

A deep learning signed medical image based on cryptographic techniques

Dalia H. Elkamchouchi^{1,2}, Abeer D. Algarni¹, Rania M. Ghoniem^{1,3}, Heba G. Mohamed^{2,4}

¹Department of Information Technology, College of Computer and Information Sciences,
Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

²Department of Electrical, College of Engineering, Alexandria Higher Institute of Engineering and Technology, Alexandria, Egypt

³Department of Computer, Mansoura University, Mansoura, Egypt

⁴Department of Electrical, College of Engineering, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

Article Info

Article history:

Received Jun 21, 2022

Revised Sep 10, 2022

Accepted Sep 28, 2022

Keywords:

Biomedical image security

Cryptography

Deep learning

DNA

Hybrid chaotic

ABSTRACT

Innovative medical multimedia communications technology requirements have enhanced safety principles, allowing significant advancement in security standards. In hospitals and imaging centers, massive amounts of medical images have been created. To successfully access the medical databases and utilize those rich resources in assisting diagnosis and research, image processing enabled communication solutions are necessary. Our article presents a rigorous verified model by employing deep learning to enhance the cryptographic performance of biomedical images using hybrid chaotic Lorentz map diffusion and de-oxyribonucleic acid (DNA) confusion stages. It consists of two encryption/decryption techniques, the initial signal is verified using digital signature and two unique non-consecutive stages of chaotic diffusion with a single DNA scrambling stage in between. The encoded secret bit stream is generated and used to encrypt or decode the original signal in the diffusion manner to disintegrate the redundancy in the plain image statistics, utilizing hybrid chaotic system. Using DNA confusion step to make the relationship between the original signal and the utilized key more ambiguous. These stages make the proposed image cryptosystem more resistant to known/chosen plaintext assaults. The performance of the suggested technique will be assessed to the most similar techniques reported in the literature for comparative purposes.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Dalia H. Elkamchouchi

Department of Information Technology, College of Computer and Information Sciences

Princess Nourah bint Abdulrahman University

PO. Box 84428, Riyadh 11671, Saudi Arabia

Email: dhelkamchouchi@pnu.edu.sa

1. INTRODUCTION

Secure multimedia communications in modern communication networks are a very important process. Several research studies have recently been dedicated to the development of several schemes strengthening digital images. At these days, deep neural network presents superior results even in existence of amorphous data which is totally independent toward the data labelling. Deep learning (DL) [1]–[3] represents a technique kind of representational learning which learns abstract mid-/high- level features embedded in the images. In between the DL advantages, the ability of learning the complex patterns. DL algorithms, especially, convolutional neural networks (CNNs), convolutional neural networks, employ hidden layers in between the inputs and outputs to model the intermediate representations from image data which cannot be easily learnt by other algorithms. Thus, they directly produce high-level representations of features from the medical raw

images. CNNs [3], [4] that are networks inspired biologically, have many crucial contributions in the domain of medical image analysis, e.g., organ segmentation [5], texture analysis, and disease classification [6]. Recent studies revealed that the deep learning algorithms can offer an optimal form of encryption approach of images. Maniyath and Thanikaiselvan [7] proposed an integrated deep learning model with chaotic map for optimized security performance. The computational complexity was assessed with regard to computational processing time and memory consumption. The proposed algorithm was characterized by quick response time (30.18 s) in addition to satisfactory retention of signal quality. Hassan *et al.* [8] presented a secure content-based image retrieval (CBIR) framework which performs image recovery on the cloud without any user's interaction. A generic pre-trained deep neural network type (e.g., VGG-16) was applied to obtain the feature vectors of an image at the user side. The cloud servers apply secure image inference with a pre-trained private deep network model and perform approximate nearest neighbor (ANN) image retrieval protocols without any more interaction of the user.

Guo *et al.* [9] a privacy-preserving CNN framework allowing the search-ing and classification of content-based, secure, big-scale ciphered images (incorporating big-size medical images) using the homomorphic encryption algorithm. The experiment results were implemented using four real-world datasets, (i.e., retinal OCT images, blood cell images, chest X-Ray images, and Caltech101 image set). The experimental conclusions showed that their proposed framework achieved above 86% accuracy rate on the real-world datasets along with the same CNN structure of the plaintext domain having much less searching time (faster more than six times) contrasted with other current systems.

Hashemi and Mozaffari [10] proposed a noise-generative adversarial network (Noise-GAN) GAN to perform targeted and non-targeted assaults opposed to deep neural networks. The Noise-GAN has a multi-class discriminator intended for creating a noise which when added to the original plain image, adversarial cases can be attained. Distinct types of elusion attacks were beholden, and the suggested technique performance was evaluated on several victim examples underneath several defensive approaches. where the experiment results were dependent on MNIST and CIFAR10 datasets and reporting and comparing the average success rates for various attacks with state-of-the-art techniques. The non-targeted attack success rates on deep neural networks (DNNs) after training by adversarial models, produced by Noise-GAN, were rejected from 87.7% to 10.41% utilizing MNIST dataset and rejected from 91.2% to 57.66% utilizing CIFAR-10 dataset.

On the other side the chaos behavior of chaotic map also provides comprehensive security. Consequently, integration of deep learning, chaotic behavior and DNA computation can offer a superior method for image encryption algorithms. Digital images have discriminative properties within the neighboring pixels, for instant broad spectrum and high correlation. In this manner, unused plans, and approaches, such as deoxyribonucleic corrosive (DNA) [11]-[13] also chaotic maps [14], [15] have been utilized in advanced computerized picture encryption plans. These approaches offer assistance to make strides vigor averse to chosen/known plaintext assaults, enhanced factual characteristics, upgraded key domain, revise the plaintext content affectability, up-dating key affectability preference to prior plans. Telem *et al.* [16] have introduced strong encryption system for gray image utilizing artificial neural network and chaotic logistic map, employing an external private key to obtain initial conditions used for generating weights and biases matrices of the perception of the multi-layer, achieving an improved security. Dridi *et al.* [17] presented a new cryptographic system which is based upon a combination of neural network and chaotic functions, as the purpose of using this procedure compared with the present methods is to confirm the security of medical images using minimal complex process, which is compatible along with digital imaging and communications in medical specialty.

Dowlin *et al.* [18] have employed the machine learning method with problems involving medical, monetary, and other forms of precise data, which needs sensible consideration to providing data confidentiality and secrecy. By sending encrypted data to the cloud service hosting the network. The ciphered data stays private since the keys of the decryption process are not known by the cloud. Lakshmanan *et al.* [19] synchronized an inertial neural network and applied it to secure wireless transmission lines. The encryption process utilizes the chaotic signals generated by the inertial neural network. In the results, the encryption scheme is found to be efficient and reliable for secure communication. Shifa *et al.* [20] implemented a joint cryptostego algorithm for improved image security. It was demonstrated that the system is efficient when used with RGB images with varying sizes and resolutions. Li *et al.* [21] suggested a deep learning-based iris image cryptographic algorithm which can resolve the inconsistent iris features and enhance the secrecy of the encrypting and decoding procedures, according to simulated studies performed on iris samples from the public iris database. Ali *et al.* [22] created a deep-learning-based safe searchable blockchain as a data structure utilizing homomorphic encryption, allowing users to access data securely through searching.

Ding *et al.* [23] proposed a deep learning-based key generation network (DeepKeyGen) to encrypt or decrypt medical images using a stream cipher. In this paper, an authenticated secured algorithm based on deep learning is presented using mixed chaotic Lorentz maps and DNA confusion stages. The main contributions of the paper are:

- In order to improve the performance and the security analysis of the proposed algorithm, The VGG16 convolutional neural network is employed as the main learning network for transferring the medical image from its original domain into the target domain.
- Furthermore, an encryption and decryption schemes uses a new scrambling stage at the beginning of the process to be robust against multiple attacks. The displayed calculation is given in a precise numerical dialect with no extraordinary components and tried against the list given in [24].
- The key space of the calculation is evaluated and examined. Diffusion processes are illustrated in arithmetic equations and DNA is shown with numerical examples. As Kerckhoff's method follows, it does not rely on any secret factors but rather on the key.
- In addition, Shannon's two primitive principles also apply here as it includes two non-consecutionary stages of spread utilizing hybrid-chaotic outlines and one disarray arrangement between them. Based on the numerical investigation, it passes numerous measurement and arbitrariness tests, including histogram analysis, a number of pixel change rate, a bound together normal change concentration, and numerous relationship tests since its score is substantially bigger than already displayed plans. It is more resistant to brute force attacks, differential cipher pictures, and entropy attacks than past methods. As a result, it includes a wider key space Additionally, it is also more sensitive to slight variations in the chosen secret key.

The following is the outline of the paper: section 2 offers some broad theoretical foundations. Section 3 is subdivided into three subsections, beginning with datasets of liver computerized tomography (CT) images, deep feature extraction using CNN, and lastly a detailed explanation and argument for the deep feature encryption algorithm. Section 4 introduces the experimental results and analysis. Finally, section 5 concludes our paper.

2. THE COMPREHENSIVE THEORETICAL BASIS

2.1. Convolutional neural network

CNNs comprise a sequence of processing layers with different types [25]-[27]. Regular CNNs have convolutional, fully connected, as well as pooling layers. The most intensive part in CNNs is indicated as the convolutional layers convolving the 3-D kernels to the input feature maps so as to produce output feature maps. Nodes of such feature maps are known as activations. The convolution in a 3-D kernel over an input feature map generates one output feature map. Thus, the count of feature maps produced in this layer equal to the count of kernels. The architecture of CNNs as feature extractors is shown in Figure 1. While Figure 2 demonstrates the convolution process. A fixed-size kernel is employed to multiply corresponding elements in each sub-region of input matrix then find their sum to be one element of the new matrix. Thereafter, the convolutional kernel slides with fixed stride (in Figure 2 the stride is 2); the process is done again until all elements in the input are involved; eventually, a new matrix is formed and then nonlinearly mapped by activation function i.e., rectified linear unit function, ReLU, which saves positive activations unaltered, and adjusts negative ones to zero. Pooling layers come after the convolutional layers and perform by down-sampling output feature map through summarization of its embedded features into patches. In this context, computation of pooling is performed by obtaining the mean from each patch inside the feature map or taking the greatest value in each patch. Figure 3 depicts a max-pooling process, the pooling dimensionality is $10 \times 10 \times 10$, stride value is 2, and kernel size is 2×2 . The pooling output is reduced to $10 \times 10 \times 5$.

The input to the fully connected layer (F-C) is the output from the final pooling or convolution layer that is flattened and passed into it. A node in this layer is linked to all nodes from the previous layer. Final F-C layer outputs probability of any object class with one class node [28].

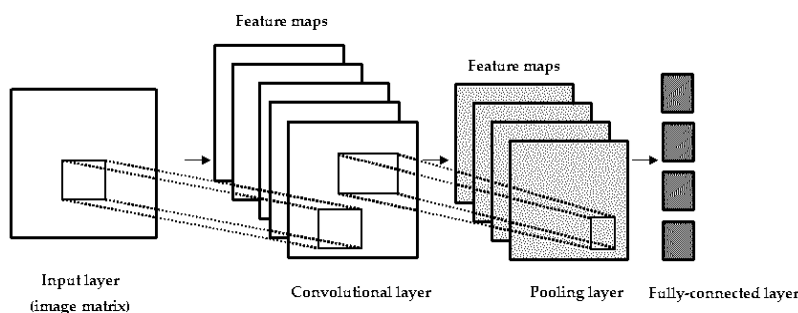


Figure 1. Basic architecture of the CNN

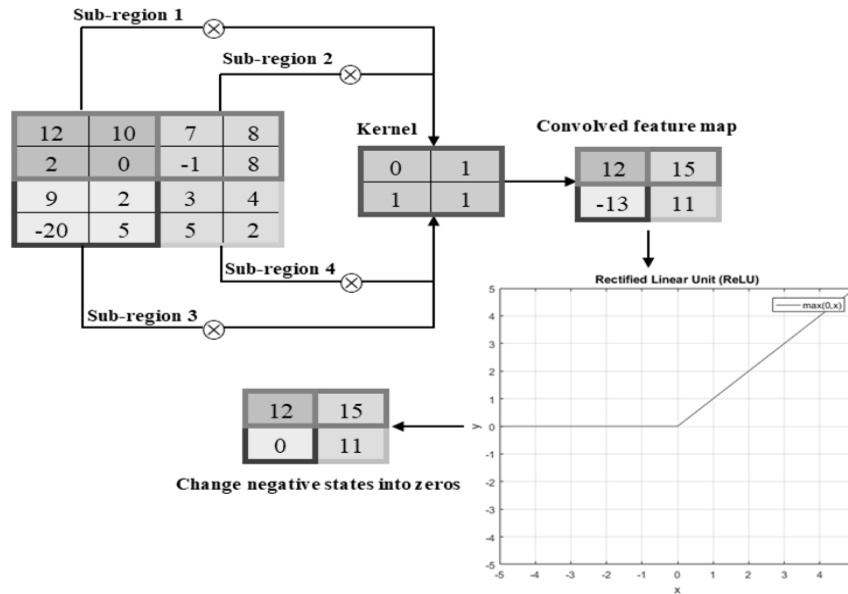


Figure 2. Convolution process followed by rectified linear units (ReLU) activation

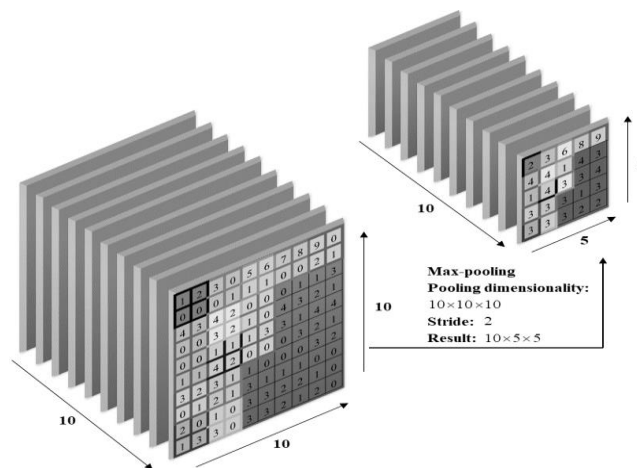


Figure 3. Max-pooling using 2 × 2 filters along with stride of 2, as observed the size of each feature map is diminished to the half

2.2. Hyperchaotic lorenz system

In hyperchaotic Lorenz maps [29], $\alpha, \beta, \varepsilon$ and ω are real constant parameters that determine the chaotic behavior and bifurcation. When $\alpha = 10, \sqrt{\beta} = \frac{8}{3}, \varepsilon = 28,$ and $\omega = 1$ the system behaves hyperchaotically. It is always considered $x_{01} \in (-40,40), x_{02} \in (-40,40), x_{03} \in (1,81),$ and $x_{04} \in (-250,250)$ part of the secret key to obey the initial state obeying and matching the upper and lower bounds of the choice of initial state. With the fourth order Runge-Kutta method [30], one can discretize (1) at 0.002 steps.

$$\begin{aligned}
 \dot{x}_1 &= \alpha(x_2 - x_2) + x_4, \\
 \dot{x}_2 &= \varepsilon x_1 - x_2 - x_1 x_3, \\
 \dot{x}_3 &= x_1 x_2 - \beta x_3, \\
 \dot{x}_4 &= -\omega x_4 - x_2 x_3
 \end{aligned}
 \tag{1}$$

2.3. DNA cryptography

Research in DNA computation and new technologies have led to a novel field called DNA cryptography, which makes use of the understanding of DNA structures to provide unbreakable algorithms. In

terms of DNA sequence, it is used to hide data as it is transmitted or stored. The deoxyribonic acid molecule is a complex molecule from which all of the information required to build and maintain an organism can be obtained. DNA is made up of long polymers of nucleotides, which are the building blocks of DNA. Nucleotides comprised of Deoxyribose sugar, a phosphate group, and nitrogenous base. Adenine (A), cytosine (C), guanine (G) and thymine (T) are the four nucleic acids that make up nitrogen base. By pairing two nucleic acid chains together, DNA forms a double helix. As an example, A and T are complementary pairs; G and C are alternative complementary pairs. Binary operations consist of the 0 and 1, which means that 00 and 11 and 01 and 10 are complement pairs. The nucleic acid bases A, T, G, and C can be coded as 00, 11, 10 and 01, respectively. Table 1 lists the eight DNA encoding rules in use that satisfy the complementary rule [31].

Table 1. Eight DNA mapping rules

1	2	3	4	5	6	7	8
00-A	00-A	00-C	00-C	00-G	00-G	00-T	00-T
01-C	01-G	01-A	01-T	01-A	01-T	01-C	01-G
10-G	10-C	10-T	10-A	10-T	10-A	10-G	10-C
11-T	11-T	11-G	11-G	11-C	11-C	11-A	11-A

2.4. Digital signature algorithm

The digital signature scheme is an asymmetric cryptosystem enables people to electronically sign their documents in a secure and efficient manner. That it is difficult to forge the signature yet verifying the validity of the digital signature is easy. A private key is used to sign the message producing the signature, and then being verified using public key so that no one can sign the message except the party having the private key, but all parties can verify it. Digital signature confirms confidentiality via the following three attributes authentication, integrity and non-repudiation. Digital signatures are employed extensively in banking applications, software distribution, and in many other situations concerning authority, it is crucial to disclose falsification or impersonating [32].

3. METHOD

3.1. Datasets of liver CT images

The proposed approach of this study was tested based on publicly available dataset, which was previously tested in [5], [33] namely, LiTS, which encompass 131 scans of CT images, in addition to their clinical annotation (ground truth). The dataset of LiTS also comprises a number of 70 images as a testing set, but no accompanying annotations are provided for that set. Therefore, in this work, we only employed the 131 annotated set of images.

3.2. Deep feature extraction using CNN

In this work, the VGG16 deep network is employed to extract the deep features from the medical raw images as given in Figure 4, which comprises the following layers:

- Input layer: is the first layer of the network architecture that passes the patches into the network to generate features as in Figure 4. The network adjusts automatically each patch image into 224×224 size to be suitable to the subsequent feature extraction.
- Convolutional layer: in l th convolutional layer, subsection of each input batch image is to a convolutional operation is performed. Supposing h_c indicates an input batch image from l th convolutional layer, then a k th kernel with $m \times m$ size is sliding across the input using stride s . Let f_l be the number of filter channels, $w_l^{i \in f}$ and $b_l^{i \in f}$ denotes the weight as well as bias of i th filter, as shown in (2) defines the output of l th convolutional layer.

$$m_l^i = \sigma(w_l^i - h_l + b^i) \quad (2)$$

where σ denotes the activation function used for mapping input to non-linear space. The output m_l^i represents feature map resulted from the medical image. Afterwards, the result (feature maps). At l th convolutional layer will be activated by employing an activation function in order to obtain non-linear features. In this model, a ReLu [34] activation was used, which inverses each input x from negative into positive and stores the positive values, by using (3). The $\max(0, x)$ refers to ReLu function whereas $F(x)$ represents the output from ReLu.

$$F(x) = \max(0, x) \text{ where } \frac{\partial F(x)}{\partial x} = \begin{cases} 0 & \text{if } x \leq 0 \\ 1 & \text{if } x > 0 \end{cases} \quad (3)$$

- Pooling layer: Max-pooling for output feature maps is performed using (4), x indicates the output for convolution layer, where $R_{i,j}$ refers the (i, j) th region of pooling, while $P_{i,j}$ denotes the max-pooled output.

$$P_{i,j} = \max_{r,s \in R_{i,j}} \{X_{r,s}\} \quad (4)$$

- Fully-connected layer: Probability distribution of the output from the last pooling layer is computed using the softmax formula in (5). The resulted vector size is 1×1000 .

$$\text{softmax}(r)_j = \frac{e^{r_j}}{\sum_{i=1}^c e^{r_i}} \quad (5)$$

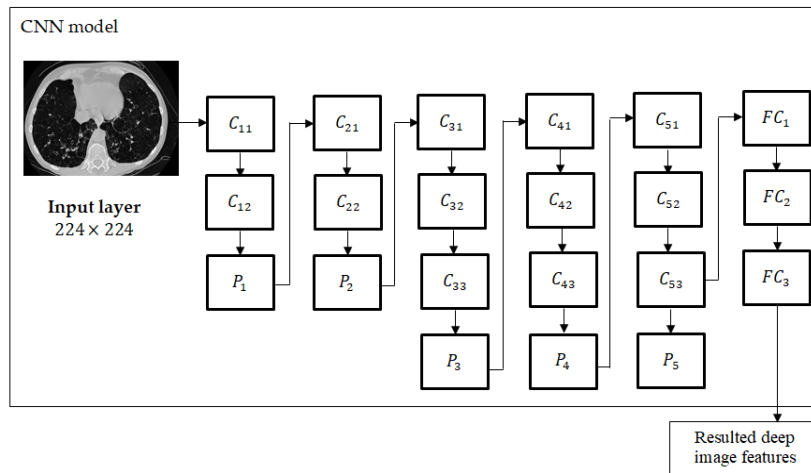


Figure 4. Deep feature extraction using CNN

3.3. Deep feature encryption algorithm

Our proposed system architecture is demonstrated in Figure 5. Firstly, a signal is input to the system and analyzed to get its features. Then the proposed encryption algorithm is applied to the resultant deep image's features based on a forward diffusion stage using hybrid-chaotic Lorenz function, followed by a confusion stage using DNA, and signed with a digital signature using MD5. The proposed cryptosystem consists of same encryption and decryption procedures, simplifying the securely signal transmission and reception implementation systems.

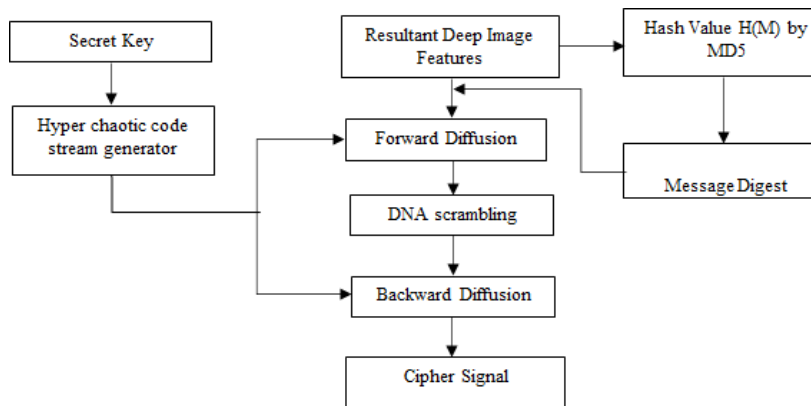


Figure 5. Proposed system architecture

For both transmitting and receiving schemes, two distinct non-successive stages of forward and backward diffusion using the hybrid-chaotic stream generator are used, with a DNA scrambling stage engaged between them. The lorentz hybrid-chaotic system generates a coded secret stream of bits which is used to encrypt or decrypt the original signal employed in both forward and backward diffusion procedures, so as to disperse the redundancy of the statistics of the plain image, while the stage of the confusion using DNA is used for increasing relationship complexity between both the original signal and the employed key.

3.4. Binary image encryption

Let M_o represents the original transmitted medical image, and V_B is the resultant deep image features binary vector, representing the original image M_o from the fully-connected layer, the resultant vector size is 1×1000 Binary bits. The V_B is then represented in the form of a Matrix M_B , in which M_B is the binary image output matrix having the same dimensions of the original image Matrix M_o with size $L \times N$ where L and N are correspondingly the size of both, the columns and rows of the matrix. The proposed image encryption scheme is illustrated in Figure 5. Its private key is given by: $S = \{x_{01}, x_{02}, x_{03}, x_{04}, v_1, v_2\}$, where x_{01}, x_{02}, x_{03} and x_{04} are known as initial conditions for the four dimensions hyperchaotic function, having ranges of values as follows $x_{01} \in (-40,40), x_{02} \in (-40,40), x_{03} \in (1,81)$, and $x_{04} \in (-250,250)$ where v_1 and v_2 are eight bit random numbers chosen by the user. The size of the step x_{01}, x_{02}, x_{03} is given by 10^{-13} even though the size of the step x_{04} is given by 10^{-12} . In the encryption procedure, Reiterating the hyperchaotic system results in two pseudo-random matrices, R and Z , which are used to encrypt the Binary picture. The identical techniques used in the encryption process are used to generate the pseudorandom matrices in the decryption algorithm. The decoding and encryption algorithms used in the proposed approach use the same steps of the image forward diffusion stage, DNA confusion stage, and backward image diffusion to scramble the results. The algorithm has four primary steps, which are illustrated in the following sections. The user selects eight-bit random numbers v_1 and v_2 . This model has a step size of 10^{-13} for x_{01}, x_{02}, x_{03} , while x_{04} is 10^{-12} . By repeating the hyperchaotic system to encrypt the Binary image, two pseudo-random matrices R and Z are generated. Pseudorandom matrices are created by the same methods used in the encryption algorithm during decryption. The decryption and encryption algorithms in the presented scheme are the same. The forward image stage counts the same stages, and the DNA sequence stage uses the backward diffusion to scramble the outcome. There are four stages contained within the algorithm, as described in sub section.

3.5. Streaming code generator

The hyperchaotic Lorenz system, given by (1), is used to generate two pseudorandom matrices, R and Z , of size $L \times N$. Start by iterating this equation for times to get four pseudo-noise streams, designated $\{x_{01k}\}, \{x_{02k}\}, \{x_{03k}\}$ and $\{x_{04k}\}, k = 1, 2, \dots, L \times N$, separately, commencing with the 4 initial values specified in the private key K_s . From the sequences $\{x_{01k}\}, \{x_{02k}\}$, produce the two matrices R, Z by:

$$R(i, j) = F \left((r_{(i-1) \times N + j} + 500 \text{mod} 1) \times 10^{13} \right) \text{mod} 256 \tag{6}$$

$$Z(i, j) = F \left((z_{(i-1) \times N + j} + 500 \text{mod} 1) \times 10^{13} \right) \text{mod} 256 \tag{7}$$

$F(\cdot)$ gives the largest principal integer number, and "+500" is used to convert any negative numbers into positives. Both forward and backward diffusion are done in the encryption process by using these two matrices.

3.6. Stage of forward diffusion

During the given stage, the algorithm builds a new matrix indicated by S by employing XOR (\oplus) operations to both matrices M_B and R of the binary image element as shown in:

$$S(1,1) = M_B(1,1) \oplus R(1,1) \oplus v_1 \tag{8}$$

$$S(1, l) = M_B(1, l) \oplus R(1, l) \oplus S(1, l - 1), \text{ for } l = 2, 3, \dots, L \tag{9}$$

$$S(k, 1) = M_B(k, 1) \oplus R(k, 1) \oplus S(k - 1, 1), \text{ for } k = 2, 3, \dots, N \tag{10}$$

$$S(k, l) = M_B(k, l) \oplus R(k, l) \oplus S(k - 1, l) \oplus S(k, l - 1) \oplus S(k - 1, l - 1), \text{ for } k = 2, 3, \dots, L \text{ and } l = 2, 3, \dots, N \tag{11}$$

in subsequent sections, the output matrix S will be input into a subsequent step of DNA scrambling.

3.7. DNA mutation scrambling stage

For the encryption scheme to resist the chosen/known plaintext assaults, a novel scrambling phase depending on the mutation of the DNA. Applying this phase strengthens the complexity comparative among binary image, ciphered image, and employed key. A slightly change in the binary image or key causes a huge discrepancy in the ciphered image with consent. The following steps shows how scrambled matrix is obtained: i) matrix S is divided into two matrices of equal size by choosing the odd columns all together and form the one matrix SO then again choosing the even columns and form the other matrix SE . The two splitted matrices will be of the same size $L \times N / 2$; ii) using the DNA encoding complementary 4th rule as shown in Table 1, encode all binary element of the two matrices SO and SE ; iii) two outputs matrices of DNA encoded elements of size $L \times N / 2$ are then deduced. For illustration, using the 4th rule of the DNA complementary rules '10011000', and '01001110' will give output of 'ATAC', and 'TCGA', correspondingly; iv) mutating the resultant pairs of DNA in the previous step by addition of the two matrices using the DNA addition as given in Table 2 at the encryption side while applying the DNA subtraction process at the decryption side using Table 3; v) changing the values of the mutated DNA elements to their equivalent binary values corresponding to Table 1; and vi) the two matrices SO and SE will be concatenated so as to form one binary matrix represented by Q with size of $L \times N$, then passing Matrix Q as an input to the backward diffusion stage.

Table 2. An adding algebraic process of DNA sequence used in encryption side

ADD	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G

Table 3. Subtracting algebraic process of DNA sequence used in decryption side

SUB	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T

3.8. Backward Diffusion Stage $L \times N$

Backward image diffusion is performed by converting the matrix Q into a matrix signified by C , and the pseudo-noise matrix Z by XOR operations as shown in:

$$C(N, L) = Q(N, L) \oplus Z(N, L) \oplus v_1 \quad (12)$$

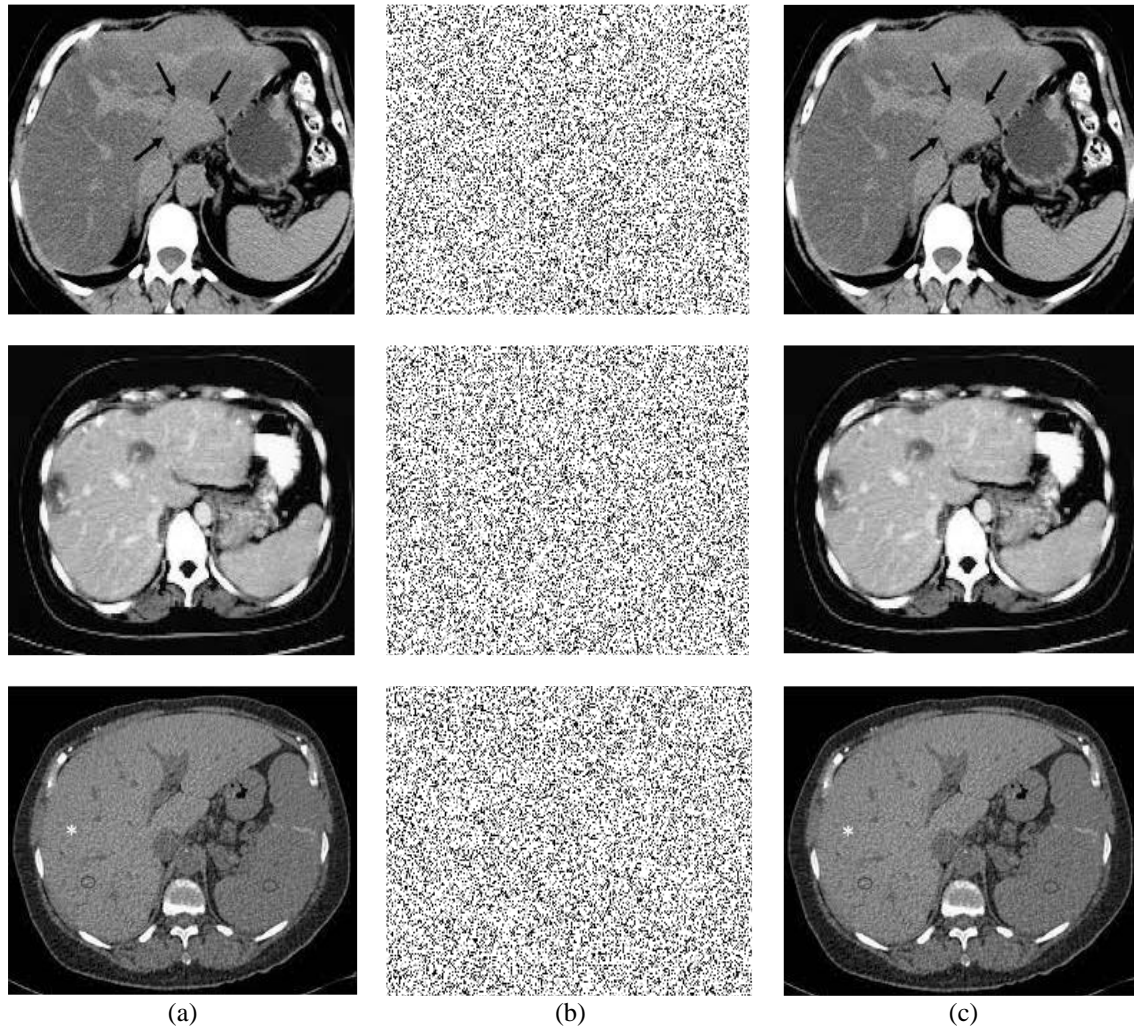
$$C(N, l) = Q(N, l) \oplus Z(N, l) \oplus Q(N, l + 1), \text{ for } l = L - 1, \dots, 1 \quad (13)$$

$$C(k, L) = Q(k, L) \oplus Z(k, L) \oplus Q(k + 1, L), \text{ for } k = N - 1, \dots, 1 \quad (14)$$

$$C(k, l) = Q(k, l) \oplus Z(k, l) \oplus Q(k + 1, l) \oplus Q(k, l + 1) \oplus Q(k + 1, l + 1), \text{ for } k = N - 1, \dots, 1, \text{ for } l = L - 1, \dots, 1 \quad (15)$$

4. RESULTS AND DISCUSSION

This section demonstrates the results acquired by implementation of algorithm analyzed in previous section. The proposed scheme is carried out on the resulted deep binary image features; therefore, the analysis of the outcomes is generally considered into three sections evaluating the quality of the decrypted image, security analysis, and analysis of computational complexity. The intended scheme was implemented using MATLAB (R2015a) software (MathWorks, Natick, MA, USA). The simulation results are shown in Figure 6, where in Figure 6(a) the used private symmetric key $S = [4.2314, 13.0451, 50.7751, 23.3523, 43, 201]$ is utilized in both the decoding and encoding algorithms, and the original medical images utilized are 256×256 pixels in size. A cipher image for the corresponding encryption algorithm is depicted in Figure 6(b). Using the appropriate secret key S , we then decrypted the cipher image in order to regenerate the reconstructed image as shown in Figure 6(c). The recovered decrypted image is a perfect reconstruction of the original plain image, and the cipher image pattern does not resemble the plain image. Based on the visual evaluation of the standard plain images, we conclude that the proposed encryption process does not adversely affect the visual quality.



Figur 6. Simulation results by (a) original images, (b) ciphered images of (a), and (c) decrypted images

4.1. Analysis of key space

The domain of key space must be commonly considered enormous to prevent the adversary employing brute-force assault to reveal the private key. The size of the key space determines how secure a cryptosystem is. Since an attacker will attempt to decrypt an intercepted message using every key combination conceivable, a message with a wider keyspace will be more resistant to an analytical attack. In our proposed system, the key space employs four initial conditions given by $\{x_{01}, x_{02}, x_{03}, x_{04}, v_1 \text{ and } v_2\}$ related to the hyperchaotic system. Hence, the size of key space of our intended algorithm can be calculated as 1.6777×10^{64} , as a results our system has a huge key space domain that actually become rubost against brute-force assaults, and taking about 2.03451×10^{52} days for breaking down our proposed scheme.

4.2. Analysis of statistical attacks

4.2.1. The grey histogram evaluation

The proposed encryption algorithm should be robust and can withstand various satistical and cipher images attacks which can be evaluated using the related analysis of the histogram as shown in Figure 7. The original images histograms presented in Figure 7(a) example, Image 1, Image 2 and Image 3 are extremely not uniform with an obvious characteristic peak where the images information are mostly obtained easily. while Figure 7(b) shows the cipher images histograms having almost uniformly statistical distribution. Hence, the employed system can withstand the cipher images and statistical assaults. Figure 7(c) displays the decrypted images histograms.

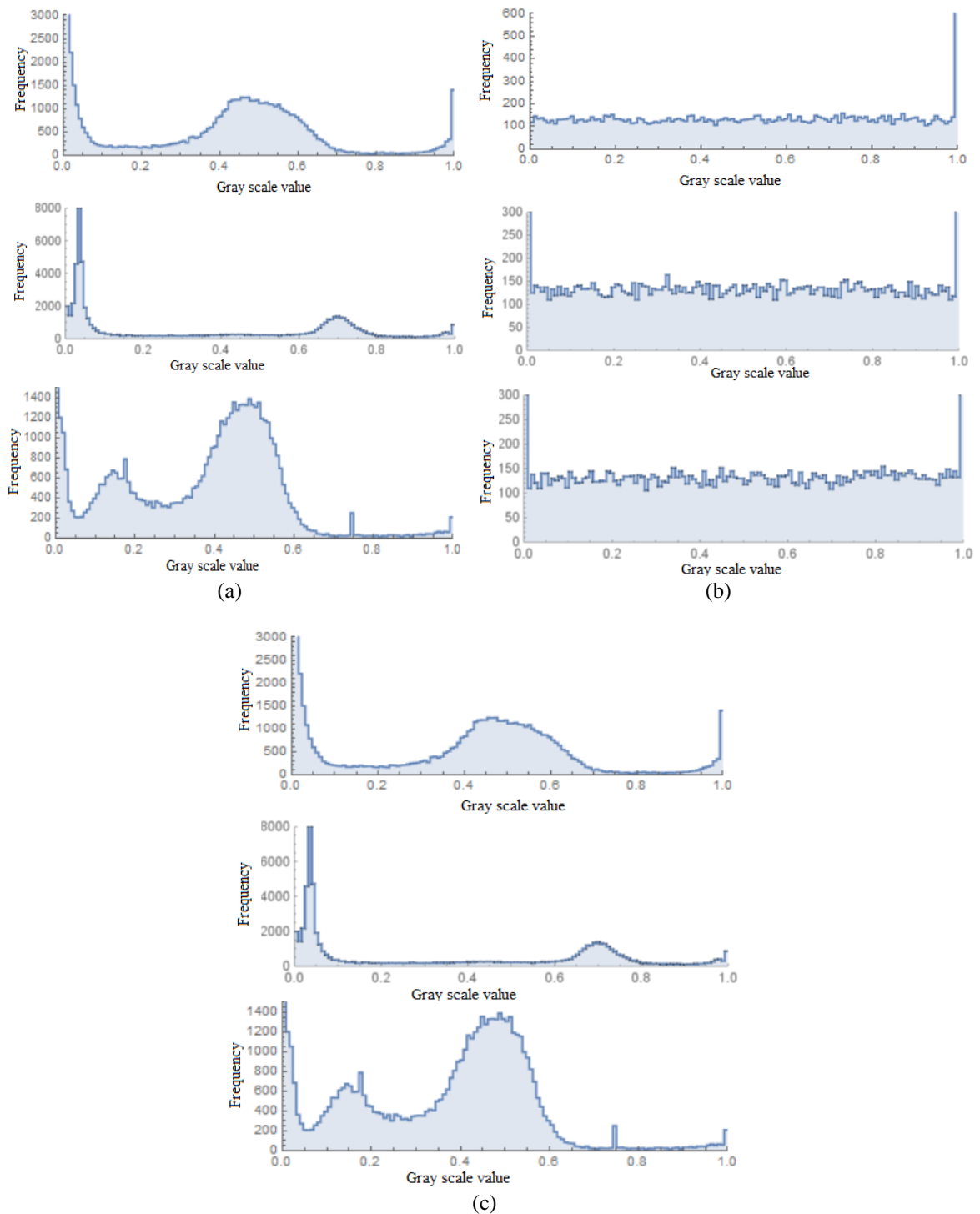


Figure 7. Related histogram analysis by (a) original images histograms (b) ciphered images histograms, and (c) decrypted images histograms

4.3. Evaluating image quality

The procedure of encryption, in general, consists of reiterative steps that are performed to make sure that the result is a safe and challenging for an intruder to access. To enhance encryption strength, substantial number of pixels must be encrypted, which also impacts image quality. As a result, it is imperative to determine whether the encryption process actually affects image quality. correlation, number of changing pixel rate (NPCR), and unified averaged changed intensity (UACI) are the performance parameters used to assess image quality. Using comparative analysis, the analysis is also carried out to determine its computational complexity.

4.3.1. Correlation coefficient analysis

With regard to horizontal, vertical, and diagonal direction of the pixels, correlation-coefficients are used to appraise graphical quality. It is carried out to compare the decrypted output image with the original input image. Pick N random pixels nearby, and (x_i, y_i) represent the values of i-th pixel pair $(i=1, 2, \dots, N)$. Afterwards, the correlation coefficient can be calculated as:

$$\begin{aligned}
 E(x) &= \frac{1}{N} \sum_{i=1}^N x_i \\
 D(x) &= \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \\
 cov(x,y) &= \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \\
 C.F &= \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}}
 \end{aligned}
 \tag{16}$$

(x_i, y_i) represent the grey values of the adjacent pixels for an image, $D(x)$ represents the variance, $E(x)$ denotes the mean and $cov(x,y)$ denotes the covariance. Assuming $N=2000$, then correlation-coefficients resultant for related original and cipher images are displayed in Table 4. The analysis of correlation coefficient is shown in Figure 8, the analysis of horizontal correlation coefficient is presented in Figure 8(a), while the horizontal correlation for their encrypted images is shown in Figure 8(b).

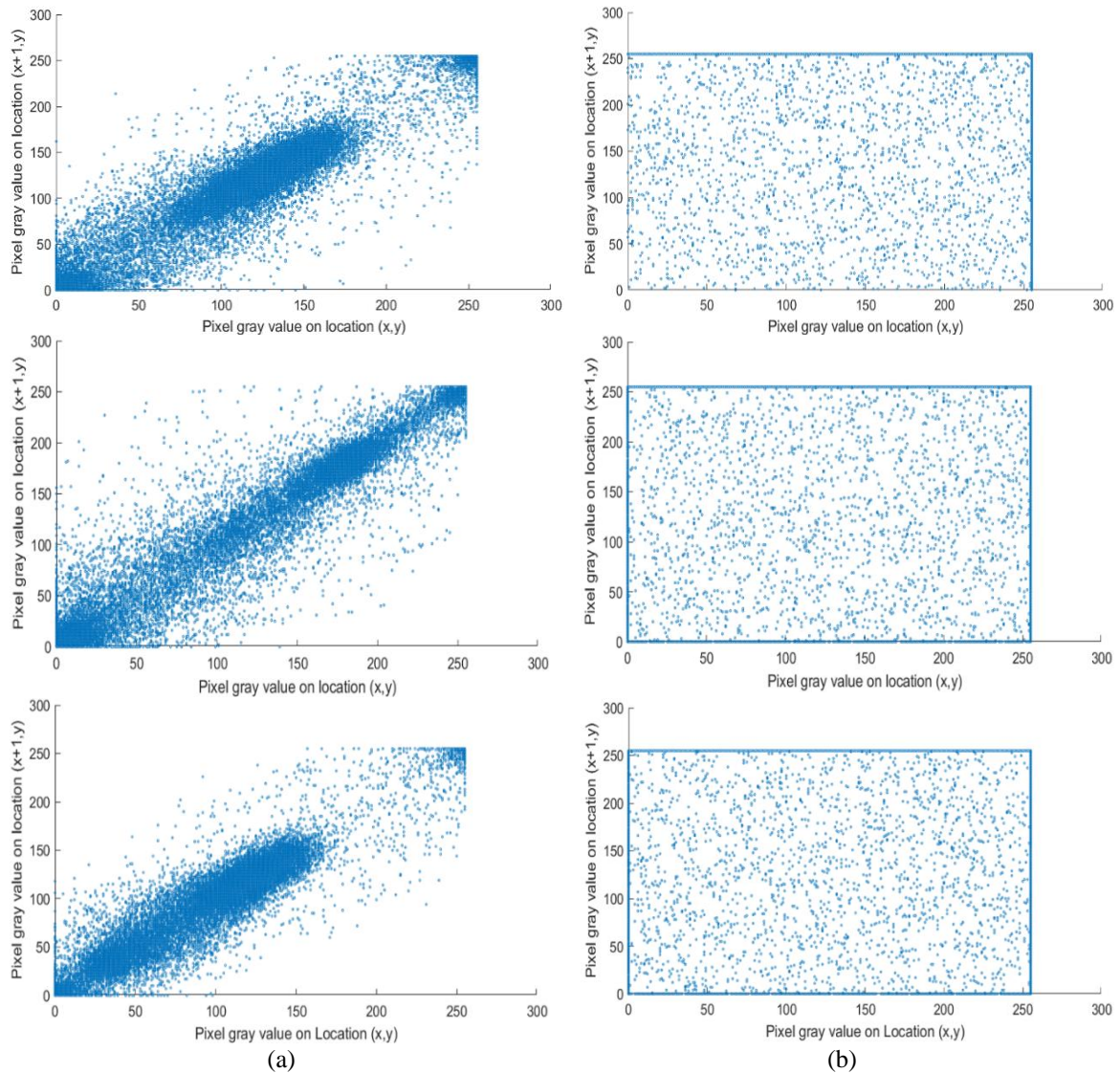


Figure 8. Analysis of correlation coefficient by (a) correlation in horizontal directions of plain-images 1, 2 and 3 and (b) horizontal correlation for their encrypted images correspondingly

Table 4. Correlation factor between two adjacent pixels in three images

Model	Original Image 1	Original Image 2	Original Image 3	Encrypted Image 1	Encrypted Image 2	Encrypted Image 3
Horizontal	0.9694	0.9597	0.9723	0.0038	0.0036	0.0047
Vertical	0.9682	0.9460	0.9453	0.0031	0.0031	0.0034
Diagonal	0.9266	0.9349	0.9318	0.0038	0.0017	0.0021

In addition, a comparative analysis between the suggested system and some related works displaying the correlation coefficient is shown in Table 5, It was noticed that the correlation coefficient value of original images is high and has value near to one. On the other side we find that cipher images correlation value is low and in close proximity to zero, obviously it has been realized that the new presented system can break the relativeness efficiently; and so, our system has a vigorous capability for resisting the statistical assault, and will not affect the decrypted image quality.

Table 5. Comparative analysis for the correlation coefficient

Method	Horizontal correlation coefficients	Vertical correlation coefficients	Diagonal correlation coefficients
Proposed	-0.0019	0.0008	0.0024
Chen <i>et al.</i> [35]	-0.0024	0.0012	0.0035
Chenaghlu <i>et al.</i> [36]	-0.0021	0.0014	0.0031
Ding <i>et al.</i> [23]	0.0383	0.2259	0.1158

4.3.2. Resistance to differential attack attackers

The NPCR and UACI hypothetical values are 99.609% and 33.464% for images having 256 gray levels. Moreover, the values are assessed compared to the critical values [37], [38] which indeed proves the capability of the proposed algorithm in resisting differential attacks. Therefore, this provided scheme attains high-level performance with the values of NPCR and UACI near to the theoretical standards. As shown in Table 6 which displays the comparative results assessing our proposed system with older systems due to their NPCR and UACI values, from the following analysis, it has been proved that the proposed scheme is robust and can withstand the differential assaults.

$$NPCR = \frac{1}{L \times N} \sum_{i=1}^L \sum_{j=1}^N |Sign(C_1(i, j) - C_2(i, j))| \times 100\% \quad (17)$$

$$UACI = \frac{1}{L \times N} \sum_{i=1}^L \sum_{j=1}^N \frac{|Sign(C_1(i, j) - C_2(i, j))|}{256} \times 100\% \quad (18)$$

Table 6. Comparative analysis for the correlation coefficient

Method	Average NPCR	Average UACI
Proposed	0.9971	0.3359
Chen <i>et al.</i> [35]	0.9961	0.3357
Ding <i>et al.</i> [23]	0.9959	0.2319
Bao and Xue [39]	0.9964	0.3349

4.4. Information entropy

In any cryptographic system, expressing the degree of uncertainty is measured the information entropy [35]. It can also be used in expressing the uncertainties in image information by measuring the grey values distribution in an image. The more uniform the grey values distribution the greater the information entropy is. The information entropy is defined as:

$$H(m) = - \sum_{i=0}^L P(m_i) \log_2 P(m_i) \quad (19)$$

m_i represents the i th grey value used for the L level grey image, where the emergence probability of m_i is denoted by $P(m_i)$, given that for $\sum_{i=0}^L P(m_i) = 1$. The information entropy theoretic value of an ideal greyscale random image is 8, therefore an efficient cryptographic system have to get the information entropy nearby 8. Table 7 demonstrates the values of the information entropy of encrypted medical images, which are

near to the hypothetical value. Thus, the results confirm that our new suggested scheme can be able to effectively counteroffensive the information entropy.

Table 7. Comparative analysis for the correlation coefficient

Method	Information entropy
Proposed	7.9989
Chen <i>et al.</i> [35]	7.9944
Ding <i>et al.</i> [23]	7.9986
Bao and Xue [39]	7.9972

4.5. Complexity analysis

It is possible to calculate the difficulty of employing the introduced encryption scheme [40], given an image of size as $w \times L \times N$. In this case, n represents the number of pixels within the image. This can be determined by following the considered steps. Conversion of binary data, operation of scrambling DNA, generation of the private key, forward and backward diffusion processes, as well as decimal data conversion are all involved in this process. The binary data conversion complexity is $O(n^2)$ and for the DNA scrambling is $O(4n^2)$. Creating the private key entails three steps, namely producing pseudo-random sequences, binary transformations, and scrambling of DNA, all having complexity of $O(6n^2)$. Alternatively, the processes of forward and backward diffusion have a complexity of $O(62n^2)$. Converting DNA into binary data and converting binary data into decimal data takes $O(5n^2)$. Consequently, the overall complexity of the produced encryption image algorithm is equal to $O(78n^2)$.

5. CONCLUSION

The increasing interest over recent years to conserve the secrecy of sensitive patient health information, has increased the need for new cryptographic methods appropriate for addressing privacy-related concerns. This article has presented a robust authenticated model where deep learning using hybrid chaotic Lorentz map diffusion and DNA confusion stages has been utilized for performing enhanced optimization concerning enhancing the encryption performance of medical images, our new encryption scheme proved its robustness due to its demonstrated large key space in resisting brute-force attack, having strong key sensitivity, strong plaintext sensitivity and strong cipher-text sensitivity. As a result, our proposed method achieved a high level of security with a good efficiency performance in the field of deep learning image security.

ACKNOWLEDGEMENTS




This research project was funded by the Deanship of Scientific Research, Princess Nourah bint Abdulrahman University, through the Program of Research Project Funding after Publication, grant No (41-PRF-A-P-9).

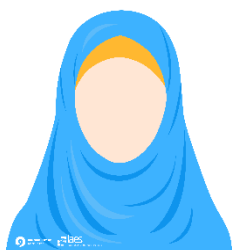
REFERENCES




- [1] Y. Fu and C. Aldrich, "Flotation froth image recognition with convolutional neural networks," *Minerals Engineering*, vol. 132, pp. 183–190, Mar. 2019, doi: 10.1016/j.mineng.2018.12.011.
- [2] B. B. Traore, B. Kamsu-Foguem, and F. Tangara, "Deep convolution neural network for image recognition," *Ecological Informatics*, vol. 48, pp. 257–268, Nov. 2018, doi: 10.1016/j.ecoinf.2018.10.002.
- [3] L. Fang, Y. Jin, L. Huang, S. Guo, G. Zhao, and X. Chen, "Iterative fusion convolutional neural networks for classification of optical coherence tomography images," *Journal of Visual Communication and Image Representation*, vol. 59, pp. 327–333, Feb. 2019, doi: 10.1016/j.jvcir.2019.01.022.
- [4] M. Vinícius dos Santos Ferreira, A. Oseas de Carvalho Filho, A. Dalíia de Sousa, A. Corrêa Silva, and M. Gattass, "Convolutional neural network and texture descriptor-based automatic detection and diagnosis of glaucoma," *Expert Systems with Applications*, vol. 110, pp. 250–263, Nov. 2018, doi: 10.1016/j.eswa.2018.06.010.
- [5] N. Nanda, P. Kakkar, and S. Nagpal, "Computer-aided segmentation of liver lesions in CT Scans Using cascaded convolutional neural networks and genetically optimised classifier," *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 4049–4062, Apr. 2019, doi: 10.1007/s13369-019-03735-8.
- [6] A. Esteva *et al.*, "Dermatologist-level classification of skin cancer with deep neural networks," *Nature*, vol. 542, no. 7639, pp. 115–118, Feb. 2017, doi: 10.1038/nature21056.
- [7] S. R. Maniyath and V. Thanikaiselvan, "An efficient image encryption using deep neural network and chaotic map," *Microprocessors and Microsystems*, vol. 77, p. 103134, Sep. 2020, doi: 10.1016/j.micpro.2020.103134.
- [8] A. Hassan, F. Liu, F. Wang, and Y. Wang, "Secure content based image retrieval for mobile users with deep neural networks in the cloud," *Journal of Systems Architecture*, vol. 116, Jun. 2021, doi: 10.1016/j.sysarc.2021.102043.
- [9] C. Guo, J. Jia, K. K. R. Choo, and Y. Jie, "Privacy-preserving image search (PPIS): Secure classification and searching using convolutional neural network over large-scale encrypted medical images," *Computers and Security*, vol. 99, Dec. 2020, doi: 10.1016/j.cose.2020.102021.

- [10] A. S. Hashemi and S. Mozaffari, "Secure deep neural networks using adversarial image generation and training with Noise-GAN," *Computers and Security*, vol. 86, pp. 372–387, Sep. 2019, doi: 10.1016/j.cose.2019.06.012.
- [11] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024, Nov. 1994, doi: 10.1126/science.7973651.
- [12] A. Gahlaut, A. Bharti, Y. Dogra, and P. Singh, "DNA based cryptography," in *Communications in Computer and Information Science*, vol. 750, 2017, pp. 205–215.
- [13] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Computers & Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, Sep. 2012, doi: 10.1016/j.compeleceng.2012.02.007.
- [14] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Applied Soft Computing Journal*, vol. 12, no. 5, pp. 1457–1466, May 2012, doi: 10.1016/j.asoc.2012.01.016.
- [15] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, May 2014, doi: 10.1016/j.optlaseng.2013.12.003.
- [16] A. N. Kengnou Telem, C. Meli Segning, G. Kenne, and H. B. Fotsin, "A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network," *Advances in Multimedia*, vol. 2014, pp. 1–13, 2014, doi: 10.1155/2014/602921.
- [17] 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 Processing*, vol. 10, no. 11, pp. 830–839, Nov. 2016, doi: 10.1049/iet-ipr.2015.0868.
- [18] N. Dowlin, R. Gilad-Bachrach, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, "Manual for using homomorphic encryption for bioinformatics: This paper provides a new homomorphic encryption algorithm and associated software for bioinformatics to enhance the security and privacy associated with computing on human genomes," *Proceedings of the IEEE*, vol. 105, no. 3, pp. 552–567, 2017, doi: 10.1109/JPROC.2016.2622218.
- [19] S. Lakshmanan, M. Prakash, C. P. Lim, R. Rakkiyappan, P. Balasubramaniam, and S. Nahavandi, "Synchronization of an inertial neural network with time-varying delays and its application to secure communication," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 1, pp. 195–207, Jan. 2018, doi: 10.1109/TNNLS.2016.2619345.
- [20] A. Shifa *et al.*, "Joint crypto-stego scheme for enhanced image protection with nearest-centroid clustering," *IEEE Access*, vol. 6, pp. 16189–16206, 2018, doi: 10.1109/ACCESS.2018.2815037.
- [21] X. Li, Y. Jiang, M. Chen, and F. Li, "Research on iris image encryption based on deep learning," *Eurasip Journal on Image and Video Processing*, vol. 2018, no. 1, p. 126, Dec. 2018, doi: 10.1186/s13640-018-0358-7.
- [22] A. Ali *et al.*, "Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: a novel approach to cryptography," *Sensors*, vol. 22, no. 2, Jan. 2022, doi: 10.3390/s22020528.
- [23] Y. Ding, F. Tan, Z. Qin, M. Cao, K. K. R. Choo, and Z. Qin, "DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 9, pp. 4915–4929, Sep. 2021, doi: 10.1109/TNNLS.2021.3062754.
- [24] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dynamics*, vol. 92, no. 2, pp. 305–313, Apr. 2018, doi: 10.1007/s11071-018-4056-x.
- [25] W. Y. Lee, S. M. Park, and K. B. Sim, "Optimal hyperparameter tuning of convolutional neural networks based on the parameter-setting-free harmony search algorithm," *Optik*, vol. 172, pp. 359–367, Nov. 2018, doi: 10.1016/j.ijleo.2018.07.044.
- [26] R. M. Ghoniem, A. D. Algarni, B. Refky, and A. A. Ewees, "Multi-modal evolutionary deep learning model for ovarian cancer diagnosis," *Symmetry*, vol. 13, no. 4, p. 643, Apr. 2021, doi: 10.3390/sym13040643.
- [27] R. M. Ghoniem, "A novel bio-inspired deep learning approach for liver cancer diagnosis," *Information*, vol. 11, no. 2, p. 80, Jan. 2020, doi: 10.3390/info11020080.
- [28] R. M. Ghoniem, "Deep genetic algorithm-based voice pathology diagnostic system," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11608 LNCS, 2019, pp. 220–233, doi: 10.1007/978-3-030-23281-8_18.
- [29] X. Wang and M. Wang, "A hyperchaos generated from Lorenz system," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 14, pp. 3751–3758, Jun. 2008, doi: 10.1016/j.physa.2008.02.020.
- [30] Y. Zhang, "A chaotic system based image encryption scheme with identical encryption and decryption algorithm," *Chinese Journal of Electronics*, vol. 26, no. 5, pp. 1022–1031, Sep. 2017, doi: 10.1049/cje.2017.08.022.
- [31] N. Srividhya and T. Vino, "Genome based highly secured image using DNA cryptography and trellis algorithm," in *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, Mar. 2016, pp. 1658–1662, doi: 10.1109/WiSPNET.2016.7566421.
- [32] E. H. H. G. Mohamed, F. Ahmed, and D. H. ElKamchouchi, "A secure digital signature scheme with fault tolerance based on the improved RSA system," in *Computer Science & Information Technology (CS & IT)*, May 2016, pp. 35–44, doi: 10.5121/csit.2016.60704.
- [33] P. Kakkar, S. Nagpal, and N. Nanda, "Automatic liver segmentation in CT images using improvised techniques," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10983 LNCS, 2018, pp. 41–52, doi: 10.1007/978-3-030-03649-2_4.
- [34] F. F. Ting, Y. J. Tan, and K. S. Sim, "Convolutional neural network improvement for breast cancer classification," *Expert Systems with Applications*, vol. 120, pp. 103–115, Apr. 2019, doi: 10.1016/j.eswa.2018.11.008.
- [35] W. Chen, Y. Guo, and S. W. Jing, "General image encryption algorithm based on deep learning compressed sensing and compound chaotic system," *Wuli Xuebao/Acta Physica Sinica*, vol. 69, no. 24, p. 240502, 2020, doi: 10.7498/aps.69.20201019.
- [36] M. Asgari-Chenaghlu *et al.*, "Cy: Chaotic yolo for user intended image encryption and sharing in social media," *Information Sciences*, vol. 542, pp. 212–227, Jan. 2021, doi: 10.1016/j.ins.2020.07.007.
- [37] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, May 2016, doi: 10.1016/j.combiomed.2016.03.020.
- [38] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Transactions on Nanobioscience*, vol. 16, no. 8, pp. 850–858, Dec. 2017, doi: 10.1109/TNB.2017.2780881.
- [39] Z. Bao and R. Xue, "Research on the avalanche effect of image encryption based on the Cycle-GAN," *Applied Optics*, vol. 60, no. 18, p. 5320, Jun. 2021, doi: 10.1364/ao.428203.
- [40] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.




BIOGRAPHIES OF AUTHORS

Dalia H. Elkamchouchi    was born in Alexandria, Egypt in 1974. She received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the University of Alexandria, Egypt, in 1997, 2006, and 2010, respectively. Starting from 2010, she was an Assistant professor at Alexandria Higher Institute of Engineering and Technology, Ministry of Higher Education, Egypt, and from 2018 and still, an Assistant professor at Faculty of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Saudi Arabia. Her research interests include cryptography, wireless sensor networks, mobile data communication, internet of things, cyber security and project management. She can be contacted at email: dhelkamchouchi@pnu.edu.sa.






Abeer D. Algarni    received the B.Sc. (Hons.) in Computer Science from King Saud University, Riyadh, Saudi Arabia in 2007. She received the M.Sc., and Ph.D. degrees from the School of Engineering and Computer Sciences, Durham University, United Kingdom in 2010 and 2015, respectively. She worked as an assistant professor at the College of Computer and Information Sciences at Princess Nourah Bent Abdulrahman University from 2008 till 2020 and as an associate professor since 2020 up to now. Her current research interests include networking and communication systems, digital image processing, digital communications and cyber security. She can be contacted at email: adalqarni@pnu.edu.sa.



Rania M. Ghoniem    received the Ph.D. degree in integrating artificial intelligence techniques in medical diagnosis from Mansoura University, Egypt. She is currently working as assistant professor with the Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. She is associate professor in computer science from 2021 till now. Her research interests include computer-aided diagnostic systems, medical image and sound processing, natural language processing, deep learning, and meta-heuristic optimization methods. She can be contacted at email: RMGhoniem@pnu.edu.sa.



Heba G. Mohamed    was born in Alexandria, Egypt in 1984. She received the B.Sc., M.Sc. degrees in electrical engineering from Arab Academy for Science and Technology in 2007 and 2012, respectively, then, the Ph.D. degree in electrical engineering from the University of Alexandria, Egypt, in 2016. Starting from 2016, she was an Assistant professor at Alexandria Higher Institute of Engineering and Technology, Ministry of Higher Education, Egypt, and from 2019 and still, an Assistant professor at Faculty of Engineering, Communication department, Princess Nourah bint Abdulrahman University, Saudi Arabia. Her research interests include cryptography, wireless communication, mobile data communication, internet of things and computer vision. She can be contacted at email: HeGMohamed@pnu.edu.sa.