Neural Computing and Applications (2021) 33:6671–6684
https://doi.org/10.1007/s00521-020-05447-9

ORIGINAL ARTICLE

Neural-assisted image-dependent encryption scheme for medical image cloud storage

C. Lakshmi[1] · K. Thenmozhi[1] · John Bosco Balaguru Rayappan[1] · Sundararaman Rajagopalan[2] · Rengarajan Amirtharajan[1] · Nithya Chidambaram[1]

Received: 17 January 2020 / Accepted: 14 October 2020 / Published online: 13 November 2020

Abstract

Current medical technology evolves massive reports such as electronic patient records and scanned medical images; such reports are needed to be stored securely for future references. Existing storage systems are not feasible for massive data storage. Fortunately, cloud storage services meet the demand through their properties such as scalability and availability. Cloud computing is encouraged by amazing web innovation and modern electronic contraptions. Medical images can be stored in the cloud area, but most of the cloud service providers keep the client data in the plain text format. Cloud users need to take the responsibility to preserve the medical data with their strategy. Most of the existing image encryption solutions are vulnerable to the chosen-plaintext attack because the increasing power of computers and ingenuity of hackers are opening up more and more cracks in this mathematical armour. This paper proposes Hopfield neural network (HNN)-influenced image encryption technique to withstand against various attacks which optimize and improvise system through continuous learning and updating. These methods provide a critical security feature that adapts itself for day-to-day miracles of the real world. In this scheme, the back propagation neural network has been employed to generate image-specific keys that increase the resiliency against hackers. The generated keys are used as an initial seed for confusion and diffusion sequence generation through HNN.

Keywords Hopfield neural network (HNN) · Back propagation neural network (BPN) · Image-specific key generation · Image encryption · Cloud storage

1 Introduction

In recent days, the advancements in Information Technology (IT) and processing are incredible. Cloud computing is one such kind which is being adopted by various enterprise for hosting their applications and storage. The digitalized data sharing via modern gadgets set the new stage for the distribution of information around the world irrespective of applications. Being shared information through the public, there is a question on the intensity of privacy and security for the personnel and sensitive information [1]. Increased rate of information sharing among various organizations, including medical imaging system users, leads to the adoption of new storage techniques like a cloud [2], edge [3], etc. Most of the online services like e-commerce, telemedicine, online money access, and social network are deployed in the cloud [4].

Cloud has reached its peak in recent days; Storage as a Service (SaS) is the full demanded service by most of the Internet of Things (IoT) applications [5]. Cloud storage data security is a shared responsibility of customer and service provider, so mainly the issues related to medical data privacy need to be well tackled through the proper crypto standards. It is crucial to offer data security for a medical image stored in an open and shared environment like a cloud. From the discussion over the cloud data security, cloud service providers concentrate on security measures about infrastructure, host, and data. However, user data are exposed as a plain text up to a certain level.

✉ Nithya Chidambaram
cnithya@ece.sastra.edu

[1] School of Electrical and Electronics Engineering, SASTRA Deemed University, Thanjavur 613 401, India

[2] TATA Communication, Chennai, India

To address this issue, encryption schemes are suggested to store the data in an encrypted format [6]. Qin et al. proposed a fully homomorphic encryption (FHE) approach to encrypting the image in cloud storage to offer image security where the complexity has been increased even for small scale images [7].

Numerous encryption schemes exist; they can encrypt text, image, and audio. Still, security measure employed for the text transmission presents poor performance for the image, because of the intrinsic features of the images such as bulk data capacity, high redundancy, and high correlation among the pixel data; thus, independent security scheme is required for each type of multimedia data security [8]. Because of the difficulty in handling images when compared to the textual data, image security gains more importance. Besides, most of the sensitive applications, such as telemedicine, education, and biometric authentication, share their context in terms of images. Chaos-based image encryption schemes [9–13] are gained attention due to its enhanced key strength through key sensitivity. The significance of the chaos is that the key has a real value.

As per the chaos theory, chaotic nature purely depends on the initial seed. However, cryptanalysts are reported that chaos-based encryption schemes are not withstood against the chosen-plaintext attack. However, most of the modern cryptographic techniques are subjected to cryptanalysis where the attackers compromise the cryptosystem through known-plaintext and chosen-plaintext attacking schemes.

Reversible exclusive-OR operation has been incorporated in image encryption due to its merits such as reversibility, and it offers bitwise confusion. Also, it feasible to create a stream cipher. However, it allows cryptanalysis through a chosen-plaintext attack [14–20]. The homomorphic encryption scheme is addressed as a leading encryption technique, especially for cloud data security. Yet, the homomorphic encryption scheme has cryptanalysis by Baocang Wang, in which security keys are retrieved with lesser than 8 s [21].

From the above survey, most of the existing schemes are compromised by the chosen-plaintext attack due to their common utility of simple XOR-based diffusion and constant rounds of operation. The rounds of operations may increase the complexity but unnecessary change in execution time which results in poor throughput. To prevent the cryptanalysis and especially the chosen-plaintext attack, the encryption scheme must be complex, reversible, self-adaptive, and parameter sensitive. Neural-based encryption schemes are the desired solution to satisfy the requirements, as mentioned earlier. An artificial neural network (ANN) is a distributed network that can execute the parallel task and the primitive elements called neuron [22]. Integration of ANN with conventional schemes provides accurate results due to its self-learning and adaptive nature. Also, ANN has the calibre to learn the environment through real-time data and training data. Thus, the neural networks are integrated with various applications such as data security, big data analytics, medical data classification, and neural can be utilized in the civil structure analysis [23, 24], in which this paper focuses the data security.

As per the fundamental rule, artificial neurons should resemble biological neurons. Accordingly, it has chaotic behaviour. This chaotic behaviour of neurons gets the attention of the cryptography applications [25].

From the literature, it has been noticed that ANN can be extended to model the reversible complex encoders. Besides, ANN can apply to a non-traditional image encryption scheme. ANN can be modelled as a nonlinear encoder that can be extended to replace the traditional diffusion [26–31]. In addition to the diffusion, random indexes are needed to achieve confusion. To obtain the random indexes, the neural network also needs recurrent behaviour, which is inevitable in the generation of the pseudo-random sequence for image encryption. Thus, this paper proposes recurrent Hopfield neural network (HNN) as a primary component to implement the neural blended adaptive image encryption. A variant type of neural model is called the Hopfield neural network (HNN), which is a recurrent network, and it is derived from the human brain dynamics [32–37]. It exhibits temporal behaviour. It is different from other neural architectures. Because other neural networks consist of independent hidden units to process the inputs, hence the networks are appropriate for classification and clustering applications. Conversely, recurrent HNN has interconnected hidden units, one of the hidden units activates at the time to attain temporal or sequential behaviour. It is useful in the applications based on the sequence of successive events such as pseudo-random sequence generation.

Significances of the proposed algorithm as follows:

- Multilayered architecture and nonlinear transfer function-assisted weight matrix of BPN reduces the probability of prediction of the key.
- Distinctive features of the image are taken as the input for the BPN, thus generated keys are more adaptive to the input plain image.
- Keys can be dynamic due to their self-learning capability of BPN.
- Unique key for every image, thus unauthorized persons cannot hack the image and key using chosen-plaintext attack.
- Confusion and diffusion are implemented using a Hopfield neural network, so this scheme enhances the complexity of the prediction of the algorithm.

- Weight matrix of the HNN can be updated for every image; thus, it produces the image-specific pseudo-sequence generation.
- Image-specific pseudo-sequence generation in turn to attain adaptive confusion and diffusion.
- Due to the recurrent and chaotic behaviour, HNN requires key seeds similar to the chaos which is better than linear neural architectures such as BAM, BPN as the initial key seed larger in size (size is greater than plain image), which increases transmission overhead.
- Establishing connectivity between the authenticated user and the public cloud environment.
- Augmented privacy for medical image repository in the cloud.

The rest of this paper is organized as follows. Section 2 presents pre-requisites such as four-nodes Hopfield neural network (HNN) and its chaotic behaviour analysis. Section 3 presents the proposed scheme with five phases, in which, Phase I presents adaptive key generation using back propagation network, Phase II presents the random sequence generation using HNN and image-specific key, Phase III employs adaptive confusion using random sequence generation. Phase IV includes adaptive diffusion using random sequence generation, and Phase V explains the connectivity establishment between the cloud and the proposed cryptosystem. Section 4 presents the results and discussion. Finally, Sect. 5 presents the conclusions and future work directions.

2 Pre-requisites

2.1 Hyperchaotic HNN

Hyperchaotic HNN has metastable states using external input and chosen previous state [30, 32–34]. HNN is designed with minimum node, selected node connection along with an appropriate asymmetric weighted path, provide the chaotic behaviour.

The proposed work is employed for the four-nodes HNN. In a four-nodes HNN architecture, every node might be connected with every other node, along with external input. Besides, it has self-connection. The output of every node depends on the previous state of the input nodes along with external input. Every node is connected to other nodes with the weighted path. Recurrent HNN is reconfigured as chaotic architecture with four nodes which is illustrated in Fig. 1. In chaotic architecture, each node is considered as an input/output node, which results in a faster generation of the pseudo-random sequence. Thus, it is considered as a kind of hyperchaotic architecture. The speciality of this architecture is that every node is not connected to every other node, and weights are updated using the Hebb rule along with hyperbolic activation function. Besides, HNN has designed with a selected number of nodes, along with the appropriate asymmetric weighted path, to provide the desire chaotic behaviour.

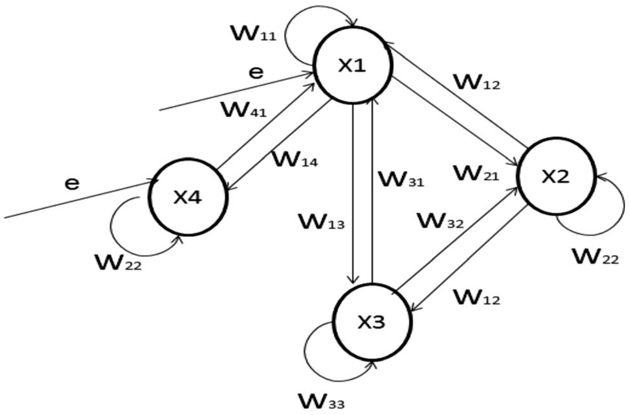


Fig. 1 Architecture of hyperchaotic HNN with four nodes

Chosen Hopfield neural network has four nodes, so the weight matrix dimension is 4 × 4, namely W_{11}–W_{44} as in Eq. (1).

$$W_{ij} = \begin{bmatrix} w_{11} & w_{12} & w_{13} & w_{14} \\ w_{21} & w_{22} & w_{23} & w_{24} \\ w_{31} & w_{32} & w_{33} & w_{34} \\ w_{41} & w_{42} & w_{43} & w_{44} \end{bmatrix} \tag{1}$$

Weight values in Eq. (1) resemble the strength of the neural network through training, which decides the accuracy of the result (percentage of closeness between expected and obtained output). Weight values are either integer or floating decimal which depends on the activation function (identity or hyperbolic activation function). Each node is sequentially updated with the following Eqs. (2) and (3). From Eq. (2), each node receives the weighted signal from other nodes along with external input (e_i) and input from other nodes (X_i). Subsequently, the sigmoid transfer function is calculated using updated X_i as in Eq. (3).

$$\mathrm{Net}(x_i) = N(x_{i+1}) = e_i + \sum_{i=1}^{4} \sum_{j=1}^{4} x_i w_{ij} \tag{2}$$

where Net(x_i) represents some of the weighted inputs.

$$X_{i+1} = \tanh(\mathrm{Net}(x_i)) = \frac{1}{1 + \mathrm{e}^{-\mathrm{Net}(X_i)}} \tag{3}$$

The architecture, shown in Fig. 1, develops the cyclic random sequences using the following Eqs. (4) and (5), which are derived from Eqs. (2) and (3)

$$x_{i+1} = -c_i x_i + \sum_{j=1}^{4} w_{ij} v_j \tag{4}$$

$$v_i = \tanh(x_i) \tag{5}$$

where c_i is constant and $c_1 = c_2 = c_3 = 1$; $c_4 = 100$; x_i is the previous state, and w_{ij} is the weight matrix, respectively.

2.2 Chaotic behaviour analysis of HNN

To attain the chaotic behaviour, node connections should not have symmetrical weights. The chosen weights of the hyperchaotic HNN are given as follows.

$$w_{ij} = \begin{bmatrix} 1 & 0.5 & -3 & -1 \\ 0 & 2+p & 3 & 0 \\ 3 & -3 & 1 & 0 \\ 100 & 0 & 0 & 170 \end{bmatrix},$$

where p is the control parameter.

The chaotic behaviour of the HNN (with control parameter p = 0.3) is visually confirmed in Fig. 2. Figure 2a–c expresses the unstable state generation from X_1 to other states, and Fig. 2d–f expresses the unstable state generation from X_2 to other states. This is the evidence for the chaotic behaviour of the muted HNN which exhibits periodic and chaotic points. This chaotic behaviour depends on the initial seed x_i, weight values, and the control parameter p.

3 Proposed scheme

This paper proposes Hopfield governed image-dependent encryption scheme for medical image cloud storage which is shown in Fig. 3. This framework consists of five phases in which Phase I describes the adaptive key generation using the BPN network;

Phase II presents image-specific random sequence generation using HNN,

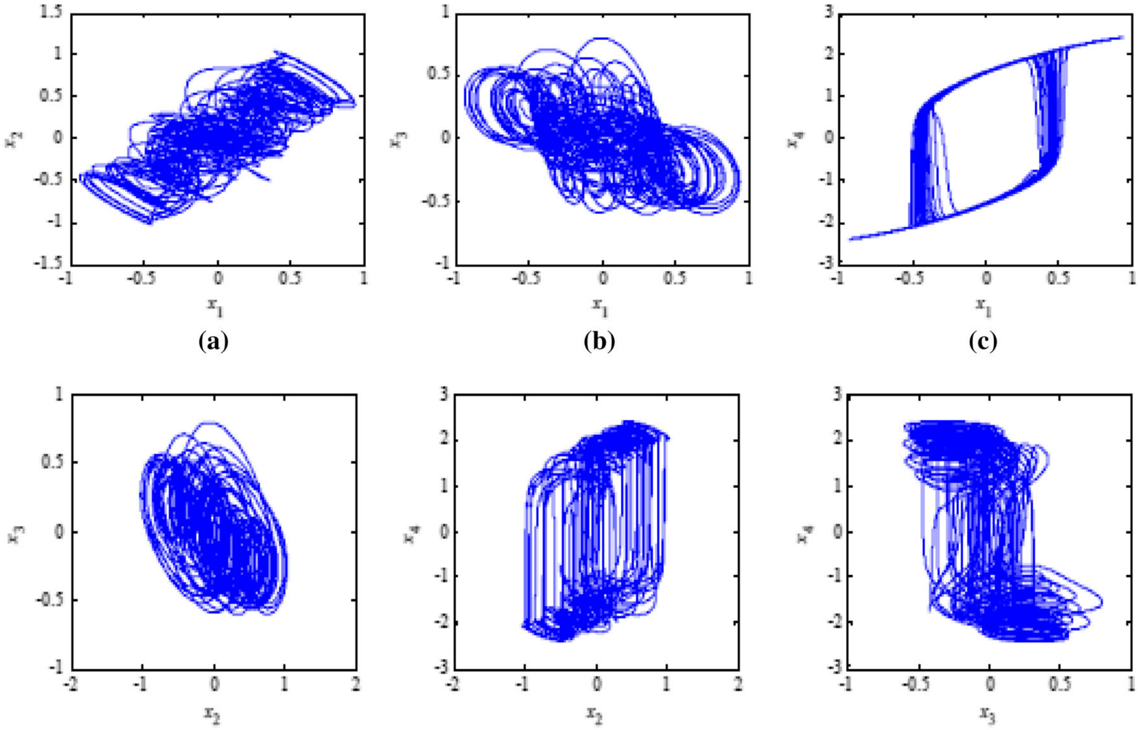
Phase III and IV deal with the confusion and diffusion process, respectively,

Phase V illustrates connectivity establishment between the cloud and the proposed cryptosystem.

In this proposed work, the initial seed and the control parameter are generated from the input image to design the adaptive encryption scheme.

3.1 Phase I: adaptive key generation using back propagation network

Once the key has been deduced, the security of the cryptosystem will be compromised. This research work develops a method to prevent chosen-plaintext attacks using



(a) (b) (c)

(d) (e) (f)

Fig. 2 Chaotic behaviour of HNN with p = 0.3

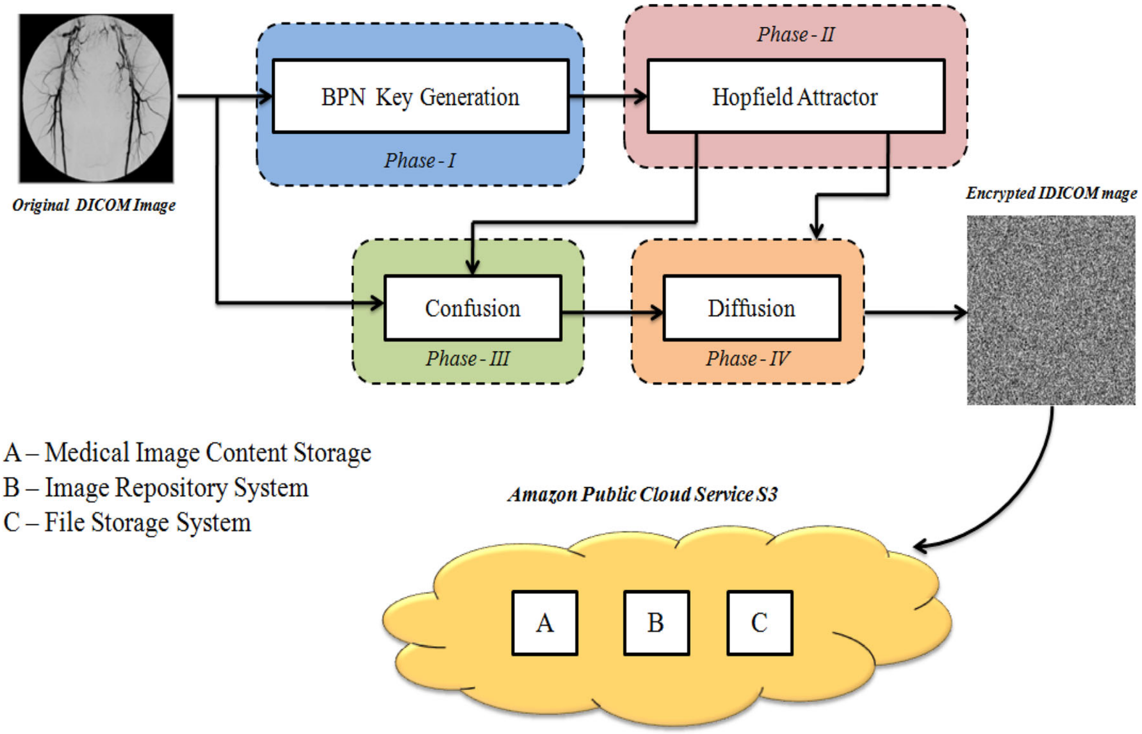


Fig. 3 Discrete Hopfield attractor image-dependent encryption scheme for medical image cloud storage

neural networks. It generates a session key that is unique for every image, as shown in Fig. 4. During training, the set of image features in the dataset is a map to the key using a feed-forward neural network. The network is trained using multilayer BPN with the image features as inputs and session keys as the target. The trained network generates a unique key such a way that if at least one of the image feature changes, the output key must change. As the key generated is adaptive to the image, it can be called an adaptive key generation. Tables 1 and 2 present the training dataset for BPN.

Normalized significant features of the image are extracted and considered as the training inputs for the neural network as shown in Table 1. For the training, the desired unique key of every image is assigned as the target as shown in Table 2. These input and target pairs are used to train the BPN network. It is to be noted that these values

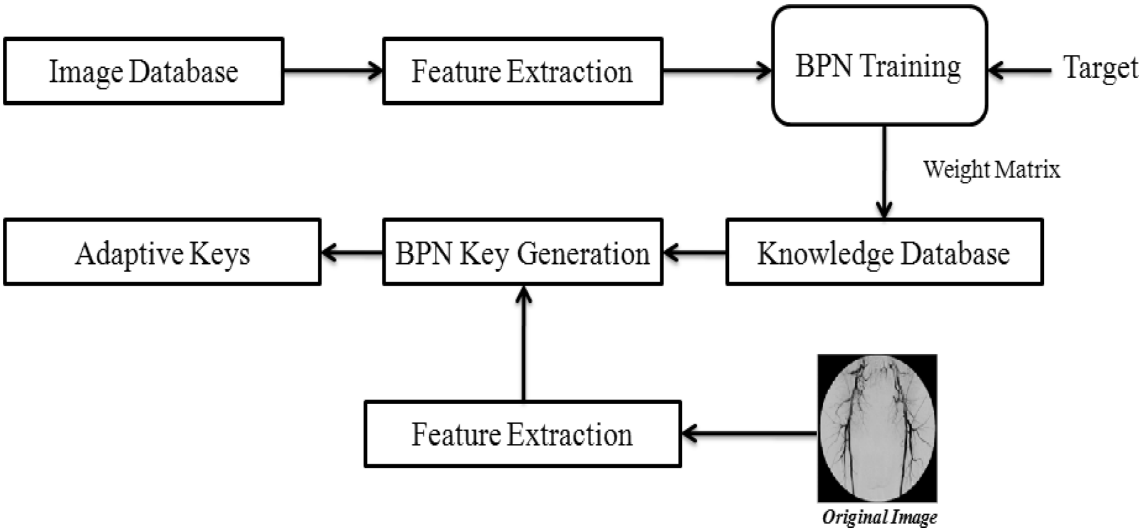


Fig. 4 Adaptive key generation

Table 1 Extracted feature from the images as a training dataset

Test image	Min	Max	DC value	Hist. mean	Entropy	Segment mean	Segment DC value	Segment histogram mean
I1	0.3333	0.0093	0.0357	0.0059	0.9654	0.1944	0.0250	0.0082
I2	0.0277	0.0227	0.0357	0.0167	0.9881	0.3055	0.5000	0.0228
I3	0.0277	0.0160	0.0357	0.0106	0.9968	0.1388	0.5000	0.1116
I4	0.2638	0.1786	0.0357	0.0368	0.9131	0.9444	0.5000	0.0093
I5	0.8055	0.0040	0.0357	0.0011	0.8233	0.2777	0.5000	0.0116
I6	0.4027	0.3809	0.5357	0.1506	0.5094	0.6944	0.5000	0.2898
I7	0.0555	0.0273	0.0357	0.0161	0.1388	0.3969	0.5000	0.0250

Min minimum intensity value, *Max* maximum intensity value, *DC value* DC component of an image, *Hist. mean* histogram mean, *Entropy* entropy of an image, *Segment mean* mean of each segment, *Segment DC value* DC component of segments, *Segment histogram mean* histogram mean of segments

Table 2 Target creation

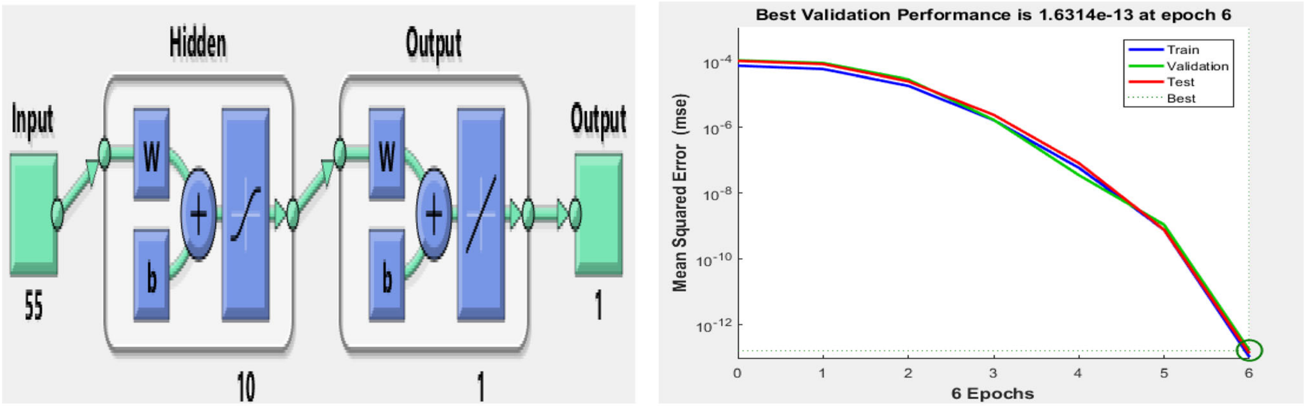
Training image	I1	I2	I3	I4	I5	I6	I7
Target	2.3495	2.36582	2.33447	2.42089	2.35676	2.38254	2.36295

are unique to the image, and hence the output will be changed even with the slight variation of image features.

Figure 5 shows the training performance of the developed multilayer BPN network. Figure 5a illustrates the fitting architecture of multilayer BPN network for the proposed adaptive key generation process in the encryption algorithm. Figure 5b depicts MSE versus the number of epochs. It can be noticed that as the epoch number increases, the MSE decreases. This is since the Net converges to the optimum value at every succeeding epoch. Hence, it can be inferred that the Net finally converges to a global minimum and therefore is with stable weights. The weight matrix finally produced can then be used as an image-specific key generator.

3.2 Phase II: random sequence generation using HNN and image-specific key

The scheme proposed here is to generate the chaos sequences through HNN rather than using nonlinear equations that exhibit the chaotic nature. Image-specific key is considered as a control parameter, and the random sequences are generated using the pseudo-code given as follows.



(a) (b)

Fig. 5 Training performance of the developed multilayer BPN network; **a** BPN fitting architecture with 55 input features, **b** respective training performance graph

Algorithm: Random sequence generation using HNN and image specific key

Input: Multiplicative identity matrix $(B)_{4\times4}$, Sampling rate T_w, Random initiator $h_{1\times4}$

Output: Non-linear random sequence Ω

```
Initialize $w_{ij} \leftarrow [w\ \ w/2\ \ \sigma\ \ -w;\ \Psi\ \ 2w\ \ 3w\ \ 0;\ 3w\ \ \phi\ \ w\ \ 0;\ mw\ \ 0\ \ 0\ \ nw] \leftarrow [1\ \ 0.5\ \ -5\ \ -1;\ -0.37\ \ 2\ \ 3\ \ 0;\ 3\ \ -13\ \ 1\ \ 0;\ 100\ \ 0\ \ 0\ \ 170]$
 Update the $w_{ij}$ with new $\sigma$, $\Psi$, $\phi$
    Get $H(0) \leftarrow [h]^T$
    Repeat
          $f(H(r)) = \tanh H(r)$
          $H(r+1) = (1 - BT_w)\,H(r) + T_w w f\left(H(r)\right)$
          $Dh = \left|\left(H(r+1) - \lfloor |H(r+1)| \rfloor\right)\right|$
    Until $r \leq$ (Image size / 4)
    Initialize $\Omega \leftarrow \{\}$
    for $f \leftarrow 1$ to 16384
        for $i \leftarrow 1$ to 4
            $\Omega((4\times(f-1))+i) = Dh(i)$
        end
    end
  Return (Ω)
```

3.3 Phase III: adaptive confusion using random sequence generation

Two different sets of nonlinear random sequences are generated for the processes substitution and permutation. The detailed flow is given in Fig. 3, which integrates the adaptive and image-specific key generation, confusion, and diffusion. The following section presents part of a detailed encryption algorithm which includes confusion.

3.4 Phase IV: adaptive diffusion using random sequence generation

Second random sequences are considered for the diffusion process, and the detailed algorithm is given as follows

Algorithm: Adaptive confusion using random sequence generation

Input: Plain image I of size M×N, Non-linear random sequence Ω

Output: Scrambled image matrix C' Get $[R, \forall] \leftarrow sort\ (\Omega, \text{'}ascend\text{'})$

```
where R is the ascending order of keystream $\Omega$;
                 $\forall$ is the index of the sorted keystream $\Omega$
                Repeat
                      Set $C'(j) \leftarrow I(\forall(j))$
                Until $j < (M\times N)$
                 Return (C')
```

```
Algorithm: Adaptive diffusion using random sequence generation
Input: Scrambled image matrix C', Non-linear random sequence $\Omega$
Output: Encrypted image e Set key $Y \leftarrow \lfloor mod\ (\Omega * 10^{14}, 256) \rfloor$
    Find $Y(\Phi,\Omega)$=reshape(Y,[256,256])
      Repeat
          $e(\Phi,\Omega) = Bitxor\ (Y(\Phi,\Omega)\ , C'(\Phi,\Omega))$
      Until ($\Phi \le 255$ & $\Omega \le 255$)
      Return(e)
```

3.5 Phase V: connectivity establishment between cloud and cryptosystem proposed

The ciphered medical images of the user are stored into S3 bucket of AWS with sole login credentials. If the user credentials are invalid, then the system denied the access, and it will be handled as a user-defined exception else image access is allowed. The procedural flow is explained as follows:

Step 1 Register with AWS to get AWS_Username and AWS_Password

Step 2 Create AWS secret key pairs for file storage in S3 of AWS

For every cloud access, follow the given steps

Step 3 Match the AWS user credentials with the currently received credentials

Step 4 If step 3 results with "NO", then return with the message 'Access Denied'

Step 5 If step 3 results with "YES", then, match the AWS secret key pairs

Step 6 If step 5 results with "NO", then return with the message 'Invalid Credentials'

Step 7 If step 5 results with "YES", then put the ciphered images into S3 of AWS

4 Results and discussion

The ciphered medical image has been stored in public cloud storage, and authenticated users only can access the cloud to get a ciphered image. The retrieval of the plain image is only through the associated private key(s) employed. Figure 6 illustrates the block diagram for pushing encrypted medical images into S3 bucket of AWS. As evidence, the view of the uploaded medical image in AWS S3 bucket is shown in Fig. 7.

To ensure the resistivity of this developed work, various attack analyses like statistical, differential, encryption quality, bit plane correlation and entropy, keyspace, key sensitivity, computational and time complexity, and chosen-plaintext attack are carried out. The ability of the proposed algorithm is verified with medical images of size 256 × 256. The images before encryption after encryption and after decryption are shown in Fig. 8a–f.

4.1 Statistical analysis

To verify the statistical resistivity of the developed work, correlation analysis, entropy analysis, and histogram analysis are carried out.

4.1.1 Correlation analysis

Correlation analysis is carried out and results are entered in Table 3. Figure 9 depicts the closeness of intensities between the co-located pixels of the medical images before and after encryption.

The adoption of the Hopfield neural network and the key generation using an intrinsic property of the image results in the more adaptive confusion process. As evidence, the average correlation arrived is nearly 10^{-3} in all the direction of the encrypted image as shown in Table 3.

4.1.2 Information entropy analysis

The statistical features like frequency of occurrence and randomness of pixels are the hint to know the image. Any encryption algorithm is capable of attaining the standard entropy values globally as well in local. The global entropy value for an ideal case is expected as 8, and the local entropy also has optimal value for various significance levels such as 5%, 1%, and 0.1%. Table 4 reveals the proposed approach offers the better conversion of a plain image into random noise and also arrived entropies are in the acceptable range. The proposed Hopfield neural attractor updates the weight matrix for every single medical

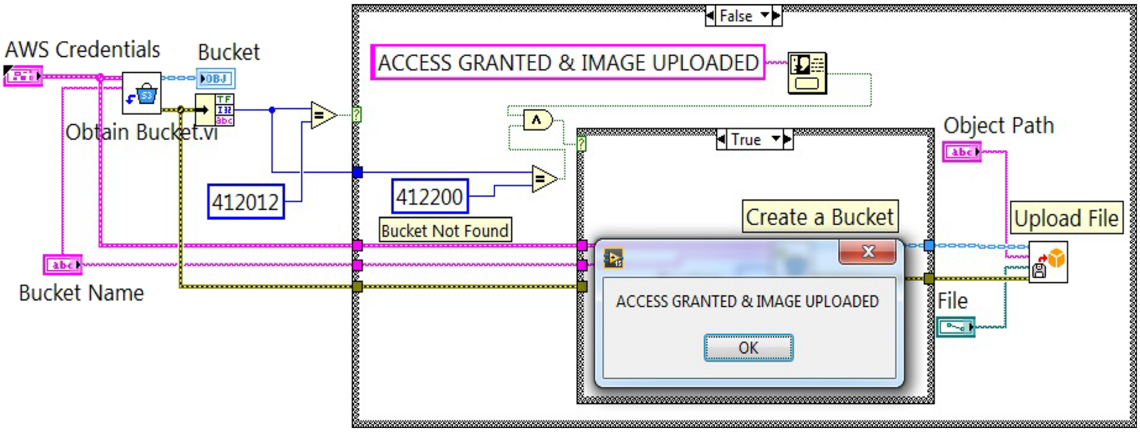
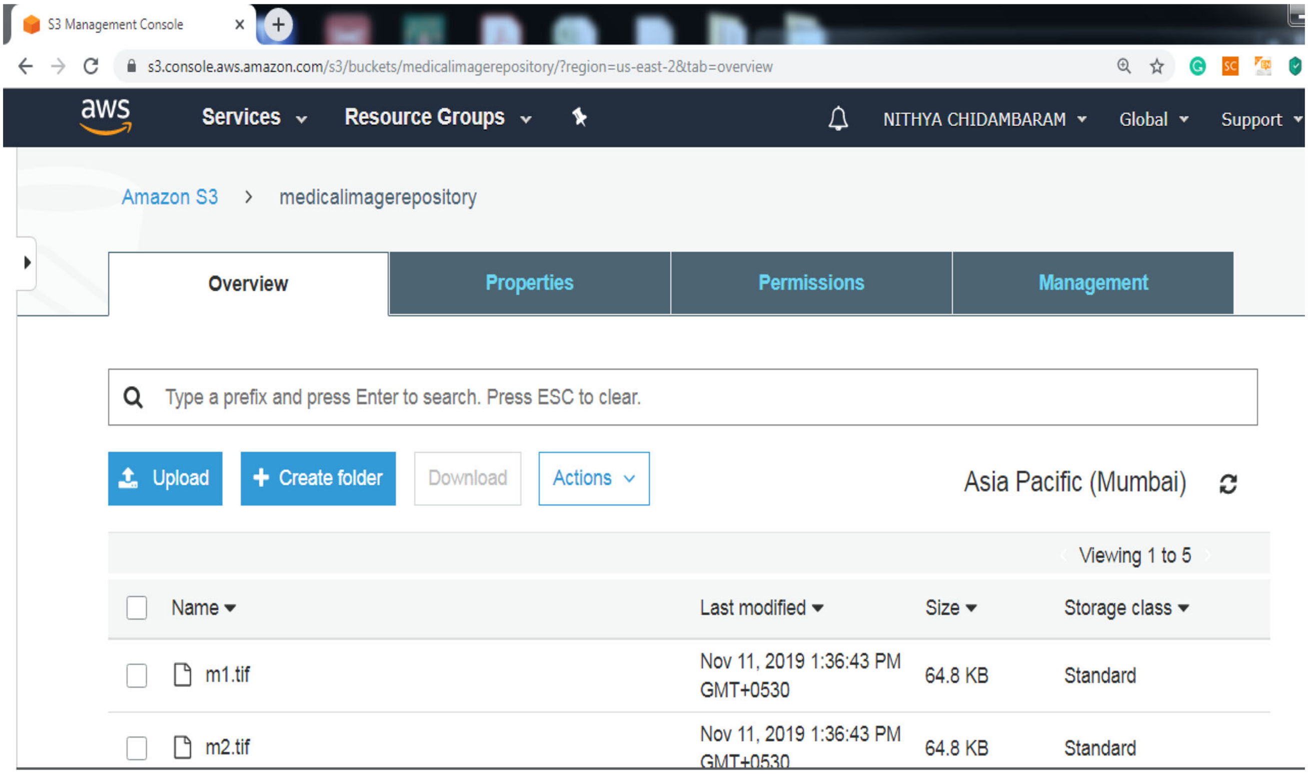


Fig. 6 Block diagram for pushing encrypted medical image into S3 bucket of AWS



Viewing 1 to 5

	Name	Last modified	Size	Storage class
□	m1.tif	Nov 11, 2019 1:36:43 PM GMT+0530	64.8 KB	Standard
□	m2.tif	Nov 11, 2019 1:36:43 PM GMT+0530	64.8 KB	Standard

Fig. 7 Available uploaded medical images in AWS S3 bucket

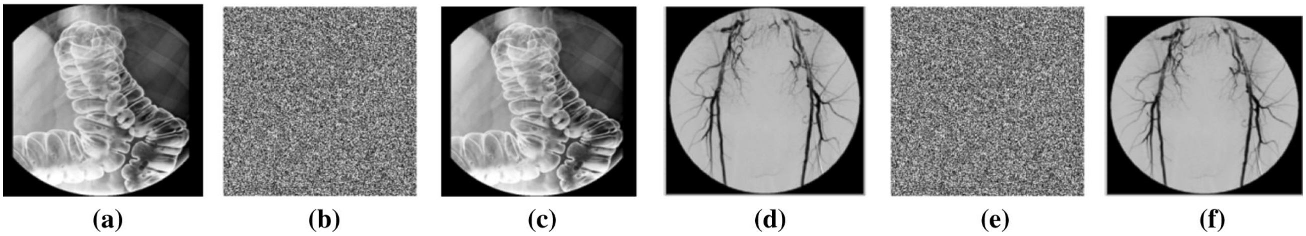

(a) (b) (c) (d) (e) (f)

Fig. 8 Medical: **a** plain (M_1); **b** encrypted ($E_1 = E(M_1)$); **c** decrypted ($M_1 = D(E_1)$); medical: **d** plain (M_2); **e** encrypted ($E_2 = E(M_2)$); **f** decrypted ($M_2 = D(E_2)$)

Table 3 Correlation analysis

Test images	Direction	M_1	M_2	M_3	M_4	M_5
Original image	H	0.9587	0.9635	0.9808	0.9898	0.9948
	V	0.9449	0.9798	0.9760	0.9875	0.9933
	D	0.9196	0.9503	0.9603	0.9801	0.9939
Encrypted image	H	− 0.0064	0.0035	0.0037	− 0.0017	0.0008
	V	0.0031	0.0007	− 0.0038	0.0013	0.0069
	D	0.0004	0.0047	0.0006	− 0.0005	− 0.0012

H horizontal, *V* vertical, *D* diagonal

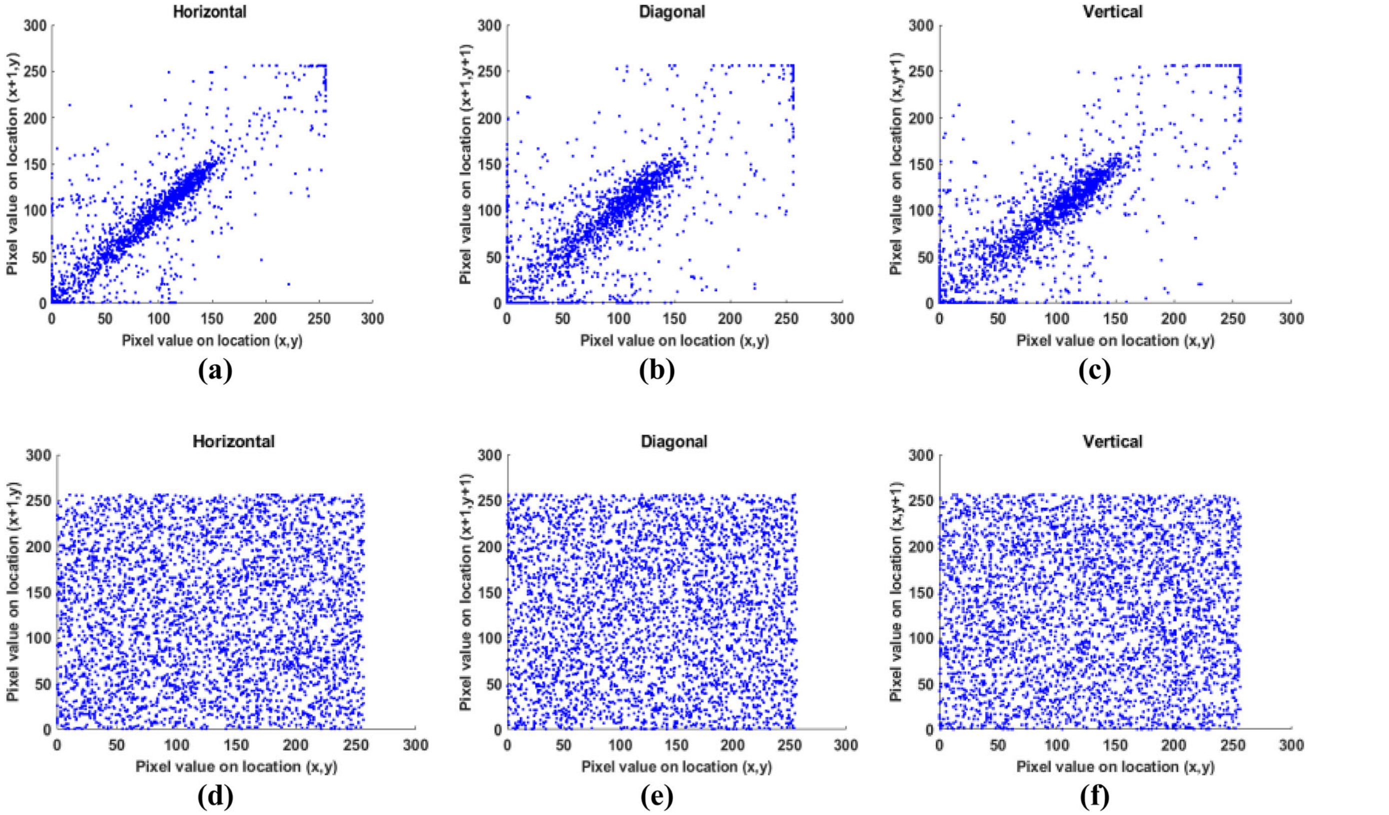


Fig. 9 Adjacent pixels correlation in all the directions of the image (M_1) (**a**–**c**); adjacent pixels correlation in all the directions of the image ($E_1 = E(M_1)$) (**d**–**f**)

Table 4 Randomness analysis

Test images	Global entropy		Local entropy No. of blocks = 30 Block size = 44 × 44
	Original image	Encrypted image	Encrypted image
M_1	4.425	7.9913	7.9017
M_2	5.032	7.9945	7.9031
M_3	6.32	7.9932	7.9023
M_4	6.51	7.9922	7.9000
M_5	4.784	7.9917	7.9033

image, which results in arriving exclusive encrypted images for every single medical image. Due to the adaptive encoding feature of the proposed work, the average entropy of 7.99 has arrived irrespective of original medical images.

4.1.3 Histogram analysis

The uniform pixel intensity distribution over the image plane offers image unpredictability. Figure 10a–c shows the distribution of pixel intensities in the plain medical images M_1, M_2, and M_3, which are not uniformly distributed. Histograms for the encrypted medical images M_1, M_2, and M_3 are represented using Fig. 10d–f where the intensities of the pixels are uniformly distributed.

From the histogram analysis, it is proven that the redundancy of plain medical image pixels is entirely obscured. As a result, the actual pixel intensities are stretched and shifted out from the original and arrived with a flat histogram. The proposed scheme also achieves one of the features to resist a statistical attack.

4.2 Encryption quality analysis

The quantitative analysis for the histogram is also supported to ensure encryption quality. Maximum deviation (MD) and deviation from uniform histogram (DH) are the metrics to do the process as mentioned earlier. Compared to the confusion stage, the diffusion stage needs to be tested for encryption quality. For a different set of sample test images, MD and DH are computed and tabulated in Table 5.

The proposed algorithm carries out the diffusion process in an adaptive manner, so the distribution of pixel intensities is uniform by having the redundancy of pixels with the expected count. From Table 5, the higher value of MD reveals that the encrypted image has deviated from the original.

From Table 5, the DH value for the test images after encryption is very low which indicates that the histogram of encrypted images is close to the ideal one. Due to the complex, nonlinear, and dynamic encoding process as diffusion strategy in the proposed algorithm, occurrence of pixels values is utmost equal.

4.3 Keyspace analysis

According to the cryptographic law, strength for any encryption proposal resides in the key. For a smaller keyspace with smaller exhaustive search, itself algorithm can be broken. The proposed algorithm has a larger keyspace to keep up the potency of the algorithm. Here, the proposal has eight different keys in a set $\{k_1,\ldots, k_8\}$ each with the precision of 10^{14}, so the total keyspace is 10^{112}. Besides, the session keys are also obtained from the inherent features of plain medical images that are used in encryption.

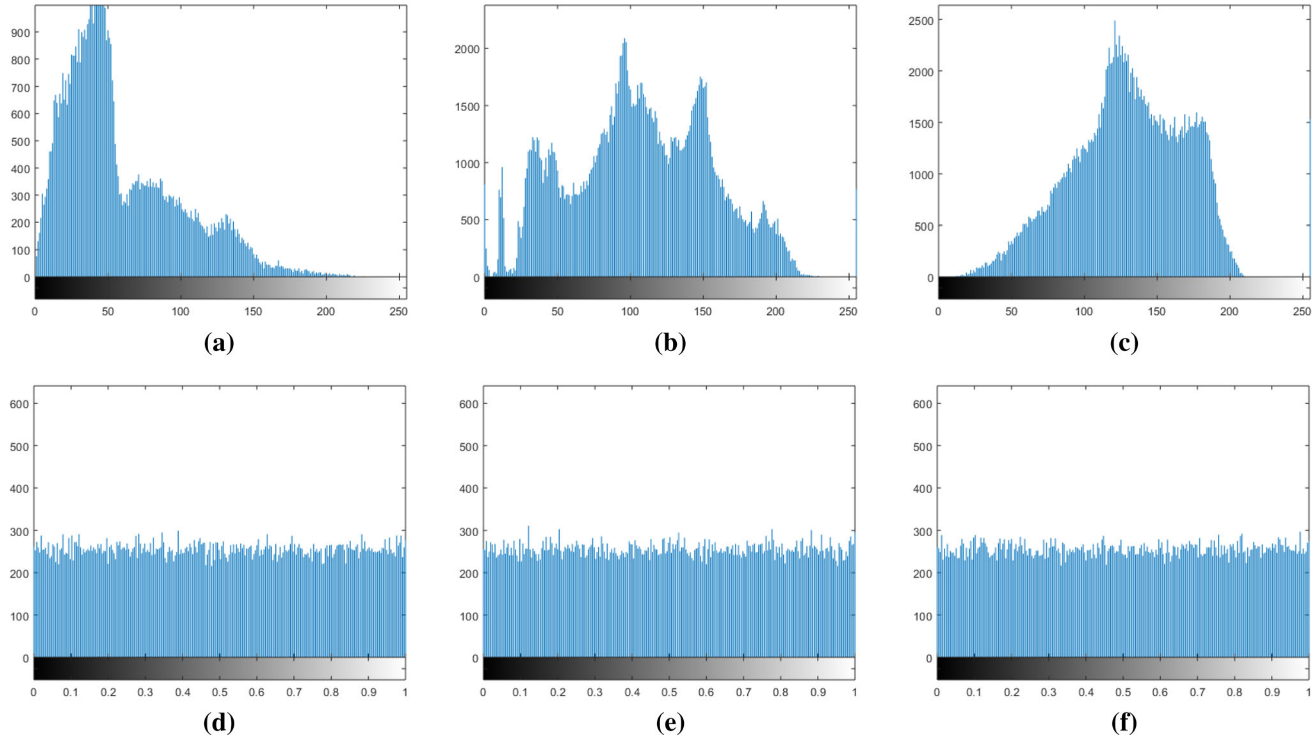


Fig. 10 Histogram analysis for the plain and encrypted image of medical images M_1, M_2, and M_3, respectively (**a**–**f**)

Table 5 Image encryption quality analysis

Encryption quality metrics	M_1	M_2	M_3	M_4	M_5
MD	63,480	89,800	45,019	51,694	86,329
DH	0.0658	0.029	0.03808	0.0271	0.5561

Session keys, together with the key set, are adequate to resist the brute force attack.

4.4 Key sensitivity analysis

Keys perform a vital role in the encryption schemes, and key sensitivity analysis is an important metric to evaluate the robustness of the encryption schemes. Most of the encryption schemes utilize the same key for every image transmission. But the proposed scheme offers an independent and adaptive key for each image using image features. When the key is in the double data type, it can reflect the minor change in the image features. NPCR is measured between the images after a slight change in image content. The test is carried out using the identical image with pixel change, and the pixels are selected from various locations. Tabulated NPCR values in Table 6 are evident to confirm that the proposed scheme generates the independent key after a slight change in image content, and this scheme can resist the exhaustive search.

4.5 Chosen-plaintext attack analysis

XOR-based substitution methods are tested with this traditional analysis to ensure the potential to resist the chosen-plaintext analysis. While examining the resiliency of the proposed scheme against the chosen-plaintext attack, it should satisfy Eq. (6)

$$M_1 \oplus M_2 \neq CM_1 \oplus CM_2 \tag{6}$$

where M_1, M_2, CM_1, and CM_2 are plain medical image 1, plain medical image 2, cipher medical image 1, and cipher medical image 2, respectively. Figure 11a indicates the XOR between medical image 1, medical image 2, and Fig. 11b shows the XOR between the corresponding cipher images, accordingly both the images are not the same which is a visual proof for the ability of the proposed scheme against chosen-plaintext attack. From this analysis, it is clear that the hacker cannot obtain the key by applying the chosen-plaintext attack.

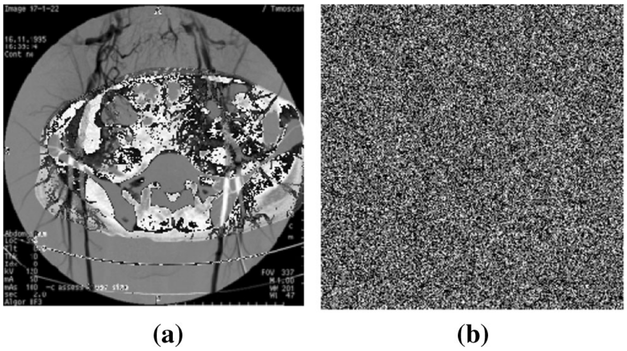


Fig. 11 Chosen-plaintext attack analysis: **a** $M_1 \oplus \mathrm{M}_2$, **b** $CM_1 \oplus \mathrm{CM}_2$

4.6 Computational effectiveness/efficiency

The computational effectiveness/efficiency of the proposed method depends on the pseudo-random sequence generation, permutation, and substitution process. The number of operations that are employed to develop the pseudo-random sequence through HNN is about $O\ \{n\ (M \times N)\}$. Consequently, the number of permutation operations is about $O\ \{2 \times M \times N\}$, and the total number of substitution operations are performed about $O\ \{2 \times M \times N\}$. The proposed scheme is tested with a grey image with a size of 256 × 256, and it takes 0.451 s for the encryption process. Also, the elapsed time for the adaptive key generation is about 0.018845 s for each plain image. The time taken for uploading a file through a WiFi network of speed 130 Mbps into the AWS S3 bucket is 0.546 s. The propagation delay is inversely proportional to network speed.

Table 6 Key sensitivity analysis

Image with % of change in the content (with different location)	Generated key	NPCR (%)
Medical image 1 with 5 pixels change	5.99999999999999909999	99.6262
Medical image 1 with 10 pixels change	5.99999999999990999999	99.5941
Medical image 1 with 15 pixels change	5.99999999099999999999	99.6002
Medical image 1 with 20 pixels change	5.99990999999999999999	99.5544
Medical image 1 with 25 pixels change	3.99099999999999999999	99.5880

Table 7 Comparison analysis

Existing schemes	VC	HC	DC	NPCR	UACI	Entropy
Ref. [9]	0.0017	0.0030	0.0010	99.60	33.47	7.99
Ref. [13]	− 0.0032	0.0031	− 0.0030	99.59	33.45	NA
Ref. [10]	0.0064	0.0035	− 0.0036	99.5705	33.4781	7.99
Ref. [37]	0.0009	− 0.001	0.001	NA	NA	7.99
Ref. [34]	− 0.0036	0.0083	− 0.021	99.6	33.46	7.99
Ref. [12]	0.0092	0.0182	0.0051	99.4	33.04	7.99
Ref. [11]	− 0.0016	0.0043	− 0.0061	99.64	33.43	7.99
Ref. [36]	0.0827	0.0756	0.0485	99.572	33.52	7.99
Proposed scheme	− 0.0038	0.0037	0.0006	99.6	33.41	7.99

4.7 Performance comparison analysis

The proposed scheme is compared with the recent methods using entropy, correlation, NPCR, and UACI. The comparison analysis is shown in Table 7. The proposed scheme is compared with three different modes of techniques such as Refs. [9, 11, 13] are chaos-based encryption, Ref. [10] is inter- and intra-plane shuffling-based encryption, Ref. [12], and Refs. [34, 37] are genetic and neural-based encryption, respectively. Chaos-based works are framed in such a way to resilient against statistical, dictionary attack, but sometimes Chaos-based works fail in entropy when the modality of image changes. Plane- and pixel-wise rotation algorithms offer desire entropy but fail in the keyspace. However, most of the works are cryptanalysis by chosen-plaintext analysis [14–20]. Based on the obtained metric values, the proposed scheme can withstand statistical, differential, and brute force attacks. Besides, the adaptive key generation using the BPN algorithm formulates a strong and image-specific encryption scheme.

Cloud data storage is chosen for data sharing between groups of intended users to avoid multiple transmissions. In such a scenario, every single image storage and transmission demands security. When the cloud is approached for storage, the encryption module should encrypt any type of medical image, and it should result in the desire and uniform metrics. This demand is fulfilled by the proposed scheme using adaptive key generation. In the proposed scheme, the adaptive key from BPN is inserted in the weight matrix of the Hopfield neural network as control parameters, which decide the chaotic behaviour of the HNN. Hence HNN starts self-learning with every plain image, which results in an image-specific random sequence. The image-specific random sequence employs the self-adaptive confusion and diffusion. Due to the self-adaptive property of the proposed Hopfield neural network and unique key for every image transmission, the proposed scheme resists the chosen-plaintext attack. Besides, tabulated metrics prove that the proposed scheme is not compromised with any other metrics, so it can make resilient against statistical, differential, and encryption quality attacks.

5 Conclusion

Cloud storage environments are vulnerable to many security breaches because of open and multi-tendency. When the cloud is approached for the creation of a medical image repository, it’s vital to ensure the security solutions are impenetrable. This proposed solution offers security for the data stored in the cloud storage and for a different state like underuse, at rest, and in transit. The motivation of this work is to build a secure medical image repository in the cloud. Hopfield attractor is a major component of the security system for the medical images to be stored in the cloud, and fitness is also validated using the standard metrics. The proposed work employed Hopfield attractor for the confusion of pixels followed by diffusion has confirmed the resiliency against the various attacks. The proposed work has keyspace 10^{112}. Also, adaptive keys are generated by BPN; thus, hackers cannot predict the key using the chosen-plaintext attack strategy. The integration of supervised and associative neural networks increases the complexity of key and algorithm predictions. In the future, the neural-assisted security solutions will be developed for multimedia data such as colour medical image, audio, and video storage in the cloud.

Acknowledgements Authors thank Department of Science and Technology, New Delhi for the FIST funding (SR/FST/ET-II/2018/221). Also, authors wish to thank the Intrusion Detection Laboratory at School of Electrical and Electronics Engineering, SASTRA Deemed University for providing infrastructural support to carry out this research work.

References

1. Rathore S, Sharma PK, Loia V et al (2017) Social network security: issues, challenges, threats, and solutions. Inf Sci (Ny) 421:43–69. https://doi.org/10.1016/j.ins.2017.08.063

2. Singh A, Chatterjee K (2017) Cloud security issues and challenges: a survey. J Netw Comput Appl 79:88–115. https://doi.org/10.1016/j.jnca.2016.11.027
3. Shahzadi S, Iqbal M, Dagiuklas T, Qayyum ZU (2017) Multi-access edge computing: open issues, challenges and future perspectives. J Cloud Comput. https://doi.org/10.1186/s13677-017-0097-9
4. Asadi S, Nilashi M, Husin ARC, Yadegaridehkordi E (2017) Customers perspectives on adoption of cloud computing in banking sector. Inf Technol Manag 18:305–330
5. Tao M, Ota K, Dong M (2017) Ontology-based data semantic management and application in IoT- and cloud-enabled smart homes. Future Gener Comput Syst 76:528–539. https://doi.org/10.1016/j.future.2016.11.012
6. Nithya C, Pethururaj C, Thenmozhi K, Amirtharajan R (2020) An advanced framework for highly secure and cloud-based storage of colour images. IET Image Process. https://doi.org/10.1049/iet-ipr.2018.5654
7. Qin Z, Weng J, Cui Y, Ren K (2018) Privacy-preserving image processing in the cloud. IEEE Cloud Comput 5:48–57. https://doi.org/10.1109/MCC.2018.111121403
8. Kaur M, Kumar V (2020) A comprehensive review on image encryption techniques. Arch Comput Methods Eng 27:15–43. https://doi.org/10.1007/s11831-018-9298-8
9. Chandrasekaran J, Thiruvengadam SJ (2017) A hybrid chaotic and number theoretic approach for securing DICOM images. Secur Commun Netw. https://doi.org/10.1155/2017/6729896
10. Diaconu AV (2016) Circular inter-intra pixels bit-level permutation and chaos-based image encryption. Inf Sci (Ny) 355–356:314–327. https://doi.org/10.1016/j.ins.2015.10.027
11. Dagadu JC, Li JP, Aboagye EO (2019) Medical image encryption based on hybrid chaotic DNA diffusion. Wirel Pers Commun 108:591–612. https://doi.org/10.1007/s11277-019-06420-z
12. Nematzadeh H, Enayatifar R, Motameni H et al (2018) Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Opt Lasers Eng 110:24–32. https://doi.org/10.1016/j.optlaseng.2018.05.009
13. El Assad S, Farajallah M (2016) A new chaos-based image encryption system. Signal Process Image Commun 41:144–157. https://doi.org/10.1016/j.image.2015.10.004
14. Wang B, Wei X, Zhang Q (2013) Cryptanalysis of an image cryptosystem based on logistic map. Optik (Stuttg) 124:1773–1776. https://doi.org/10.1016/j.ijleo.2012.06.020
15. Özkaynak F, Özer AB (2016) Cryptanalysis of a new image encryption algorithm based on chaos. Optik (Stuttg) 127:5190–5192. https://doi.org/10.1016/j.ijleo.2016.03.018
16. Akhavan A, Samsudin A, Akhshani A (2017) Cryptanalysis of an image encryption algorithm based on DNA encoding. Opt Laser Technol 95:94–99. https://doi.org/10.1016/j.optlastec.2017.04.022
17. Dhall S, Pal SK, Sharma K (2018) Cryptanalysis of image encryption scheme based on a new 1D chaotic system. Signal Process 146:22–32. https://doi.org/10.1016/j.sigpro.2017.12.021
18. Li M, Guo Y, Huang J, Li Y (2018) Cryptanalysis of a chaotic image encryption scheme based on permutation–diffusion structure. Signal Process Image Commun 62:164–172. https://doi.org/10.1016/j.image.2018.01.002
19. Zhang Y (2019) Security analysis of a chaos triggered image encryption scheme. Multimed Tools Appl 78:31303–31318. https://doi.org/10.1007/s11042-019-07894-6
20. Zhang Y (2020) Cryptanalyzing an image cryptosystem based on circular inter–intra pixels bit-level permutation. IEEE Access 8:94810–94816. https://doi.org/10.1109/ACCESS.2020.2995839
21. Bogos S, Gaspoz J, Vaudenay S (2018) Cryptanalysis of a homomorphic encryption scheme. Cryptogr Commun 10:27–39. https://doi.org/10.1007/s12095-017-0243-8
22. Kohonen T (1988) An introduction to neural computing. Neural Netw 1:3–16. https://doi.org/10.1016/0893-6080(88)90020-2
23. Chen Y, Yan J, Sareh P, Feng J (2020) Feasible prestress modes for cable-strut structures with multiple self-stress states using particle swarm optimization. J Comput Civ Eng 34:1–10. https://doi.org/10.1061/(ASCE)CP.1943-5487.0000882
24. Domer B, Fest E, Lalit V, Smith IFC (2003) Combining dynamic relaxation method with artificial neural networks to enhance simulation of tensegrity structures. J Struct Eng 129:672–681. https://doi.org/10.1061/(ASCE)0733-9445(2003)129:5(672)
25. Yu W, Cao J (2006) Cryptography based on delayed chaotic neural networks. Phys Lett Sect A Gen At Solid State Phys 356:333–338. https://doi.org/10.1016/j.physleta.2006.03.069
26. Tang H, Li H, Yan R (2010) Memory dynamics in attractor networks with saliency weights. Neural Comput 22:1899–1926. https://doi.org/10.1162/neco.2010.07-09-1050
27. Qin K (2017) On chaotic neural network design: a new framework. Neural Process Lett 45:243–261. https://doi.org/10.1007/s11063-016-9525-y
28. Kassem A, Al Haj Hassan H, Harkouss Y, Assaf R (2014) Efficient neural chaotic generator for image encryption. Digit Signal Process Rev J 25:266–274. https://doi.org/10.1016/j.dsp.2013.11.004
29. Ma X, Chen X, Zhang X (2019) Non-interactive privacy-preserving neural network prediction. Inf Sci (Ny) 481:507–519. https://doi.org/10.1016/j.ins.2018.12.015
30. Bigdeli N, Farid Y, Afshar K (2012) A novel image encryption/decryption scheme based on chaotic neural networks. Eng Appl Artif Intell 25:753–765. https://doi.org/10.1016/j.engappai.2012.01.007
31. Al Azawee H, Husien S, Yunus MAM (2016) Encryption function on artificial neural network. Neural Comput Appl 27:2601–2604. https://doi.org/10.1007/s00521-015-2028-3
32. Hopfield JJ (1982) Neural networks and physical systems with emergent collective computational abilities. Feynman Comput. https://doi.org/10.1201/9780429500459
33. Hopfield J (1984) Neurons with graded response have collective computational properties like those of two-state neurons. Proc Natl Acad Sci U S A 81:3088–3092. https://doi.org/10.1073/pnas.81.10.3088
34. Wang X-Y, Li Z-M (2019) A color image encryption algorithm based on Hopfield chaotic neural network. Opt Lasers Eng 115:107–118. https://doi.org/10.1016/j.optlaseng.2018.11.010
35. Lakshmi C, Thenmozhi K, Rayappan JBB, Amirtharajan R (2020) Hopfield attractor-trusted neural network: an attack-resistant image encryption. Neural Comput Appl 32:11477–11489. https://doi.org/10.1007/s00521-019-04637-4
36. Lakshmi C, Thenmozhi K, Rayappan JBB, Amirtharajan R (2018) Encryption and watermark-treated medical image against hacking disease—an immune convention in spatial and frequency domains. Comput Methods Programs Biomed 159:11–21. https://doi.org/10.1016/j.cmpb.2018.02.021
37. Bigdeli N, Farid Y, Afshar K (2012) A robust hybrid method for image encryption based on Hopfield neural network. Comput Electr Eng 38:356–369. https://doi.org/10.1016/j.compeleceng.2011.11.019

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.