are still some loopholes in existing data encryption mechanisms which calls for further scope of investigation. Currently, numerous security operations are carried out over image and adoption of robust neural network will incur less consumption of learning and processing time as it is fixed for images. It states better performance and control over time complexity compared to traditional encryption algorithms such as Rivest-Shamir-Adleman (RSA) [7], Advanced Encryption Standard (AES).

In the present manuscript, Section II presents existing research contributions in the field of image security. Section III identifies research scope. Section IV discusses the methodology that has been suggested as a remedy. The implementation of the algorithm is covered in Section V, which also includes a detailed analysis of the results and a comparison study. Briefs on contributions are offered at the end of Section VI along with closing remarks.

II. EXISTING RESEARCH CONTRIBUTION TOWARDS IMAGE SECURITY

A combination of sharing matrix and chaos-based encryption technique is a security solution that generates secret shares required to obtain the original data and is quite challenging to break by intruder [8]. The outcome shows that the mechanism is resistive towards brute-force attack and is found quite robust in protecting different types of images. It also provides the ability to recognize fake secret shares. Optical system's potential can also be exploited as a tool to improve image security [9]. It provides more effective secret key management and safeguarding the image from different key-based threats. Message-digest hashing is used over the input image through chaotic mapping [10]. This method uses one-time secret key mechanism which offers resistance from any pixel-based attacks on images. Usage of logistic map is also proven to offer better encryption performance [11]. An effective image encryption method can be a modified Lorenz chaotic system utilizing Arnold transformation with differential evolution to provide robust feature for encryption of image [12], [13]. In terms of security and better visual clarity the proposed techniques outperform all the other techniques. A computer-generated hologram-based image encryption technique has been revealed by Cao et. al. [14]. The original image is subjected to the encoding system where the hologram of the complex Fourier is subjected to the decomposition offering better security of image and video. Medical image security using encryption framework is developed using chaos theory [15]. The images are forwarded to cloud after encryption and decrypted at the other end. Cryptanalysis-based approach towards protecting multimedia data content consists of four phases to maintain the security level higher and efficient in avoiding various common attacks [16].

In the same way, Li et. al. has presented an image security scheme where lossy compression approach towards JPEG standard is utilized to offer a balance between encryption and compression [17]. The study outcome offers robust security properties assessed in the form of diffusive properties of the encrypted image. The work of Liu et. al. has offered a joint implementation of the chaos theory and secret key generation using random numbers [18]. The proposed strategy aims to create an efficient encryption method for image protection. The experimental findings show that the suggested crypto-system is reliable and efficient in terms of computational complexity and security. Multiple variants of image security techniques have also been developed using chaotic map with a combination of permutation and replacement approach. The study has also used a block-based encryption over chaotic map considering image blocking methods. The outcome exhibited faster encryption speed and higher level of security. It is quite a challenging task to achieve computational efficiency along with a robust security in chaotic-based implementation approach along with legacy encryption technique [19]. A unique scrambling mechanism using pixel using biological encoding mechanism along with bit-level scrambling is presented in Ref. [20]. Adoption of Mixed chaotic map is found to be even more effective for resisting attacks [21]. Apart from this, there is an evolution of various techniques towards image security. Recently, encryption with compression process is presented by Chuman et. al. [22], Rivest Shamir Algorithm by Zhang et. al. [7], Galois field encryption by Wang et. al. [23], compressive detecting by Ping et. al. [24], chaos synchronization by Li et. al. [25] and Ge et. al. [26], asymmetric image encryption by Luan et. al. [27]. Among the above literature, it is plausible that there are mainly three frequently used methodologies including chaotic map approach, typical cryptography approach, and compressive sensing. Two-dimensional enhanced logistic modular map (2D-ELMM) is a chaotic image encryption scheme based on vector-level operations with high encryption efficiency [28]. A high-quality color picture compression-encryption technique based on chaos and block permutation has the advantages of a high compression ratio, good image recovery quality, and a strong security level to fend off popular cryptographic assaults [29]. A novel image encryption strategy based on the memristive chaotic system by integrating dynamic DNA-level diffusion and bidirectional bit-level cyclic shift offers a high security level and can withstand a variety of attacks [30]. Nevertheless, a successful encryption system requires an incredibly light encryption mechanism; while a chaotic map improves encryption, it doesn't meet the security requirements of different dynamic attacks. Attribute based encryption is suitable for data protection in data outsourcing systems such as cloud computing [31]. A CPKEET scheme is proposed a round optimal attribute-based encryption with conditional equality test (RO-ABE-CET) high security level for data privacy protection in intelligent systems [32]. Image encryption scheme is proposed by combining 2D cascaded logistic map and permutation- substitution operations has improved the security level [41]. Additionally, Setiadi et. al. [42] proposed an image encryption technique Half-Inverted Cascading Chaos Cipheration (HIC3), designed to increase digital image security and confidentiality.

Development of encryption algorithm for securing image depends on multiple factors such as, level of sensitive information present within the image to be secured, location of storing the encrypted image, location of storage or generation of private/public keys for ciphering/deciphering and degree of resiliency towards threats. Although, such problems are critical, but there are various encryption mechanisms presented by Sankpal et. al. [33]; Kumari et. al. [34], Khan et. al. [35] that has offered solutions in highly specific means to such problems. However, certain essential problems remain unsolved in present time whereas, various new mechanism of image security exists.

III. PROBLEM IDENTIFICATION

The technical problems identified in existing literature are as follows:

- **More focus on security incorporation and less on cost:**
  Usually, encryption algorithms and approaches are highly iterative and demand a specific environment with wide availability of computational resources. Existing methods, however, provide higher security but also necessitate adequate computing resources for completing the work [7], [8], and [20]. Hence, security is offered at the cost of computational resources.
- **Usage of analytically complex approaches:**
  Usage of chaotic theory has been seen to be highly adopted at present times [11], [17], [18], [21], [36], [37], [38], [39]. However, all these approaches are associated with a problem that doesn't support dynamical system like encrypting streams of images. There is no evidence to prove that such mechanisms are cost effective and offers faster response rate.
- **Less Emphasis to Machine Learning approach:**
  Although, recursive in operation, utilization of machine learning approach is highly anticipated in all the upcoming and ubiquitous system owing to its beneficial points on performing analytical operation. Apart from this, it is also capable of offering an elite outcome and could assist in boosting the encryption performance. However, such facts remain undisclosed in existing approaches on image security.

Therefore, in this work emphasis is given to develop a cost-effective and computationally efficient model that could offer better form of resistance from lethal image attacks using machine learning algorithm.

IV. PROPOSED METHODOLOGY

The proposed study introduces a simple and computationally effective encryption mechanism with the assistance of neural network as demonstrated in Fig. 1. One-way features are one of the important characteristics of neural networks [40]. Firstly, it facilitates computing resultant from input but offers challenges in extracting input from resultants. This property acts as a good trapdoor function in securing the image after performing encryption and hence offers good forward and backward secrecy. maintaining validation of the data integrity. Secondly, by using any form of learning methods such as reinforcement or unsupervised, it is feasible to distinguish the adversarial operation from the normal operation. Thirdly, hashing is inevitable in encryption mechanism meant for authenticating the data integrity and it can be manipulated. Owing to shorter size of hash value, there is least computational complexity associated with it while performing encryption. This property offers a greater deal of security and robustness toward the encryption process of an image.

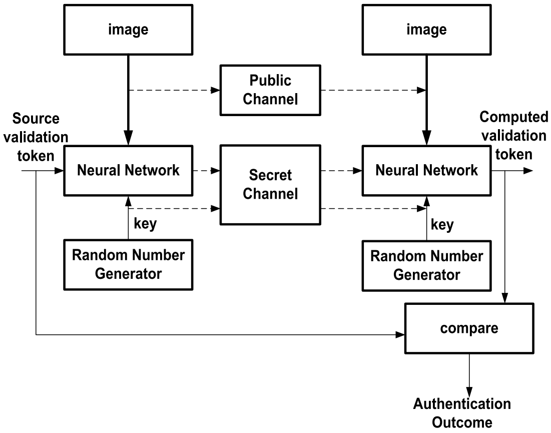


FIGURE 1. Proposed neural network in image security.

The proposed system constructs a secret attribute from input image, validation token, and a secret key that is given as an input to the neural network as shown in Fig. 1. It should be noted that size of this secret attribute is very much smaller than that of the original image. This renders simplification in either retaining or forwarding the secret attribute along

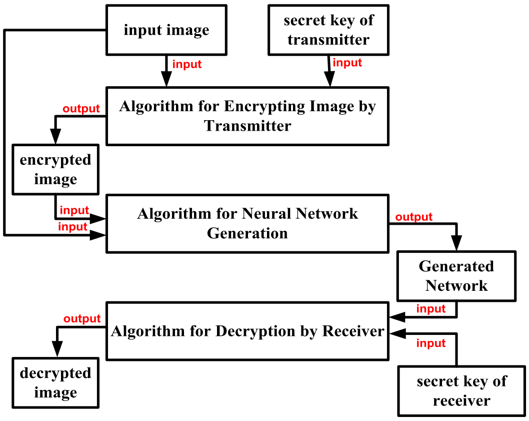

input image
secret key of transmitter
input
input
output
Algorithm for Encrypting Image by Transmitter
encrypted image
input
input
Algorithm for Neural Network Generation
output
Generated Network
input
output
Algorithm for Decryption by Receiver
input
decrypted image
secret key of receiver

FIGURE 2. Proposed research methodology.

with the secret key in safer way. These parameters are used to feed the neural network when performing data validation to produce the validation token. This makes the system more robust against any form of privacy attacks over the image. The outcome of the validation can be produced by comparing the computed version as well as source version of the secret validation token. It will eventually mean that an image can be flagged as tampered if there is a higher range of differences between them. In the process of carrying out validation of the image, the system invokes a potential condition that the secret key as well as attribute should be precise. Adopting an analytical research methodology, the proposed work introduces three sequential set of algorithms that is meant for securing the image. The proposed methodology flow is demonstrated in Fig. 2.

Accordingly, the proposed system implements its first algorithm over the transmitting node where the encryption is carried out considering image and secret key. Unlike public key encryption, the projected system doesn't use any forms of key generation technique and hence protected from any form of key-based intrusions over images. Neural network is implemented to generate a better network structure followed by decryption operation towards the receiver along with a discrete key at the receiver. Here we illustrate three different algorithms constructed to offer robustness in image security.

A. ALGORITHM FOR ENCRYPTING IMAGE BY TRANSMITTER (LEVEL-1 ENCRYPTION)

The main goal of this technique is to encrypt the image using a straightforward and affordable method. The idea is to implement a non-recursive encryption algorithm for ensuring robust backward and forward secrecy along with assurance of optimal image retention while encrypting. The output of the algorithm is basically an encrypted image that is assumed to be reposited at either physical server or distributed cloud and is resistive against various forms of image-based attacks. The following is an assessment of the suggested algorithm's design principle:

```
Input: $I$ (input image), $k_1$ (secret key of transmitter)
Output: $I_e$ (encrypted image)
Start
    Input $I, k_1, k_2$
    $I = p(I, k_1)$
        For $i = 1 : n_r$
            For $j = 1 : n_c$
            $ex_1 = \emptyset\,(I\,(i, j))$
            $I_e\,(i, j) \leftarrow ex_1$
            End
        End
    $I_e \rightarrow (I_e)$
End
```

The above-mentioned algorithm is responsible for carrying out encryption of an image by using I (input image) and k_1 (secret key of transmitter). $P(I,k_1)$ is the function which represents permutation of the given input I with the secret key k_1. The permutation is done throughout the rows and column and final result is obtained as $\emptyset\,(I\,(i, j))$ which is saved as ex_1. The algorithm, after processing, yields an outcome of I_e (encrypted image). Referring to Fig. 3, the algorithm considers that the process of performing encryption is initiated from the transmitter T that takes the input images I and uses its secret key k_1 to perform permutation of the input image. Following steps were carried out to perform permutation [41], [42].

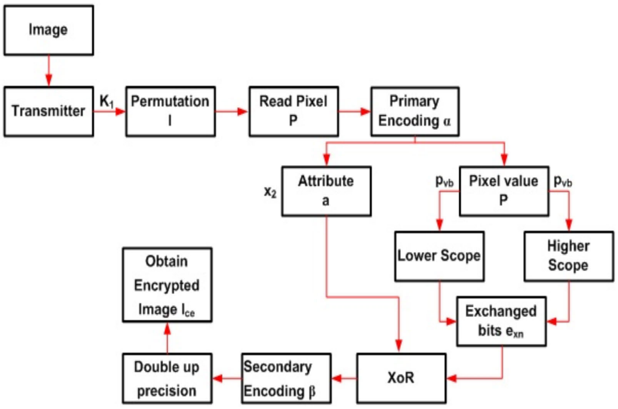


FIGURE 3. Process flow of proposed encryption scheme level-2.

The permutation process for the replacement operation of an arrangement for degree n is supplied by the first arrangement $\{p_i | i = 1, 2, \ldots n, p \in S\}$ and the second arrangement $\{q_i | i = 1, 2, \ldots n, p \in S\}$ and is expressed in (1).

$$i_x = \begin{bmatrix} p_1, p_2 \ldots\ldots . p_n \\ q_1, q_2 \ldots\ldots . q_n \end{bmatrix} \tag{1}$$

where $n!$ such permutations are feasible, and S stands for any set that is not empty. Where p and q are the pixel values across rows and columns of the input image. The opposite of this permutation process is described in (2),

$$i_x^{-1} = \begin{bmatrix} q_1, q_2 \ldots\ldots . q_n \\ p_1, p_2 \ldots\ldots . p_n \end{bmatrix} \tag{2}$$

Ø represents the function that carries out the above-mentioned operation. The processed image I_e is now extracted from its length of its matrix followed by randomly permuting the matrix to produce a random number I_x. Finally, the permutation is carried out by selecting only I_x-pixel elements from image matrix I_e followed by reshaping it with respect to row (n_r) and column (n_c) size of input image I.

This study considers input image I with specific dimension as it is resized followed by translating the resized image to column vector of image I_c. It also applies Mersenne twister random algorithm on the secret key k_1 [43]. For a w bit word length, the Mersenne Twister produces integers in the range of $[0, 2w - 1]$ based on a matrix linear recurrence over a finite binary field F_2, the x_{k+n} is a twisted generalized feedback shift register (GFSR). This method has state bit reflection tempering and is of rational normal form. By using a straightforward recurrence relation to define the series x_i, an invertible F_2 matrix known as a tempering matrix for T is utilized. This matrix then produces numbers of the form x_iT. A series of w-bit numbers with the following recurrence relation are referred to as the series x shown in (3).

$$x_{k+n} = x_{k+m} \oplus \left(\left(x_k^u \parallel x_{k+1}{}^{|}\right) A\right) \quad k = 0, 1, \ldots\ldots\ldots \tag{3}$$

Here, $\parallel$ signifies concatenation of bit vectors (with upper bits on the left) and $\oplus$ denotes the bitwise XOR. The upper $w - r$ bits of x_k is denoted by x_k^u. The lower r bits of x_{k+1} is denoted by $x_{k+1}^{|}$, n: degree of occurrence, m: middle word, an offset used in the recurrence relation defining the series x, $1 \leq m < n$, r: separation point of one word, or the number of bits of the lower bitmask, $0 \leq r \leq w - 1, u, d, l$: further Mersenne Twister tempering bit shifts/masks with the restriction that $2nw - r - 1$ is a Mersenne prime. The twist transformation A is defined in rational normal form as described in (4).

$$A = \begin{bmatrix} 0 & I_{w-1} \\ a_{w-1}, & a_{w-2} \ldots\ldots .a_0 \end{bmatrix} \tag{4}$$

After permutation, the proposed algorithm shown in Fig. 3 reads all the pixel elements and stores it in P matrix that is now subject to primary encoding α scheme which performs following operation [Level-2]. The primary encoding is performed on an initiated attribute to generate encoded bits x_2 and on pixel value P to generate another encoded value P_{vb}. The upper and lower scope of P_{vb} is extracted that are further combined in a data frame e_{xn}. The logic XOR is performed on e_{xn} and x_2 to generate final exchanged bits that are further followed by secondary encoding operation β. The primary encoding operation is carried out by converting decimal to binary numbers using left-shifting operation with most significant bits. The secondary encoding operation is carried out using reverse operation of obtaining decimal number from binary numbers using similar shifting operation. Finally, an encrypted image I_e is obtained.

B. ALGORITHM FOR NURAL NETWORK GENERATION

The outcome of the prior algorithm generates an encrypted image that is required to be forwarded to the receiver through vulnerable communication channel. The study assumes that the vulnerability is present either in communication channel or could be present in the transmission region of the receiver. Hence, mere forwarding of encrypted image doesn't ensure a complete inaccessibility and it just acts as a temporary hold-up for the attackers until they could successfully decrypt it. To offer better security shield towards the encrypted image, the proposed system incorporates a new dependable parameter that is quite hard to break in. The prime necessity of such dependable parameter is to offer higher degree of secrecy formulated with certain form of intelligence that can generate best solution towards strengthening the secrecy of the encrypted image. Hence, the proposed system relies on machine learning-based approach to generate such forms of dependable parameters. An algorithm is formulated using Artificial Neural Network (ANN) that offers extensive benefits over parallel architecture required for any upcoming security systems using multi-core processors. It also offers advantage for minimizing the computational processing time using its large range of learning approaches. The steps of the algorithm of the proposed ANN implementation towards strengthening the security are discussed as follows:

```
Input: $I$ (Array of pixels[0 : 255]), $T$ (Encrypted Image after Level-1 and 2 Algorithm)
Output: $k_{ANN}$ (Generated Network)
Generate [0 : 255] array of pixels as input $I$
Apply Level 1 and 2 Encryption Algorithm
Save the Encrypted Data as Target
Train the Neural Network model with $I$ and $T$
```

The above-mentioned learning scheme takes the input of I (An array of pixels [0 : 255]) and T (Encrypted Image) as a Target for the generation of k_{ANN} (ANN Model) as shown in Fig. 4. Both the input and target factors are applied to neural network to construct the ANN Model which is further subjected to respective training operation leading to formation of key elite networks (k_{ANN}) of size 1 × 256 double.

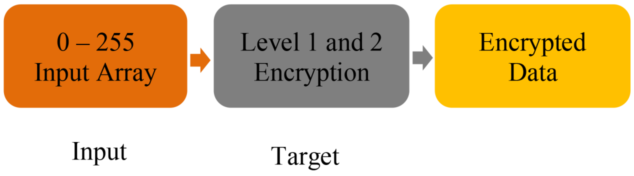


FIGURE 4. Process flow of proposed ANN training.

C. ANN MODEL GENERATION

After feed forward Neural Network training with input array of [0 : 255] pixels, an ANN Model of 256 neurons as input layer, a single hidden layer of 256 neurons and an output layer of 256 neurons with activation functions between layers are developed. Fig. 5 shows the trained ANN model for the proposed work.

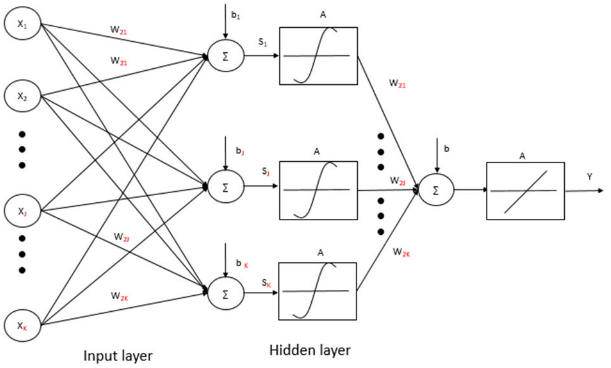


FIGURE 5. ANN architecture for the proposed work.

In this case, one input is multiplied by a bias or offset, while the other input is multiplied by the weight. The activation function generates the scalar neuron output as depicted in Fig. 6, receives the summer output, which is frequently mentioned to as the net input. Here the activation functions used are tan sigmoid in the input side and pure linear in the output side which can be represented mathematically as per (5) and (6).

$$h = \tan sig\,(B_1 + W_1 * X) \tag{5}$$

$$Y = purelin\,(B_2 + W_2 * h) \tag{6}$$

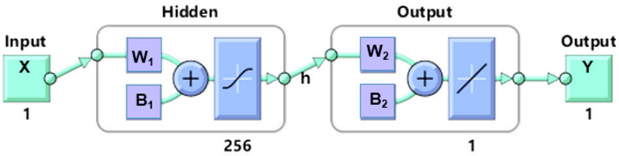


FIGURE 6. ANN constructed network for proposed implementation.

The trained output consists of 0 to 255 locations with their pixel values. Here, ANN encryption can be performed by swapping the input image's pixel values for those of the trained ANN, as seen in Fig. 7. The experimental findings demonstrate that the proposed approach produces good, encrypted outcomes and can withstand all types of statistical and differential attacks since the pixel values have been altered. ANN Decryption can be done in the same way in reverse process.

V. RESULT ANALYSIS

Neural Network Toolbox$^{\text{TM}}$ of MATLAB (Version 2019a) has been used in this work. As it is claimed of implementing non-recursive algorithm for performing encryption, the assessment of its outcome was carried out towards using multiple forms of performance parameters. The mean square error is calculated based on the Performance graph. The output activation function is by default entirely linear. To determine the ideal activation function in the hidden layers, this study analyses performance graphs, response graphs, regression co-efficient values etc. The simulation is run through twelve iterations, with the best result being counted. Along with comparison analysis, the difficulty of calculation is also analyzed. This section offers comprehensive discussion of the environment used for assessing along with result analysis.

A. DATASET CONSIDERED

The implementation of the anticipated study is carried out on multiple forms of dataset such as i) dataset of University of Southern California Weber [44] that has mainly 28 monochrome images and 16 color images that varies from lower size of 256 × 256 to higher size of 1024 × 1024 ii) high-definition color images from McGill (2018) that are normally in either JPG or in TIF format with size of 1920 × 2560 pixel ranging in gigabytes. Color images are converted to grayscale images while applied in algorithm. However, the emphasis was mainly given by real-time color images while performing analysis.

B. ANALYSIS STRATEGY

An artificial neural network is made up of a collection of straight forward processing units that interact with one another through a substantial number of weighted connections. Depending on the application, ANNs may require different architectures, numbers of layers, neurons in hidden levels, and activation functions between layers. Fig. 6 shows a single input neuron and a hidden neuron with numerous inputs and a single output neuron. In this instance, the scalar input is multiplied by the scalar weight whereas the other input has been multiplied by a bias or offset. The scalar neuron output can be produced by transferring the net input to the transfer function. $A = f\,(wp + b)$, where w is weight, p is input and b is bias; can be used to calculate the neuron output. The activation function that is selected to accomplish a certain goal of the issue that the neuron is attempting to address the actual output. Transfer functions are numerous and include the hard limit activating function, log sigmoid, and tan sigmoid. Here, the Tan Sigmoid (Hyperbolic Tangent Sigmoid) has been used. In multilayer networks, this crucial transfer function is employed. In (7), this transfer function's expression is provided as follows.

$$F\,(x) = \frac{e^{2x} - 1}{e^{2x} + 1} \tag{7}$$

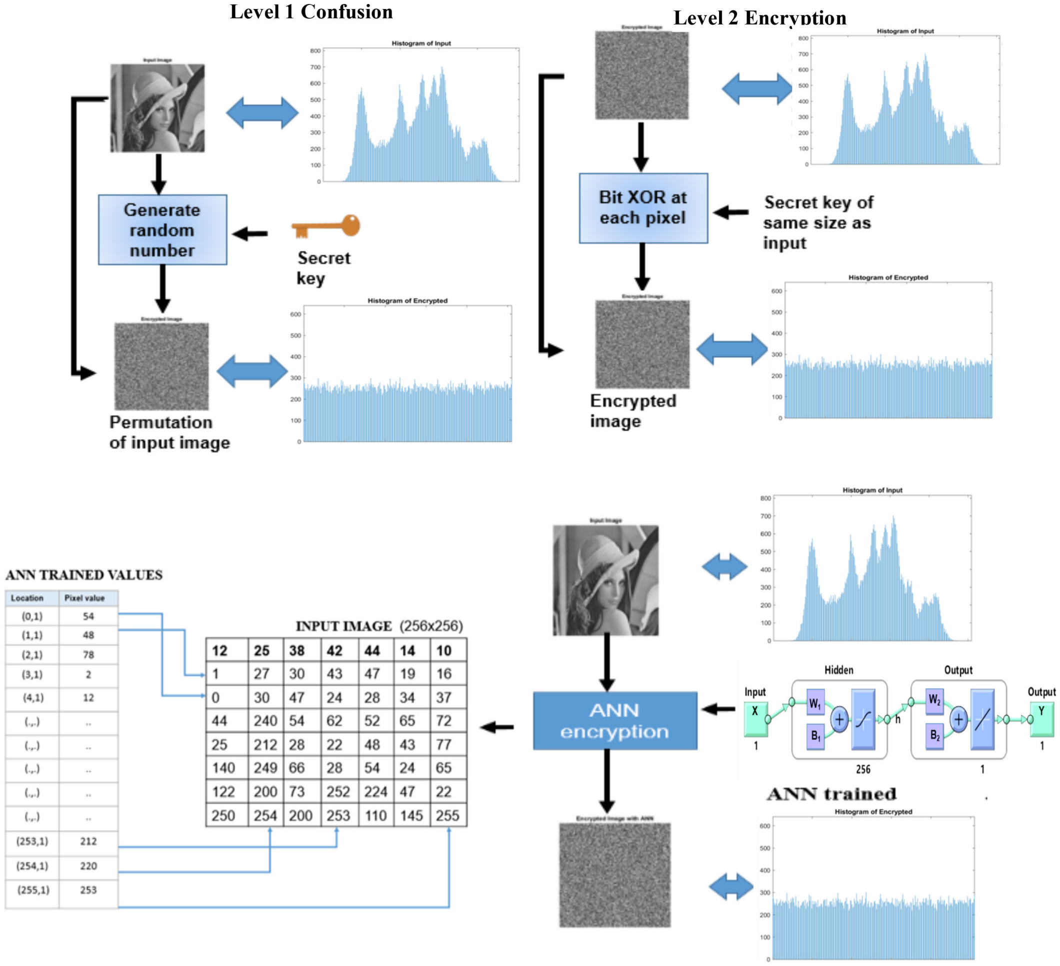
The performance error is initially recorded using the original number of neurons, layers, and activation function. Equation (8) can be used to determine the n number of hidden nodes required for a two-hidden-layer network with N input samples and M output neurons to learn N samples with a tiny error.

$$n = 2\sqrt{((M) + 2)N} \tag{8}$$

Equations (9) and (10) state that there are enough hidden nodes in the first and second layers.

$$n = 2\sqrt{(N)/((m) + 2)} + 2\sqrt{((M) + 2)N} \tag{9}$$

$$n = m\sqrt{(N)/((m) + 2)} \tag{10}$$



ANN TRAINED VALUES

Location	Pixel value
(0,1)	54
(1,1)	48
(2,1)	78
(3,1)	2
(4,1)	12
(.,.)	..
(.,.)	..
(.,.)	..
(.,.)	..
(.,.)	..
(253,1)	212
(254,1)	220
(255,1)	253

INPUT IMAGE (256x256)

12	25	38	42	44	14	10
1	27	30	43	47	19	16
0	30	47	24	28	34	37
44	240	54	62	52	65	72
25	212	28	22	48	43	77
140	249	66	28	54	24	65
122	200	73	252	224	47	22
250	254	200	253	110	145	255

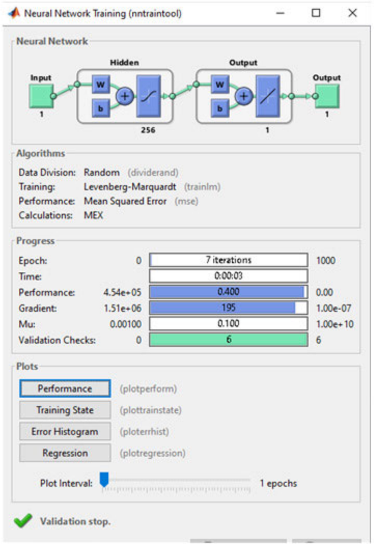
FIGURE 7. ANN encryption.

The activation function for this network is expressed in (11) and A_i is equal to

$$A_i = \sum\nolimits_{i=1}^{N} W_{ij}\left(x_i - b_i\right) \tag{11}$$

The bias is the coefficient that regulates the signal transfer carried out by this network, where N in (11) is the number of input vector elements, w_{ij} is the interconnection weight, and b_i is the bias of the neurons. A multi-layer perceptron of ANN with 255 hidden layers and a single input/output layer is used in the suggested system.

The strategies to assess the learning iterations involved in ANN and its capability include to obtain best results in lowest number of iterations, to assess the impact of ANN over the image quality using various performance metrics associated with signal quality and structural correlation aspects and to ensure the cost effectiveness while complying the above two strategies. The simulation employed in this study is carried out for a total of 12 epochs. The MSE of the performance graphs, the response graph, and the regression coefficient values are compared to get the best result. The Feed Forward Neural Network Training is depicted in Fig. 8.



Algorithms
Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

Epoch:	0	7 iterations	1000
Time:		0:00:03	
Performance:	4.54e+05	0.400	0.00
Gradient:	1.51e+06	195	1.00e-07
Mu:	0.00100	0.100	1.00e+10
Validation Checks:	0	6	6

Plots
Performance (plotperform)
Training State (plottrainstate)
Error Histogram (ploterrhist)
Regression (plotregression)
Plot Interval: 1 epochs

✓ Validation stop.

FIGURE 8. The ANN training process.

For training, the Levenberg-Marquardt algorithm was employed. By measuring the MSE, the effectiveness of the trained network may be evaluated. The Progress panel, showing specific training procedure, displays the number of repetitions that are currently running (12th iteration), the time required to finish the training procedure, the performance (7.92e-19) and Gradient (6.38e-8) in Fig. 8 demonstrate how much variance takes place in the error rate, Mu (1.00e-05) is the threshold value for every iteration that is revised, and the efficiency can demonstrate how much reduced errors happen over training.

The current state of the training process can be observed from Fig. 9. The number of epochs (12 iterations) is shown by the X-axis. The MSE that occurred for each iteration is shown on the Y-axis. The blue, green, and red colored line graph shows the training results, validation results, test outcomes respectively. Every iteration of the training process results in the computation of a performance graph, and the performance graph with the best performance is the one in which the training, validation, and testing outcomes all line up. The training should end at that moment and no more iterations should be conducted. This indicates that further training is not necessary and, if it were, would likely lead to inaccurate findings.

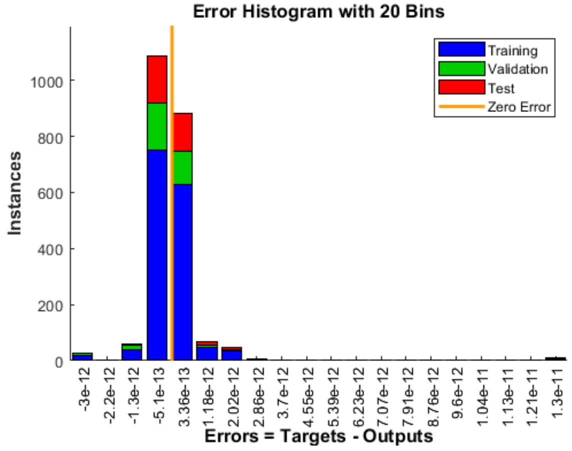


FIGURE 9. **The tan sigmoid activation function histogram error plots.**

The histogram inaccuracy graph is depicted in Fig. 9. From these Graphs, most instances' mistakes are close to 0. The following relation: $output = learning - rategoal + bias$, describes the connection between input and output parameters - is represented by the regression plot. illustrated in Fig. 10. It is still another crucial component for confirming network performance. The data can be best fitted by this network if the preferred Regression coefficient (R) value is equivalent to 1, and if it is close to 0, it is undesired. The first three plots in Fig. 10 represent training, validation, and testing data. The dashed line on each plot depicts the ideal result, which occurs when outputs and targets are met. The solid line signifies the best-fitting linear regression line between the outputs and the targets. The R value will be influenced by the connection between the outputs and the goals. If R = 1, then there is an ideal linear connection between the outputs and the targets. If R is close to 0, there is no linear correlation between the outcomes and the targets. Here, the target denotes our original image, and the outcome denotes our image following decryption. According to Fig. 10, the training data shows an excellent fit. Large R values can be seen in both the test and validation outcomes.

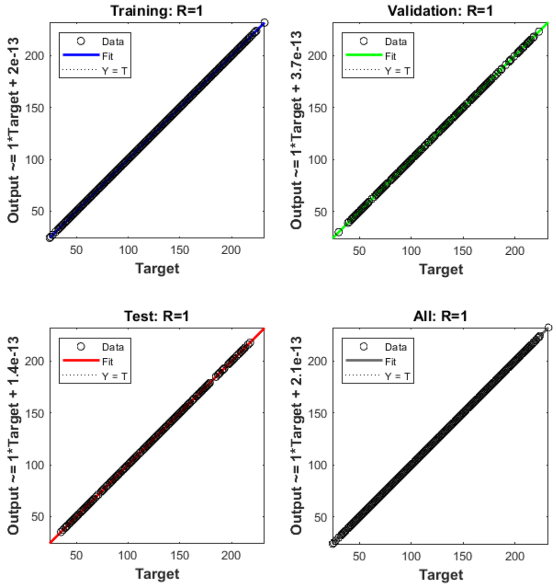


FIGURE 10. **Regression analysis.**

TABLE 1. **Chi- square test.**

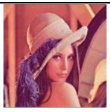
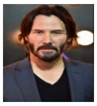
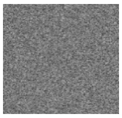
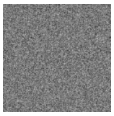
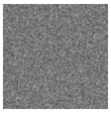
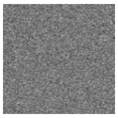
Chi-Square Test	
Original Image	Encrypted Image
Lena :28.588	Lena:194.41
Cameraman:113.654	Cameraman:241.32
Baboon: 44.39	Baboon:220.12
Pepper: 36.778	Pepper:246.7

C. VISUAL OUTCOME ANALYSIS

The visual results obtained from experiments of proposed system are showcased in Table 1 to highlight outcomes obtained during different stages of algorithm processing. A closer look into visual outcomes shows there is no dominant fluctuation in visual perception quality for standard dataset (Sample 1) with real-time images (Sample 2, Sample 3, and Sample 4). It demonstrates that projected system is exceedingly applicable on any form of security designs of commercial applications thereby increasing the scope towards image security. The proposed system offers nearly similar performance for any forms of standard and real-time color images. The testing was carried out with both standard and high-definition colored image of Sample 4 to find nearly similar performance of proposed system.

The six sample images from the USC SIPI Image Database are highlighted in Table 2. Plotting the histogram analysis

TABLE 2. Stages of visual outcomes of proposed system.

	Sample 1	Sample 2	Sample 3	Sample 4
Original Image (input)				
Grey scaled image (new Input)				
Permuted Image				
Encrypted Image				
Decrypted Image				

of the raw and encrypted images demonstrates how well our suggested technique resists statistical attacks. Equation (12) is used to compute the uniformity of a histogram caused by the proposed encryption scheme which can be justified by the Chi-square test. For the purpose of correlation analysis, 1000 randomly selected pixels from the original and encrypted images are plotted below in the horizontal, vertical, and diagonal directions. In the encrypted image, it has been demonstrated that there are no associations between adjacent pixels.

$$\chi^2 = \sum\nolimits_{k=1}^{256} \frac{(v_k - 256)^2}{256} \tag{12}$$

where k is the number of gray levels and v_k is the observed occurrence frequencies of each gray level (0–255). The experimental chi-square value should be less than the theoretical value (293 with significance level 0.05) for an ideal image encryption system. The lower value of the Chi-square value indicates a better uniformity as highlighted in Table 1.

Decryption is the reverse process of encryption. Here, RGB image is first converted to gray image, and again gray image is converted to RGB during decryption process as mentioned in Table 2.

D. GRAPHICAL OUTCOME ANALYSIS

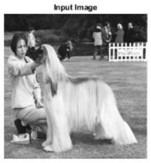
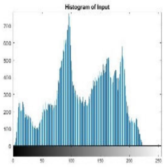
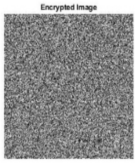
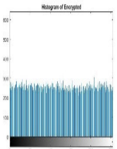
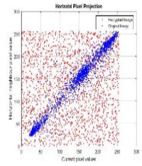
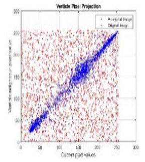
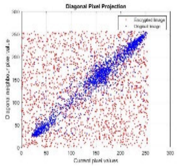
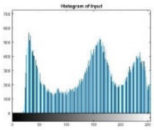
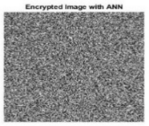
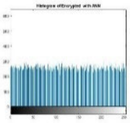
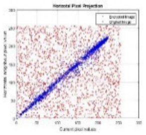
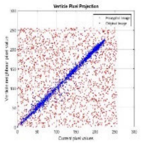
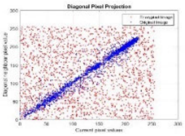
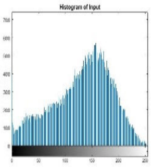
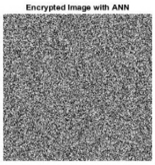
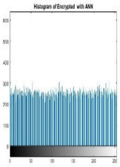
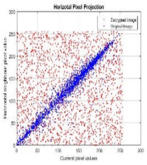
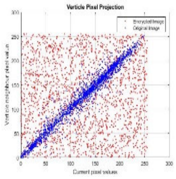
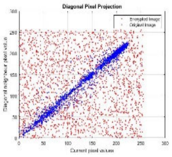
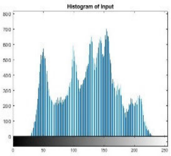
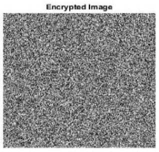
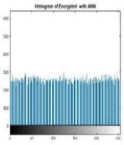
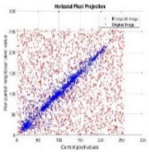
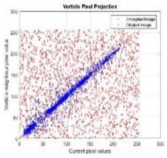
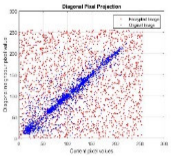
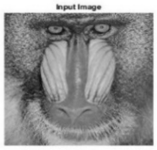
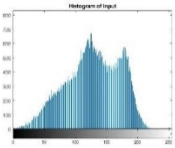
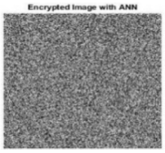
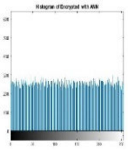
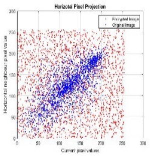
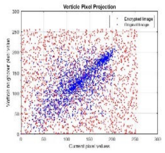
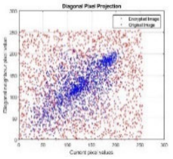
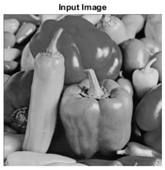
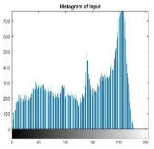
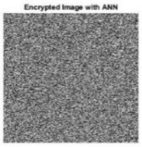
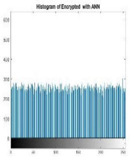
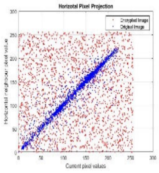
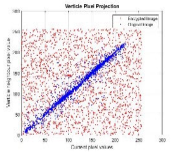
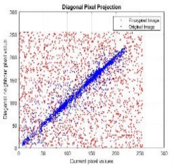
Fig. 11 displays the study of correlation coefficients for both real-time images (Samples 2/3/4 of Fig. 11 (b), (c), and (d)) and the standard dataset (Sample 1, Fig. 11 (a)). The analysis demonstrates that, over an increasing range of pixel values, the original image's correlation (horizontal, vertical, and diagonal coefficient) is significantly lower than that of the encrypted image. This demonstrates that the encryption process of the suggested approach may successfully scramble the original image.

Fig. 12 displays the histogram analysis for a typical dataset (Sample 1). The simulation results show that the histograms of the plaintext images in Fig. 12 (a) are different from the comparable histogram of the encrypted image in Fig. 12 (b), which is fairly evenly distributed after encryption. An attacker would have a hard time deducing anything valuable from the statistical characteristic. Therefore, it doesn't offer any information on how to carry out a statistical assault on the proposed system. The proposed algorithm's experimental findings demonstrate that the XOR and permutation operations make the encrypted image's greyscale distribution very uniform, demonstrating that the algorithm can withstand statistical inspection in such a way that the attacker cannot analyze the original grey value distribution set. Plotting the histogram analysis of the raw and encrypted images demonstrates how well our suggested technique resists statistical attacks.

E. ANALYSIS OF CROPPED ATTACKS

The resilience of the cryptosystem can be evaluated by looking at the outcomes of a crop attack [48]. To carry out a crop attack, it is normal practice to purposely crop the encrypted image with a modified dimension. Table 4 shows the decrypted image's correctness by calculating the quality metrics MSE, PSNR [56], and Correlation between the original and encrypted image. The calculation methods utilized to determine the MSE and PSNR are described in (13) and (14), respectively. This outcome demonstrates the resilience of our

TABLE 3. ANN result comparison of proposed system.

Input Image	Input Histogram	Encryption using ANN	Output Histogram	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
						
						
						
						
						
						

cryptosystem against cipher image attacks.

$$MSE = \frac{1}{MXN} \sum\nolimits_{i=1}^{M} \sum\nolimits_{j=1}^{N} O\left(i,j\right) - D/E(i,j)^{2} \quad (13)$$

$$PSNR = 20\log_{10}\frac{I_{max}}{\sqrt{MSE}} \quad (14)$$

O and D stand for the original and decrypted images, respectively. The image size is represented by M and N.

F. NOISE ATTACK ANALYSIS

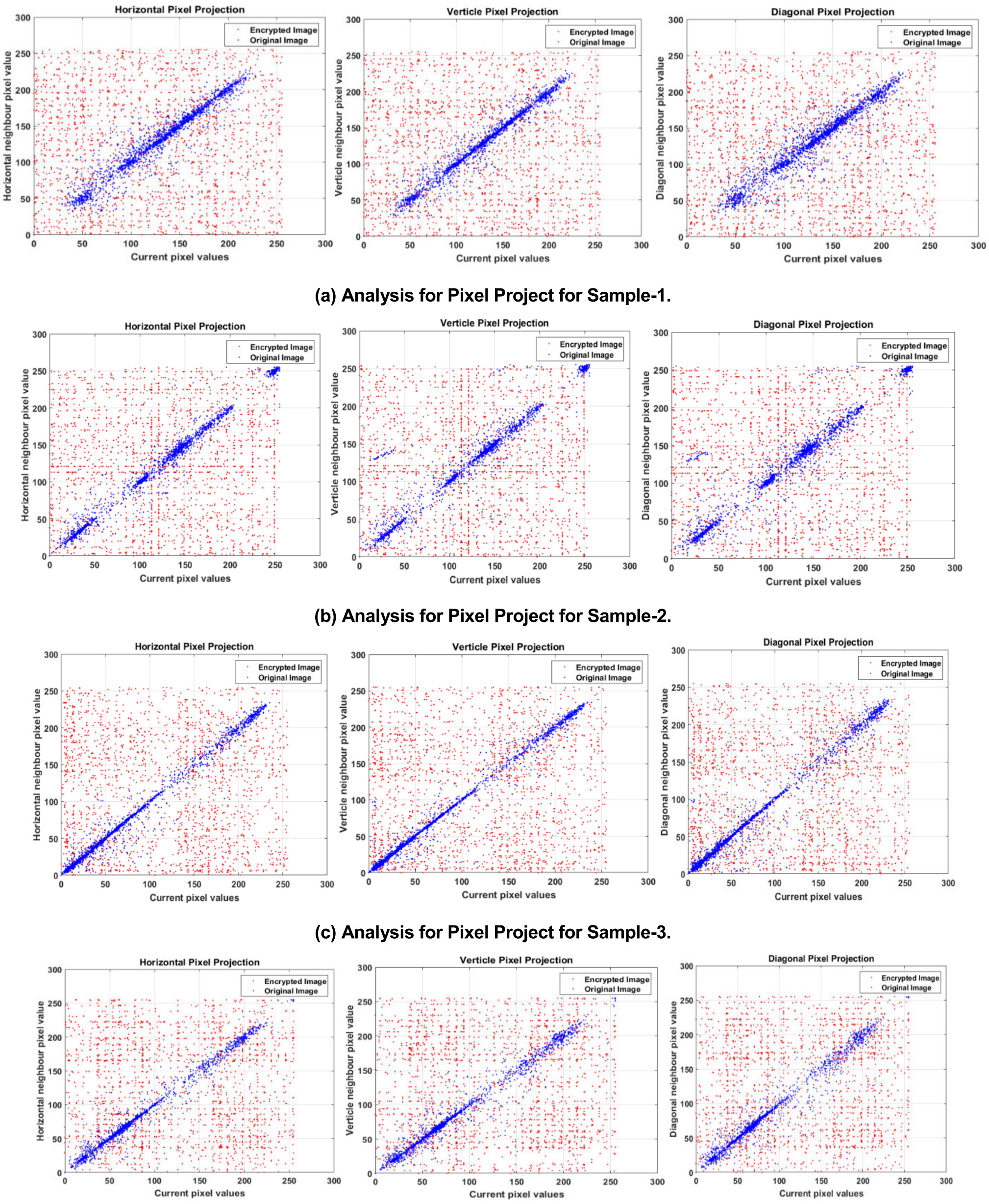
To demonstrate the resilience, noises like salt and pepper and Gaussian noise embed with the encrypted image are occasionally added during transmission, and the associated decrypted images are then examined. It can be agreed that the constructed cryptosystem is capable of withstanding attacks using Gaussian and salt and pepper noise up to 0.001 and 0.00001 amount.

G. KEY SPACE ANALYSIS

Key space is considered as an important feature in any cryptosystem. It should be large enough to produce the ability to resist against brute force attacks. It was identified that the adequate key space for image encryption scheme should be larger than 2^{100} to oppose brute force attacks. The key space of our proposed scheme is 2^{136}.

H. STATISTICAL RANDOMNESS ANALYSIS

Encrypted image generated by any cryptographic encryption scheme, should be invulnerable to statistical attacks. The presence of randomness is essential not only for pseudo random number generators (PRNGs) but also for the encrypted data. Therefore, the randomness is evaluated in the resulting encrypted data by using National Institute of Standard and Technology (NIST) statistical random test suite It is a statistical test suitable for random and pseudorandom number



(a) Analysis for Pixel Project for Sample-1.

(b) Analysis for Pixel Project for Sample-2.

(c) Analysis for Pixel Project for Sample-3.

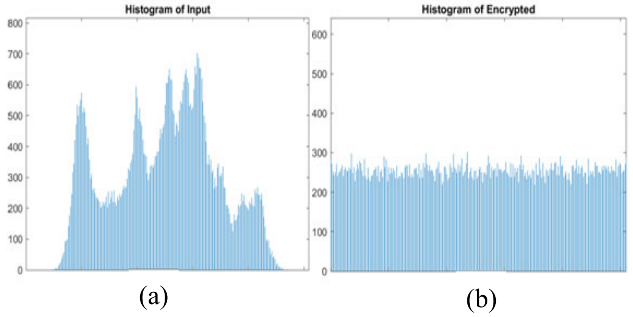
(d) Analysis for Pixel Project for Sample-4.

FIGURE 11. Analysis of correlation coefficient.

generators for cryptographic applications. We performed a NIST test for 65536 × 8 bits binary numbers of the generated encrypted image ''Lena''. The test results are listed in Table 5. It can be seen from the table that the generated cipher image passed all 6 tests, which shows that the sequence generated by our algorithm is random. With the suggested parameters for input sequence, the p-value is expected to be greater than 0.01 to qualify for the randomness in the bit stream of encrypted data.

I. COMPARATIVE ANALYSIS

We evaluated the predicted system's efficacy by contrasting this algorithm with the pertinent encryption methods that have recently been put into use by Wei et. al. [50], Fu et. al. [49], Tang et. al. [45], Maddodi et. al. [46] and Peng et. al. [47]. The performance of all comparison techniques is shown in Table 6. The suggested method's NPCR, UACI, Correlation Coefficient, and Entropy are assessed against the industry-standard ''lena'' test image (256 × 256 pixels, 24-bit RGB color) [50], [51]. Table 7 highlights the comparative analysis of NPCR (Number of Pixels Change Rate), UACI (Unified Average Changing Intensity), Correlation Coefficient Entropy, key sensitivity, and encryption time for six standard images. NPCR and UACI are frequently used in practice to assess the ability to withstand differential attack. A greater value is preferable, and the NPCR concentrates



(a) (b)

FIGURE 12. Histogram study a) original image, b) Encrypted image.

TABLE 4. Analysis of the quality of decrypted images in relation to crop and noise attack.

Cipher Image	MSE	PSNR
Crop attack	49.50	31.18

TABLE 5. NIST SP800-6 TESTS results for encrypted image.

Test Name	p-value	result
Approximate entropy	0.8673	Success
Cumulative sums forward	0.8427	Success
Cumulative sums reverse	0.7240	Success
FFT	0.9818	Success
Rank	0.6224	Success
Frequency	0.6287	Success

on the precise number of pixels that alters the value in differential attack. The average difference between two paired cipher images is the focus of UACI, where a smaller value is preferable. Expected average values for NPCR is 99.56% and for UACI is 33.46%. Entropy can be used to describe the uncertainty or randomness of an image. The theoretical maximum of the entropy is 8. The degree of relationship between pixel's gray values is known as pixel correlation.

However, the performance of the encryption technique improves when the correlation between neighboring pixels of the encrypted image decreases. The correlation coefficient lies between −1 and 1. The prime reason behind consideration of this comparative analysis is because the core domain of proposed study is basically an encryption approach whose performance is improved using neural network. Hence, it is necessary to analysis the security strength offered by the encryption approach of proposed system in comparison to existing encryption system. While performing this analysis, the complete test-bed is retained same as image dataset so that unbiased analysis can be carried out. These existing encryption approaches are found to offer much focus on ciphering the image and not much on the image quality, which makes the proposed system perform in distinction in contrast to existing approach.

The comparison between real-time and standard images is shown in Fig. 13, which demonstrates that feed forward and fitting neural networks offer minimized encryption time for real-time images due to their lower iteration involvement as opposed to self-organizing maps and feed-forward Back propagation algorithms, which do not sufficiently reduce encryption time for real-time images.

The comparison between real-time and standard images is shown in Fig. 13, which demonstrates that feed forward and fitting neural networks offer minimized encryption time for real-time images due to their lower iteration involvement as opposed to self-organizing maps and feed-forward Back propagation algorithms, which do not sufficiently reduce encryption time for real-time images.

It is clear from the pattern of the numerical results presented in Fig. 14 that the processing times of all ANN approaches are essentially the same. When compared to self-organizing maps and feed-forward backpropagation, feed-forward and fitting neural networks are found to give faster processing times, according to the data. The prime reasons behind this are feed-forward has less contribution of iteration as compared to fitting neural network, consumption of more time to reach its convergence state for self-organizing map due to initialization issues with respect to the input and target, the feed-forward back-propagation strategy requires extra processing time due to requirement of several iterations to retrieve the network key. As a result, the entire proposed technique is characterized by a quicker response time as well as excellent signal quality retention. This outcome is also somewhat better version of our earlier implementation study, in which the image was protected using Chaotic Map [46], Deep Neural Network [51], and Elliptical Curve Cryptography [52]. Further, the study outcome is also compared with existing approaches where encryption as well as neural network has been deployed.

A closer look at the numerical analysis of results presented in Table 8 reveals that the suggested system outperforms the present system in terms of processing speed and the Structural Similarity Index Measure (SSIM) value. The quality of the reconstructed images is assessed using SSIM [56]. The SSIM index measures the similarity between two images and is calculated using Eq. (15). It has value between 0 and 1, the larger the value, the smaller the image distortion. When the two images are exactly the same, the SSIM value is equal to 1. SSIM between the plain images and the encrypted image is represented as SSIM (a), and between the plain images and the decrypted images is represented as SSIM (b) as listed in table 9.

$$SSIM = \frac{(2\mu_x\mu_y + C_1) + (2\sigma_{xy} + C_2)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \tag{15}$$

where μ_{x} represents the average of x, μ_{y} signifies the average of y, σ_{X}^2 represents the variance of x, σ_{y}^2 signifies the variance of y, σ_{xy} signifies the co-variance of x and y.

The work carried out by Wang et. al. has used chaotic encryption principle which offers more focus on synchronized outcome and hence slightly more time is consumed

TABLE 6. Comparative analysis of NPCR, UACI, correlation coefficient and entropy for recent encryption approaches.

Encryption Approach	NPCR in %	UACI in %	Correlation coefficient			Entropy
			Horizontal	Vertical	Diagonal	
Proposed scheme	99.75	33.61	-0.006508	0.022328	0.015374	7.9846
Chong Fu *et. al.* [50]	99.61	33.44	0.0033	0.0155	0.0158	7.999
Zhenjun Tang *et. al.* [46]	99.6	33.39	−0.0685	0.0857	0.0059	7.9992
Gururaj Maddodi *et. al.* [47]	99.6155	28.567	0.00046	0.0011	0.0031	7.9976
Jun Peng *et. al.* [48]	99.6059	33.5364	0.0173	-0.0101	0.0172	7.9992
Xiaopeng Wei *et. al.* [51]	99.58649	33.48347	0.0054	0.0062	0.0017	7.9971

TABLE 7. Comparative analysis of NPCR, UACI, correlation coefficient, entropy, key sensitivity and encryption time for six different images.

Image Name	Correlation Coefficient			UACI	NPCR	Entropy	Key Sensitivity	Encryption time in sec
	Horizontal	Vertical	Diagonal					
Lena	-0.006508	0.022328	0.015374	33.61	99.75	7.984	0.0020	0.242
Baboon	-0.0055	0.0012	-0.002	31.33	99.30	7.997	0.0016	0.219
dog	0.0036	-0.0028	0.0072	31.81	99.46	7.997	0.032	0.208
fruits	0.0006	4x e^{-5}	0.0059	32.82	99.40	7.997	0.0090	0.205
peppers	-0.0044	-0.0003	-0.0094	32.31	99.42	7.997	0.0012	0.202
Hat	-0.0069	-0.0025	0.0004	32.30	99.462	7.99	0.0095	0.210

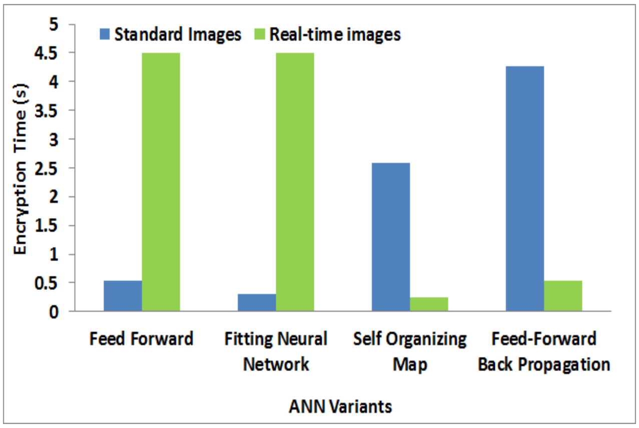


FIGURE 13. Comparative analysis of encryption time.

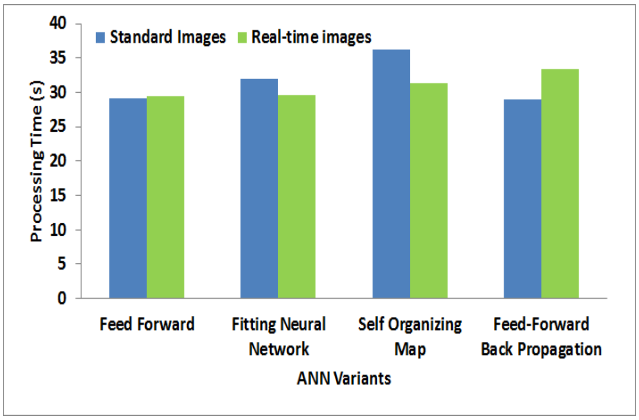


FIGURE 14. Comparative analysis of processing time.

TABLE 8. Comparative analysis.

Approaches	Processing Time in seconds	SSIM
This work	32	0.002165
Wang *et. al.* [54]	39	0.000106
Dridi *et. al* [55].	46	0.000112
Chen *et. al.* [56]	51	0.000021

TABLE 9. SSIM results of test images.

Test image	SSIM(a)	SSIM(b)
Lena	0.0021	1.000
Baboon	0.010	1.000
Peppers	0.0086	1.000
Dog	0.0063	1.000

by its algorithm [53]. The approach of Dridi et. al. uses an extensive key generation mechanism apart from using neural network and logistic map which significantly increases algorithm processing time [54]. However, its SSIM is better than that of Wang et. al. [53]. The work carried out by Chen et. al. has used neural network with reaction-diffusion where chaotic cryptosystem is used [55]. This system includes maximum processes in order to carry out image encryption and hence consumes more time and also affects in SSIM performance.

The core findings of the proposed study with respect to its contributions and advantage are as follows:

- The proposed system shows that usage of non-recursive encryption technique along with low-iterated machine learning approach boosts up the encryption process
- Feed-forward based training approach is much efficient in comparison to other variants of ANN

- Proposed system offers faster encryption as well as decryption performance with better quality of signal with less processing time.

VI. CONCLUSION

This paper has presented a simple computational model that performs non-recursive process of encryption mechanism unlike conventional encryption approaches. The robustness of the encryption is increased by using feed-forward training approach in ANN. The proposed principle further boosts up the process of technical adoption of proposed system. Results and security analysis demonstrate that our technique is effective at encrypting data and is resistant to exhaustive, statistical, and differential attacks. Although, deep neural network offers significant advantage in contrast to conventional approaches; however, their applicability is still under the radar of research community. The area of applicability of presented concept of image security has been assessed with respect to different forms of images to prove that proposed system could be commercially used in the form of application.

REFERENCES

[1] S. Shivani, S. Agarwal, and J. S. Suri, *Handbook of Image-based Security Techniques*. Boca Raton, FL, USA: CRC Press, 2018.

[2] R. Zhang, D. Xiao, and Y. Chang, "A novel image authentication with tamper localization and self-recovery in encrypted domain based on compressive sensing," *Secur. Commun. Netw.*, vol. 2018, pp. 1–15, Mar. 2018.

[3] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[4] B. Awdun and G. Li, "Retracted: The color image encryption technology based on DNA encoding & sine chaos," in *Proc. Int. Conf. Smart City Syst. Eng. (ICSCSE)*, Nov. 2016, pp. 539–544.

[5] V. A. Bharadi, H. A. Mestry, N. N. Mhaskar, and P. S. Karanjavkar, "Cloud based NoSQL database for Iris based biometric system Azure based Cosmos DB implementation," vol. 7, pp. 397–400, 2018.

[6] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 4, pp. 636–646, Apr. 2016.

[7] L. Zhang, X. Yuan, K. Wang, and D. Zhang, "Multiple-image encryption mechanism based on ghost imaging and public key cryptography," *IEEE Photon. J.*, vol. 11, no. 4, pp. 1–14, Aug. 2019.

[8] L. Bao, S. Yi, and Y. Zhou, "Combination of sharing matrix and image encryption for lossless (k, n) -Secret image sharing," *IEEE Trans. Image Process.*, vol. 26, no. 12, pp. 5618–5631, Dec. 2017.

[9] X.-Q. Fu, B.-C. Liu, Y.-Y. Xie, W. Li, and Y. Liu, "Image encryption-then-transmission using DNA encryption algorithm and the double chaos," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–15, Jun. 2018.

[10] Z. Gao, D. Chen, W. Zhang, and S. Cai, "Colour image encryption algorithm using one-time key and FrFT," *IET Image Process.*, vol. 12, no. 4, pp. 472–478, Apr. 2018.

[11] H. Huang and S. Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," *IET Image Process.*, vol. 11, no. 4, pp. 211–216, Apr. 2017.

[12] M. Kaur and V. Kumar, "Colour image encryption technique using differential evolution in non-subsampled contourlet transform domain," *IET Image Process.*, vol. 12, no. 7, pp. 1273–1283, Jul. 2018.

[13] P. N. Andono and D. R. I. M. Setiadi, "Improved pixel and bit confusion-diffusion based on mixed chaos and hash operation for image encryption," *IEEE Access*, vol. 10, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.

[14] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Process.*, vol. 132, pp. 96–109, Mar. 2017.

[15] A. A. Abd El-Latif, B. Abd-El-Atty, and M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, pp. 1073–1081, 2018.

[16] C. Li, D. Lin, and J. Lü, "Cryptanalyzing an image-scrambling encryption algorithm of pixel bits," *IEEE MultimediaMag.*, vol. 24, no. 3, pp. 64–71, Aug. 2017.

[17] P. Li and K.-T. Lo, "A content-adaptive joint image compression and encryption scheme," *IEEE Trans. Multimedia*, vol. 20, no. 8, pp. 1960–1972, Aug. 2018.

[18] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu, and S. Miao, "Image block encryption algorithm based on chaotic maps," *IET Signal Process.*, vol. 12, no. 1, pp. 22–30, Feb. 2018.

[19] M. Preishuber, T. Hütter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2137–2150, Sep. 2018.

[20] S. Sun, "A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photon. J.*, vol. 10, no. 2, pp. 1–14, Apr. 2018.

[21] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on Josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018.

[22] T. Chuman, W. Sirichotedumrong, and H. Kiya, "Encryption-then-compression systems using grayscale-based image encryption for JPEG images," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1515–1525, Jun. 2019.

[23] N. Wang, G. Di, X. Lv, M. Hou, D. Liu, J. Zhang, and X. Duan, "Galois field-based image encryption for remote transmission of tumor ultrasound images," *IEEE Access*, vol. 7, pp. 49945–49950, 2019.

[24] P. Ping, J. Fu, Y. Mao, F. Xu, and J. Gao, "Meaningful encryption: Generating visually meaningful encrypted images by compressive sensing and reversible color transformation," *IEEE Access*, vol. 7, pp. 170168–170184, 2019.

[25] L. Li, Y. Xie, Y. Liu, B. Liu, Y. Ye, T. Song, Y. Zhang, and Y. Liu, "Exploiting optical chaos for color image encryption and secure resource sharing in cloud," *IEEE Photon. J.*, vol. 11, no. 3, pp. 1–12, Jun. 2019.

[26] R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo, "A novel chaos-based symmetric image encryption using bit-pair level process," *IEEE Access*, vol. 7, pp. 99470–99480, 2019.

[27] G. Luan, A. Li, D. Zhang, and D. Wang, "Asymmetric image encryption and authentication based on equal modulus decomposition in the Fresnel transform domain," *IEEE Photon. J.*, vol. 11, no. 1, pp. 1–7, Feb. 2019.

[28] H. Li, S. Yu, W. Feng, Y. Chen, J. Zhang, Z. Qin, Z. Zhu, and M. Wozniak, "Exploiting dynamic vector-level operations and a 2D-enhanced logistic modular map for efficient chaotic image encryption," *Entropy*, vol. 25, no. 8, p. 1147, Jul. 2023.

[29] H. Wen, Y. Huang, and Y. Lin, "High-quality color image compression-encryption using chaos and block permutation," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 8, Sep. 2023, Art. no. 101660, doi: 10.1016/j.jksuci.2023.101660.

[30] Q. Kun, F. Wei, Q. Zhentao, Z. Jing, L. Xuegang, Z. Zhenggu, "A novel image encryption scheme based on memristive chaotic system and combining bidirectional bit-level cyclic shift and dynamic DNA-level diffusion," *Frontiers Phys.*, vol. 10, Aug. 2022, Art. no. 963795, doi: 10.3389/fphy.2022.963795.

[31] H. Hong, X. Liu, and Z. Sun, "A fine-grained attribute based data retrieval with proxy re-encryption scheme for data outsourcing systems," *Mobile Netw. Appl.*, vol. 26, no. 6, pp. 2509–2514, Dec. 2021, doi: 10.1007/s11036-018-1102-3.

[32] H. Hong and Z. Sun, "Constructing conditional PKEET with verification mechanism for data privacy protection in intelligent systems," *J. Supercomput.*, vol. 79, no. 13, pp. 15004–15022, Sep. 2023, doi: 10.1007/s11227-023-05253-9.

[33] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: A survey," in *Proc. 5th Int. Conf. Signal Image Process.*, Bengaluru, India, Jan. 2014, pp. 102–107.

[34] M. Kumari, S. Gupta, and P. Sardana, "A survey of image encryption algorithms," *3D Res.*, vol. 8, no. 4, p. 148, Dec. 2017.

[35] M. Khan and T. Shah, "A literature review on image encryption techniques," *3D Res.*, vol. 5, no. 4, p. 29, Dec. 2014.

[36] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[37] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, Jan. 2011.

[38] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[39] J. Wang, Q.-H. Wang, and Y. Hu, "Image encryption using compressive sensing and detour cylindrical diffraction," *IEEE Photon. J.*, vol. 10, no. 3, pp. 1–14, Jun. 2018.

[40] S. Lian, J. Sun, and Z. Wang, "One-way hash function based on neural network," 2007, *arXiv:0707.4032*.

[41] D. R. I. M. Setiadi and N. Rijati, "An image encryption scheme combining 2D cascaded logistic map and permutation-substitution operations," *Computation*, vol. 11, no. 9, p. 178, Sep. 2023.

[42] R. Robet, O. Pribadi, S. Widiono, and M. K. Sarker, "Image encryption using half-inverted cascading chaos cipheration," *J. Comput. Theories Appl.*, vol. 1, no. 2, pp. 12–28, 2023.

[43] K. L. Prasad, T. Ch. M. Rao, and V. Kannan, "A hybrid semi-fragile image watermarking technique using SVD-BND scheme for tampering detection with dual authentication," in *Proc. IEEE 6th Int. Conf. Adv. Comput. (IACC)*, Feb. 2016, pp. 517–523.

[44] A. Weber. (2018). *The USC-SIPI Image Database. 2014*. [Online]. Available: http://sipi.usc.edu/database

[45] Z. Tang, Y. Yang, S. Xu, C. Yu, and X. Zhang, "Image encryption with double spiral scans and chaotic maps," *Hindawi Secur. Commun. Netw.*, vol. 2019, Jan. 2019, Art. no. 8694678, doi: 10.1155/2019/8694678.

[46] G. Maddodi, A. Awad, D. Awad, M. Awad, and B. Lee, "A new image encryption algorithm based on heterogeneous chaotic neural network generator and DNA encoding," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 24701–24725, Oct. 2018, doi: 10.1007/s11042-018-5669-2.

[47] J. Peng and D. Zhang, "Image encryption and chaotic cellular neural network," in *Machine Learning in Cyber Trust: Security, Privacy, and Reliability*. Boston, MA, USA: Springer, 2009, pp. 183–213.

[48] X. Zeng, C. Liu, Y.-S. Wang, W. Qiu, L. Xie, and Y.-W. Tai, "Adversarial attacks beyond the image space," in *Proc. Comput. Vis. Pattern Recognit.*, Jan. 2017, pp. 4302–4311.

[49] C. Fu, G.-Y. Zhang, M. Zhu, Z. Chen, and W.-M. Lei, "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy," *Hindawi Secur. Commun. Netw.*, vol. 2018, Jun. 2018, Art. no. 2708532, doi: 10.1155/2018/2708532.

[50] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, Feb. 2012, doi: 10.1016/j.jss.2011.08.017.

[51] S. R. Maniyath and V. Thanikaiselvan, "Robust and lightweight image encryption approach using public key cryptosystem," in *Cybernetics and Algorithms in Intelligent Systems*, vol. 3. Cham, Switzerland: Springer, 2018, pp. 63–73.

[52] S. R. Maniyath and T. V, "An efficient image encryption using deep neural network and chaotic map," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103134.

[53] W. Wang, X. Wang, X. Luo, and M. Yuan, "Finite-time projective synchronization of memristor-based BAM neural networks and applications in image encryption," *IEEE Access*, vol. 6, pp. 56457–56476, 2018.

[54] M. Dridi, M. A. Hajjaji, B. Bouallegue, and A. Mtibaa, "Cryptography of medical images based on a combination between chaotic and neural network," *IET Image Process.*, vol. 10, no. 11, pp. 830–839, Nov. 2016.

[55] W.-H. Chen, S. Luo, and W. X. Zheng, "Impulsive synchronization of Reaction–Diffusion neural networks with mixed delays and its application to image encryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 12, pp. 2696–2710, Dec. 2016.

[56] J. Wang, J. Li, X. Di, J. Zhou, and Z. Man, "Image encryption algorithm based on bit-level permutation and dynamic overlap diffusion," *IEEE Access*, vol. 8, pp. 160004–160024, 2020, doi: 10.1109/ACCESS.2020.3020187.

ASISA KUMAR PANIGRAHY received the B.Tech. degree in electronics and communication engineering from the National Institute of Science and Technology, Berhampur, Odisha, in 2010, the M.Tech. degree in VLSI and embedded system design from BPUT, Rourkela, Odisha, in 2012, and the Ph.D. degree in microelectronics and VLSI from the Electrical Engineering Department, Indian Institute of Technology Hyderabad, in 2017.

Currently, he is an Associate Professor with the Department of Electronics and Communication Engineering, ICFAI Foundation for Higher Education Hyderabad, India. He has authored 25 peer-reviewed and SCI-indexed articles in prestigious publications, including IEEE, Elsevier, and Springer. His research interests include vertical IC (3D IC) integration, semiconductor device simulations and modeling, and sensors based on micro-nano materials. He received the Gandhian Young Technological Innovation Award for the research work "A Low-Cost Disposable Microfluidic Biochip for Malaria Diagnosis" from the Honorable President of India Shri Ram Nath Kovind Ji at Rhastrapati Bhavan, in March 2018. He received the Distinguished Japanese Society for the Promotion of Science (JSPS) Award by the Prof. T. Suga from The University of Tokyo, Japan, as an invited Speaker, in 2017. He received the Excellence in Research Award from the Director of Indian Institute of Technology Hyderabad during the Foundation Day of Institute, in 2015 and 2016. He received the DST Young Scientist Award by the Department of Science and Technology, Government of India, in 2016. In 2016, the CSIR, Government of India, presented him with the CSIR Young Scientist Award. He is also handling research project funded by BIRAC, Government of India. He is also an Academic Editorial Board Member of *Nanomaterials* journal (Hindawi).

SHIMA RAMESH MANIYATH (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the Government College of Engineering Kannur, Kerala, in 2009, the master's degree in embedded system from Amrita Viswa Vidyapeedam, Bengaluru, in 2011, and the Ph.D. degree in information security from the Vellore Institute of Technology, in 2021. Currently, she is an Assistant Professor with the MVJ College of Engineering, Bengaluru. She has published her research works in five international, four national journals, and five international conference proceedings. She is also having 12 years of teaching experience. She is also a member of ISTE, in 2022.

MITHILEYSH SATHIYANARAYANAN (Member, IEEE) received the Ph.D. degree from the City, University of London.

He completed his pre-doctoral fellowship from the University of Brighton, U.K. He is currently an Indian-Born Research Scientist and an Entrepreneur in London. He closely works with "MAKE IN INDIA" initiatives through his organization, MIT Square. Being the Founder and the CEO, his vision is to build Indian products and take it to the world. His research was in collaboration with the Nokia Research, Finland, which won him "Young Scientist Award." He has also won several research awards, entrepreneurship awards, and has been invited as a research consultant at various industries for his research excellence. At an age of 19, he started his career as a Social Entrepreneur and now mentoring several institutions and budding engineers in India. Recently, he was awarded International Achievers Award 2020 and the CEO of the Year 2021 for his innovation and product development. His diligence and stark sight have achieved his startup the recognition as the one of the fastest growing startups in India.

Dr. Sathiyanarayanan has been awarded with several prestigious awards, being a Scientist, a CEO, an Entrepreneur, a Mentor, an Author, and an Educationist among other hats, he wears. This gentleman has accumulated knowledge and experience across multiple industries at a young age and is now putting it all to together to brighten India's tomorrow.

MOHAN DHOLVAN is currently an Associate Professor with the Sreenidhi Institute of Science and Technology (SNIST), Hyderabad, India. He has 20 years of teaching experience, including nine years in research in electronics and communication engineering. His research interests include speech signal processing, neural networks, image processing, deep learning, and machine learning. He has published many papers in national and international journals and conferences. He has three papers in SCI, five in SCOPUS, and 15 other publications. He also holds seven patents, with six published and one granted. Additionally, he has authored various books on signal processing, image processing, and applied electronics.

T. RAMASWAMY received the Ph.D. degree in wireless communication from JNTUH, Hyderabad, in 2017. Currently, he is an Associate Professor with the Department of Electronics and Communication Engineering, SNIST Hyderabad, India. He has more than 15 years of teaching experience and ten years of research experience. He has published five international journal articles in reputed journals, such as IEEE, Elsevier, and Springer. His research interests include wireless communications, wireless multimedia networks, real time signal processing, 5G communications, and design of pay loads for micro satellites.

SUDHEER HANUMANTHAKARI (Member, IEEE) received the B.Tech. degree in EEE and the M.Tech. degree in power electronics from JNTU, Hyderabad, and the Ph.D. degree in electrical engineering from JNTU, Ananthapuram. He has got a teaching experience of 20 years. He is currently an Associate Professor with the Department of ECE, Faculty of Science and Technology (IcfaiTech), ICFAI Foundation for Higher Education. He has published 27 research articles in peer-reviewed international and national journals with as H-index of 7. His research interests include fuzzy logic, soft computing, machine learning, power electronics drives, and artificial intelligence. He is also a Passionate Learner with certifications in "Data Science and Machine Learning," AI, online teaching pedagogy, patents, and copyrights.

N. ARUN VIGNESH received the B.E. degree in electronics and communication engineering from Anna University, Chennai, in 2009, the M.E. degree in applied electronics from Anna University, Coimbatore, in 2011, and the Ph.D. degree from Anna University, Chennai, in 2016. He is currently an Associate Professor with the Department of Electronics and Communication Engineering, Gokaraju Rangaraju Institute of Engineering and Technology (GRIET), Hyderabad. His Ph.D. dissertation is focused on "Wireless Communications and Networking." He has more than 60 Scopus indexed publications in various national and international journals out of which 19 are indexed in SCI.

S. KANITHAN received the B.E. degree in electronics and communication engineering from Anna University, Chennai, in 2009, the M.E. degree in applied electronics from Anna University, Coimbatore, in 2011, and the Ph.D. degree in wireless communication for signal processing from Anna University, Chennai, in 2020. He is currently an Assistant Professor with the Department of CSE, JAIN University (Deemed to be University), Bengaluru. His research thesis was on "Swarm intelligent distortion less energy efficient techniques for cooperative MIMO-AF systems." He has published his research papers in refereed international journals and international and national conferences. His research interests include recent technologies in wireless communications and signal processing.

RAGHUNANDAN SWAIN (Senior Member, IEEE) received the Ph.D. degree in compound semiconductor-based electronic devices from the National Institute of Technology Silchar, in 2016. Then, he joined as an Assistant Professor. He is currently with the Parala Maharaja Engineering College, a Constituent College of Government of Odisha, Biju Pattnaik University of Technology. His research interests include GaN-based heterostructure devices and nano-channel FinFETs for power electronic applications. He has published 20 international journal articles in reputed journals, such as IEEE, Elsevier, and Springer. He has presented his work in 12 international conferences in the area of semiconductor devices inside India and abroad. He is also guiding four students toward their Ph.D. He is also a regular reviewer of indexed journals of IEEE, Elsevier, and Taylor & Francis. As a principal investigator on one funding research project and a co-principal investigator on another, he carried them out.