Hindawi Publishing Corporation
Advances in Multimedia
Volume 2014, Article ID 602921, 13 pages
http://dx.doi.org/10.1155/2014/602921

*Research Article*

# A Simple and Robust Gray Image Encryption Scheme Using Chaotic Logistic Map and Artificial Neural Network

**Adelaïde Nicole Kengnou Telem,[1] Colince Meli Segning,[1] Godpromesse Kenne,[1] and Hilaire Bertrand Fotsin[2]**

[1]*Laboratoire d'Automatique et d'Informatique Appliquée (LAIA), Département de Génie Electrique, IUT Fotso Victor Bandjoun, Université de Dschang, B.P. 134, Bandjoun, Cameroon*
[2]*Laboratoire d'Electronique et de Traitement du Signal (LETS), Département de Physique, Faculté des Sciences, Université de Dschang, Cameroon*

Correspondence should be addressed to Godpromesse Kenne; gokenne@yahoo.com

Received 20 September 2014; Revised 4 December 2014; Accepted 4 December 2014; Published 31 December 2014

Academic Editor: Martin Reisslein



A robust gray image encryption scheme using chaotic logistic map and artificial neural network (ANN) is introduced. In the proposed method, an external secret key is used to derive the initial conditions for the logistic chaotic maps which are employed to generate weights and biases matrices of the multilayer perceptron (MLP). During the learning process with the backpropagation algorithm, ANN determines the weight matrix of the connections. The plain image is divided into four subimages which are used for the first diffusion stage. The subimages obtained previously are divided into the square subimage blocks. In the next stage, different initial conditions are employed to generate a key stream which will be used for permutation and diffusion of the subimage blocks. Some security analyses such as entropy analysis, statistical analysis, and key sensitivity analysis are given to demonstrate the key space of the proposed algorithm which is large enough to make brute force attacks infeasible. Computing validation using experimental data with several gray images has been carried out with detailed numerical analysis, in order to validate the high security of the proposed encryption scheme.

## 1. Introduction

Many applications like military images databases, confidential video, medical imaging systems, cable TV image, and online personal photograph album require reliable, fast, and robust security system to store and transmit digital images [1]. To secure transmitted information, cryptography techniques are needed. Cryptography is the science of protecting the privacy of information during communication, under hostile conditions. The digital images have certain characteristics such as redundancy of data, strong correlation among adjacent pixels, robustness against perturbations (i.e., a tiny change in the attribute of any pixel of the image does not drastically degrade the quality of the image), and bulk capacity of data [1]. Consequently, traditional encryptions methods like IDEA, AES, DES, and RSA have limitation in encrypting image such as low efficiency, bulky data, and high correlation among pixels [2–6]. To face these challenges, a wide variety of cryptographic protocols have been proposed in the literature [7–25]. In the last decade, chaos-based encryption techniques are considered suitable for practical applications since they have good combination of speed, high security, complexity, reasonable computational overheads, and computational power. Moreover, chaos-based and other dynamical systems based algorithms have many important properties such as the sensitive dependence on initial conditions and system parameters, pseudorandom properties, ergodicity, and nonperiodicity [3, 26–28]. These properties meet some requirements such as a sensitivity to keys, diffusion, and mixing in the sense of cryptography. Therefore, chaotic dynamics are expected to provide a fast and easy way for building superior performance cryptosystems. But most of them have been cryptanalysed successfully due to finite

computing precision used to represent the floating point output of chaotic system as it introduces cycles in the behavior of chaotic systems and hence becomes vulnerable to attacks [4, 23]. The development of artificial neural network (ANN) approach is widely used by soft computing techniques that have the capability to capture and model complex input/output relationships of any system. The advantages of ANN are the ability to generalize results obtained from known situations to unforeseen situations, the fast response time in operational phase, the high degree of structural parallelism, reliability, and efficiency [29]. A number of chaos- and ANN-based image encryption schemes have been developed in recent years [29–33]. Pareek et al. in [1] have proposed a new image encryption scheme based on two chaotic logistic maps and external secret key of 80 bits to encrypt the colour image. In [34], a chaos-based image encryption algorithm with variable control parameters is introduced to improve the deficiency usually obtained by using fixed parameters in the permutation stage which is vulnerable to attacks. Mazloom and Eftekhari-Moghadam in [35] have proposed a novel chaos-based cryptosystem for color image encryption operating as a symmetric stream-cipher where the objective is to design a new chaotic algorithm which has the properties of nonlinearity and coupled structure. Patidar et al. in [36] have proposed a new substitution-diffusion approach based on chaotic standard and logistic maps, which is very fast and possesses most of the confusion and diffusion properties that any good cryptosystem should have. In [2], a modified substitution-diffusion image cipher using chaotic standard and logistic maps is proposed to improve some of the weakness obtained by Patidar et al. [36] in order to make it more robust against attacks. In [37], a new algorithm which utilizes the single logistic map against the four maps used by Nien et al. [38] is described. They used Hénon map and Lorentz map for pixel shuffling and measured correlation coefficient and key sensitivity for finding the best suited map for this algorithm. But only pixel location is changed to shuffle the whole image which is not sufficient to make the proposed algorithm robust against attacks [5, 27, 39]. In [40], a novel chaos-based bit-level permutation scheme for digital image encryption is proposed. In that work, the scheme introduced a significant diffusion effect in permutation procedure through a two-stage bit-level shuffling algorithm by chaotic sequence sorting algorithm and Arnold cat map. Ye in [6] has presented a novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. In the permutation process, he used one generalized Arnold map to generate a chaotic orbit. To improve the diffusion effect, a two-way diffusion process is presented, where one generalized Arnold map and one generalized Bernoulli shift map are utilized to generate two pseudorandom gray value sequences. Wang and He in [28] have developed cryptanalysis on a novel image encryption method based on total shuffling scheme to enhance the security of the scheme based on a novel image encryption method proposed by Zhang and Liu [41]. Wang et al. in [42] introduced a new image encryption algorithm based on chaos theory. The proposed algorithm realizes fast encryption and decryption of both gray-scale image and true color image by using the pseudorandom sequence generated by a group of chaotic maps. In [43], a bit-level image encryption algorithm based on spatiotemporal chaotic system which is self-adaptive is proposed. They used a bit-level encryption scheme to reduce the volume of data during encryption and decryption in order to reduce the execution time. They also used the adaptive encryption scheme to make the ciphered image dependent on the plain image to improve performance. In [44], an image encryption method based on total shuffling is presented to improve some of the deficiency obtained by Zhang and Liu [41]. Liu et al. in [45] have proposed optical color image encryption based on computer generated hologram and chaotic theory to reduce the amount of information and facilitate network transmission. Behnia et al. in [46] have presented a novel image encryption algorithm based on the Jacobian elliptic maps to overcome some fundamental drawbacks in the chaotic cryptosystems such as small key space and weak security [47]. Bhatnagar and Wu in [48] have presented an efficient yet simple selective encryption technique based on Saw-Tooth space filling curve, pixels of interest, nonlinear chaotic map, and singular value decomposition. The core idea of that proposed scheme is to scramble the pixel positions by the means of Saw-Tooth space filling curve followed by the selection of significant pixels using pixels of interest method. Then the diffusion selective encryption process is done on the significant pixels using a secret image key obtained from nonlinear chaotic map space filling curve and singular value decomposition. Recently, Pareek et al. in [4] have proposed an efficient encryption algorithm for gray image using a secret key of 128 bits without using chaos. In that algorithm, sixteen rounds are used in the encryption scheme. Likewise Wang et al. in [49] have proposed cryptanalysis of an image encryption algorithm using Chebyshev generator to overcome some drawbacks in chaotic cryptosystem that threat the security. Bahrami and Naderi in [50] have proposed a simple and lightweight stream encryption algorithm for image encryption. Wang and Luan in [3] have combined cellular automata (CA) with chaos to propose a new image encryption. In the confusion stage, they shuffle image on unit-level which is a smaller level than pixels by using chaotic maps. The reversible cellular automata have many advantages such as large evolution rule spaces. However, it is performed on higher half pixel bits several times in diffusion stage to substitute pixels. In [51], an improved method for fast encryption of images using chaos method is introduced. In [27] a rapid and efficient method for generating large permutation is proposed by introducing the combination operation on permutation. In that work, a large permutation has been generated by combining several small permutations in order to improve the work of Yoon and Kim [52]. Chen and Cai in [53] proposed a neural network-based authentication scheme, which can provide a dynamic and secure remote user authentication over a completely in-secure communication channel. In [32], a novel image authentication scheme based on hyperchaotic cell neural network (HCCNN) is proposed. Bigdeli et al. in [31] have presented a novel image encryption/decryption algorithm based on chaotic neural network (CNN). The employed CNN is comprised of two 3-neuron layers called chaotic neuron layer (CNL) and permutation

neuron layer (PNL). The values of three RGB (Red, Green, and Blue) color components of image constitute inputs of the CNN and three encoded streams are the network outputs. CNL is a chaotic layer where three well-known chaotic systems, that is, Chua, Lorenz, and Lü's systems, participate in generating weights and biases matrices of this layer. In that work, a 160-bit-long authentication code is used to generate the initial conditions and the parameters of the CNL and PNL and provide satisfactory performance. In [33] an efficient neural chaotic generator for image encryption is proposed. In that work, neural network can act as an efficient source of perturbation in the chaotic generator which increases the cycle's length and thus avoids the dynamical degradation due to the used finite dimensional space. On the other hand, the use of neural network enlarges the key space of the chaotic generator in an enormous way.

Most of the above image encryption schemes developed are more complicated and may be difficult to implement in real time. This is the main motivation of the proposed algorithm in this paper where a simple and efficient method for gray image encryption scheme based on chaos and multilayer perceptron (MLP) ANN techniques is investigated. The proposed algorithm satisfies the requirements of secure image encryption. Firstly, we use an external secret key on chaotic logistic map to initialize biases and weights matrices of the MLP. During the training process with the backpropagation algorithm, the MLP determines the weights matrix of connections which will be used for the first diffusion stage. Secondly, a chaotic sequence is generated from the chaotic logistic map to permutate the pixels positions on the subimage. Finally, we use the same chaotic logistic map with different parameters and different initial conditions to diffuse the subimage of the whole image. In the last two stages, the initial conditions of chaotic logistic maps are variable among subimages. The resulting cryptosystem algorithm possesses most of the diffusion and confusion properties. The computing results provide better performances compared to those obtained in [4, 51]. In addition, we use simple logistic map instead of complex ones proposed in [5, 32, 51, 54, 55]. Therefore the proposed algorithm is easily implementable and more suitable for image encryption applications.

The rest of the paper is organized as follows. Section 2 presents the proposed encryption algorithm. Section 3 describes the comparative results and security analysis of the proposed algorithm. Finally, in Section 4, some concluding remarks are reported.

## 2. Description of the Proposed Image Encryption Algorithm

In this section, we present the new step-by-step image encryption algorithm. In the proposed encryption scheme, the image is encrypted using chaos and ANN as shown in Figure 1. Image $I_{m\times n}$ to be encrypted is firstly divided into four nonoverlapping subimages $A_{m'\times n}$. Every subimage is divided into several nonoverlapping blocks. The size of the new block and the number of rounds are decided by an external secret key. The proposed encryption algorithm uses substitution and diffusion mechanisms. In the following section, the role of different steps used in the algorithm as well as complete details of encryption algorithm is discussed.

*2.1. External Secret Key.* The proposed image encryption algorithm utilizes an external secret key of thirty-two decimal numbers. Let "ABCDEFGHIJKLMNOPQRSTUVWZ$\alpha\beta\lambda\gamma\rho\eta\mu\tau$" be an external key.

(i) ABCDE refers to the parameter of the first chaotic logistic map.

(ii) FGHIJ refers to the parameter of the second chaotic logistic map.

(iii) KLM gives the initial condition of the input biases of MLP.

(iv) NOP gives the initial condition of the input weight of MLP.

(v) QRS gives the initial condition of the output biases of MLP.

(vi) TUV gives the initial condition of the output weight of MLP.

(vii) WZ is the total number of hidden layers in MLP.

(viii) $\alpha$ is used to determine the initial condition of the second chaotic logistic map.

(ix) $\beta$ is the total round.

(x) $\lambda\gamma\rho$ gives the initial condition of the first chaotic logistic map.

(xi) $\eta\mu$ determines the size of the squared nonoverlapping blocks.

(xii) $\tau$ is used to determine the training step of MLP.

*2.2. Generating Chaotic Number Using Chaotic Map.* In the proposed algorithm, two chaotic logistic maps are used to achieve the goal of image encryption which are as follows:

$$X_{n+1} = r_x \times X_n \left(1 - X_n\right), \tag{1}$$

$$Y_{n+1} = r_y \times Y_n \left(1 - Y_n\right), \tag{2}$$

where $r_x$, $r_y$ and the initial conditions $X_0$, $Y_0$ are produced by an external secret key. Therefore,

$$r_x = \frac{38}{10} + \frac{\left(A/2^8 + B/2^7 + C/2^6 + D/2^5 + E/2^4\right)}{2^3}, \tag{3}$$

$$r_y = \frac{37}{10} + \frac{\left(F/2^8 + G/2^7 + H/2^6 + I/2^5 + J/2^4\right)}{2^3}, \tag{4}$$

$$X_0 = \frac{\left(\lambda \times 100 + \gamma \times 10 + \rho\right) \bmod (256)}{10 \times 2^8}, \tag{5}$$

$Y_0$ is derived from $X$ sequence. Depending on the step, $Y_0 = X(\alpha)$.

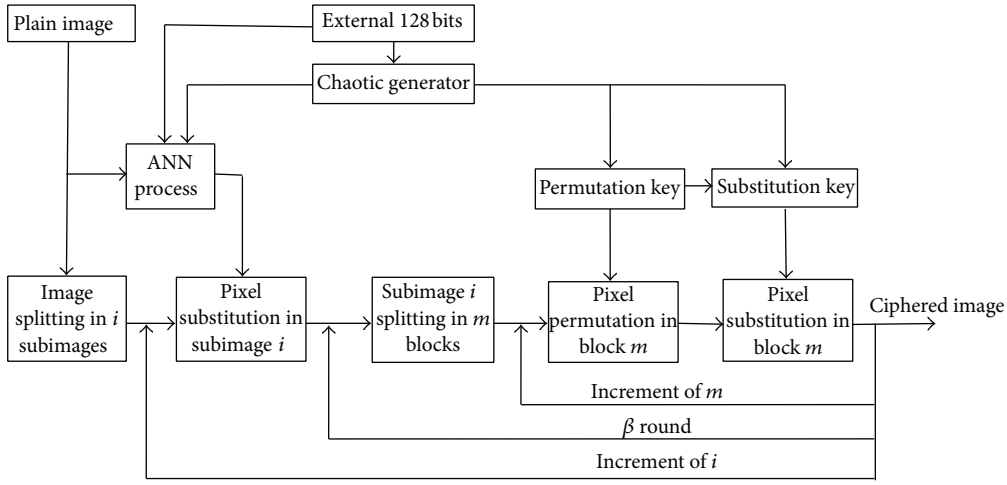



Figure 1: Block diagram of the proposed scheme.

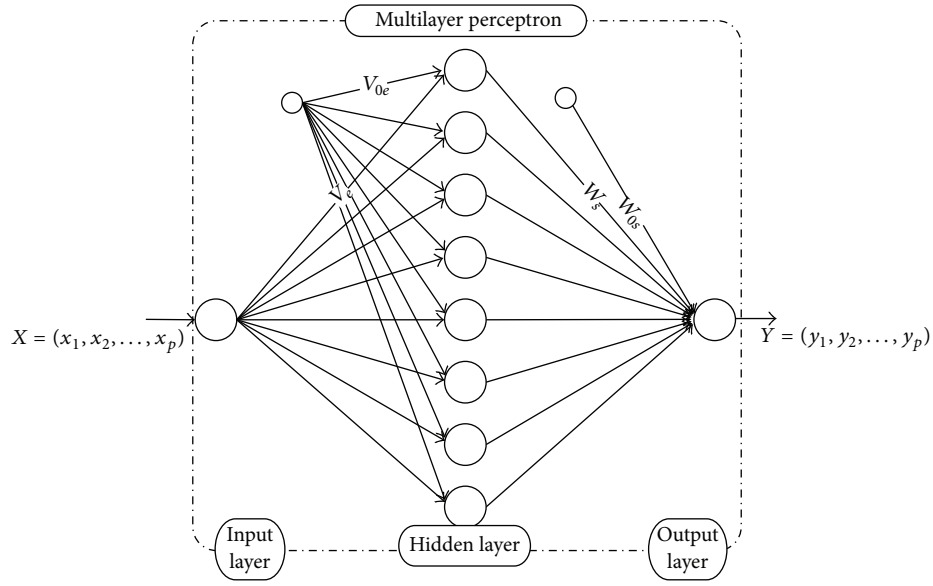



Figure 2: Multilayer perceptron structure.

*2.3. Artificial Neural Network Process.* The aim of this part is to generate the matrix code from the plain image which would be used in the first step of diffusion operation. At the end of the training process, the ANN produces the biases and weights matrices code $W$, which are used in the first diffusion step.

The type of neural network used in this paper is multilayer perceptron (MLP) trained with the well-known backpropagation algorithm. This structure is composed of one neuron in input layer, eight neurons in the hidden layer, and one node in output layer as as shown in Figure 2.

In Figure 2, $X$ is the vector of the input signal, $Y$ is the output signal vector, $V_e$, $W_s$ are the input/output weights, and $V_{0e}$, $W_{0s}$ are the input/output biases.

The process of the forward propagation of the training algorithm is given as follows:

$$y_k = g\left(W_{0s} + \sum_{j=1}^{n_{cc}} Z_j W_{s,j}\right) \quad (k = 1, 2, \ldots, p), \tag{6}$$

$$g(\xi) = a\xi, \quad a \in \Re, \tag{7}$$

$$Z_j = f\left(V_{0e,j} + x_k V_{e,j}\right) \quad (j = 1, 2, \ldots, n_{cc}), \quad (k = 1, 2, \ldots, p) \tag{8}$$

$$f(\xi) = \tanh(\xi), \tag{9}$$

$$\mathrm{ER}_k = y_k - x_k, \tag{10}$$

where $g$ is a linear function defined by (7) and $Z_j$ is the output of hidden layer defined by (8) where $f$ is a hyperbolic tangent function given by (9). This output pattern is then compared to the desired output, and an error signal is computed by (10).

The process of the backward propagation of the training algorithm is given as follows:

$$\delta_{o,k} = a\mathrm{ER}_k \quad (k = 1, 2, \ldots, p), \ a \in \Re,$$
$$\delta_{h,j} = Z_j\left(1 - Z_j\right)\sum_{j=1}^{n_{cc}}\delta_{o,k}W_{s,j} \quad (k = 1, 2, \ldots, p). \tag{11}$$

Based on the error signal received, connection weights and biases are updated for each unit until convergence of the neural network using the following equations:

$$V_e(i) = V_e(i) + \Psi \times \delta_{h,j} \times x_k,$$
$$W_s(i) = W_s(i) + \Psi \times \delta_{o,k} \times Z_j,$$
$$W_{0,s}(i) = W_{0,s}(i) + \Psi \times \delta_{o,k}, \tag{12}$$
$$V_{0,e}(i) = V_{0,e}(i) + \Psi \times \delta_{h,j},$$

with $(i = 1, 2, \ldots, \mathrm{epoch}_{\max})$ and $\mathrm{epoch}_{\max}$ the maximum iteration.

*2.3.1. Process of Neural Network Training.* The different steps of the algorithm are described as follows.

*Step 1* (preprocessing stage). The image to be encrypted is divided into two sets. 80% of the original image is used for pattern training and the rest of the image (20%) is used for patterns test. Since the pixel value is relatively high, each pattern is normalized. The process can be done using the function "mapminmax" of the MATLAB signal processing toolbox. This function processes original image by normalizing the minimum and maximum values of each row to $[-1, 1]$.

*Step 2* (initialization). One fundamental issue is how to adapt the weights of the MLP to achieve a given input/output map and choose reasonable network learning parameters (learning rate $\Psi$). The initial values of network connection weights ($V_e$, $W_s$) and biases ($V_{0e}$, $W_{0s}$) are random numbers generated using chaotic logistic map as shown in (1) where the parameter $r_x$ and the initial condition $X_0$ for the first sequence are given by (3) and (5), respectively. The next initial condition is taken in the previous sequence. The parameters $A$, $B$, $C$, $D$, $E$, $\lambda$, $\gamma$, and $\rho$ are provided by an external secret key as indicated in Section 2.1.

The learning rate $\Psi$ is given by (13) and the total neurons of the hidden layer are denoted by $n_{cc}$ where $\Psi$ and $n_{cc}$ are produced by an external secret key:

$$\Psi = \frac{\tau}{1000}. \tag{13}$$

*Step 3* (feedforward computation). The size of training set is $p \times q$. Each $q$ column of the training set $x_k$, $(k = 1, 2, \ldots, p)$ is presented to the network and each sample $x_k$ computes the actual output sample $y_k$ using (6).

*Step 4* (feedback computation). The output sample $y_k$ is used to compute the errors as shown in (10) and (11).

*Step 5* (modification of the network connection). The weights and biases connection are updated using (12).

*Step 6* (evaluation of the training accuracy). A root mean square error (RMSE) is used as a performance index to evaluate a training accuracy as follows:

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{k=1}^{p}\left(x_k - y_k\right)^2}{p}}. \tag{14}$$

If RMSE $\geq \varepsilon$, repeat Steps 3–6, where $\varepsilon$ is a given accuracy threshold.

*Step 7* (validation test). The actual outputs can be calculated using the weights and biases obtained in the training stage (Steps 2–6), and then the overall accuracy of the network can be measured by a testing RMSET given by

$$\mathrm{RMSET} = \sqrt{\frac{\sum_{k=1}^{q_t}\left(t_k - y_{t,k}\right)^2}{q_t}}, \tag{15}$$

where $t_k$ and $y_{t,k}$ represent the desired outputs and actual output of the set test and $q_t$ is the number of pattern tests.

*Step 8* (posttreatment). At the end of the test process, the inverse transformation of "mapminmax" function (see Step 1) is applied for the reconstruction of the original image and the ANN produces the biases and weights matrices code $W$, which are used in the first diffusion step.

*2.4. Masking with MLP Matrix Code.* This step is the first step of substitution in the encryption process. Here, we used the matrix code $W$ given by ANN process to change the pixel value by utilizing logical XOR operation. The plain image $I_{m\times n}$ is divided into four subimages $A_{m'\times n}$. Every subimage $A$ is divided into several blocks $B$ of size $n_{cc} \times n$. To change the value of the pixel, the corresponding code $C$ in the matrix code $W$ is selected and XORed with $B$. For the next block, the code for logical XOR operation is the block resulting from the last XOR operation. The process is done on the whole subimage $A$ and we continue with the next step of encryption algorithm.

*2.5. Permutation with Chaotic Code.* The change of the pixel location is a second step of our encryption image algorithm. Equation (1) is used to generate the sequence of permutation. The technique used for pixel permutation is based on the ascending sorting of the chaotic sequence. The subencrypted image (obtained from Section 2.4) is divided into several squared nonoverlapping blocks. The size of each block is decided by a secret key. For the first subimage block, the initial condition of the chaotic logistic map $X_0$ is derived from the external key. For the other subimage blocks, $X_0$ is provided by the last sequence generated. In the permutation process, sort the element of the sequence generated in ascending order and

compare the index between the original and sorted elements of the sequence generated and tabulate the index change. Apply this index change to the block considered to rearrange the location of each pixel within the same block.

*2.6. Masking with Chaotic Code.* In this step, we change the pixel value of the subencrypted block (obtained from Section 2.5). The chaotic sequence used to mask each pixel value in this part is generated from (2). The initial condition $Y_0$ is derived from the last sequence obtained from (1), $Y_0 = X(\alpha)$. As the numbers generated from (2) are not integer, the chaotic sequence is transformed into integer sequence as follows:

$$Y := y \times 1000, \tag{16}$$

$$Y := y \times \bmod(256). \tag{17}$$

The selected block is XORed with a block obtained from (17).

*2.7. Pseudocode of the Proposed Encryption Algorithm*

(1) Generate an external secret key.

(2) Calculate $r_x$, $r_y$, and $X_0$.

(3) Generate the matrix code $W$ by an ANN training process.

(4) Divide a plain image into four subimages.

(5) Divide the matrix code $W$ into four submatrices $C_i$.

(6) Divide subimage $A$ into several blocks $B_i$.

(7) Take the first block $B_1$ and XOR it with $C_1$.

(8) The result obtained in Step 7 is now the code for a next block $B_i$.

(9) Repeat 7 and 8 on the whole subimage $A$ to obtain subencrypted image $A$'.

(10) Divide $A$' into several squared blocks $M_i$.

(11) Generate permutation sequence using (1). Permute the location of each pixel in $M_1$ as indicated in Section 2.5.

(12) Generate masking sequence from (2) and XOR it with the block obtained from Step 11.

(13) Repeat Steps 11 and 12 on the whole $A$'.

(14) Repeat Steps 10–13 $k$ round.

(15) Repeat Steps 4–14 on the whole image $I$.

## 3. Computing Validation Using Experimental Data and Security Analysis

*3.1. Computing Validation.* Some computing results using experimental data are given in this section in order to demonstrate the efficiency of the proposed scheme. Several gray-scale images are evaluated. The duration of the training process in the case of Baboon image is one min (using Intel(R) core (TM) i3-2328M CPU 2.20 GHz, RAM 4Go). For the evaluation of encryption quality, the correlation coefficient (C.O) is used and is calculated as [1, 22]

$$\text{C.O} = \frac{N\sum_{j=1}^{N}\left(x_j \times y_j\right) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{\left(N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right) \times \left(N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right)}}, \tag{18}$$

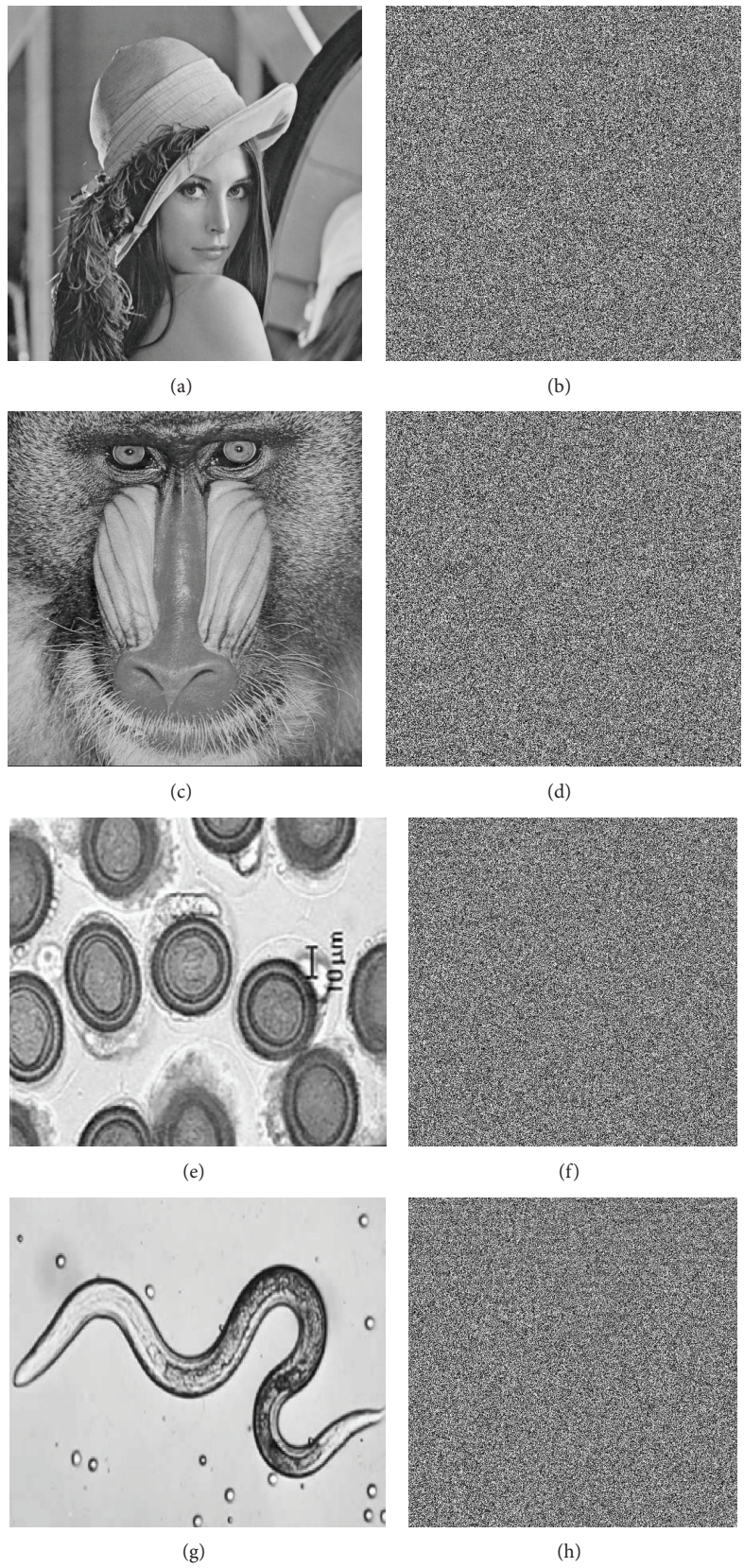
where $x$ and $y$ are gray-scale pixel values of the original and encrypted images and $N$ is the total number of pixels. We used the USC-SIPI image database which is a collection of digitized images available and maintained by the University of Southern California [1]. We used miscellaneous volume to measure the correlation coefficient of several USC-SIPI image databases (freely available at http://sipi.usc.edu/database/) [1]. The results are firstly compared with the encryption scheme presented by Fouda et al. [51], and an encrypted image scheme generated by the Pareek et al. [4] is applied secondly in the medical image. A striking example of the degree provided by the proposed cipher reveals patterns in the plain text as shown in Figure 3, where the plain images are encrypted by the secret key "234211004529726043091008812970 41" (decimal). Computationally, it is clear that there is negligible correlation between the plain image and ciphered image, as shown in Tables 1 and 2 where the proposed scheme shows the smallest correlation coefficient (C.O). Thus, the proposed scheme provides better performances than those obtained by Fouda et al. (2014) [51] and Pareek et al. methods (2013) [4] (Table 1).

*3.2. Security Analysis.* A good encryption scheme should resist against all kinds of known attacks, such as known-plain-text attack, cipher text attack, statistical attack, and various brute force attacks [1, 4, 51]. Some security analyses on the proposed image encryption scheme, including the most important ones like key space analysis and statistical analysis, which demonstrated the satisfactory security of the proposed scheme, are described. Various images have been tested, and similar results are obtained. However, due to page limit, only the results for Lenna, Baboon, and medical images such as *Taenia saginata* and *Toxocara canis* (Figure 3) are used for illustration.

*3.2.1. Key Space Analysis.* A good image encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to make brute force attacks infeasible. For the proposed image encryption algorithm, key space analysis and testing have been performed and completely carried out and the results are summarized as follows.

*(i) Key Space.* The proposed image cipher has $2^{128}$ different combinations of secret keys.

*(ii) Key Sensitivity Test.* An ideal image encryption procedure should be sensitive with respect to the secret key; that is, the change of a single bit in the secret key should produce a completely different encrypted image. To test the sensitivity of




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

Figure 3: Encryption by the proposed scheme using the secret key "234211004529726043091008812970 41." Frames (a) and (b) show a plain image "Lenna" and its corresponding cipher image, respectively. Frames (c) and (d) show a plain image "Baboon" and its corresponding cipher image, respectively. Frames (e) and (f) show a plain image "*Taenia saginata*" and its corresponding cipher image, respectively. Frames (g) and (h) show a plain image "*Toxocara canis*" and its corresponding cipher image, respectively.

Table 1: Comparative results.

| Image parameters | | | Correlation coefficients | | | Entropy information | | |
|---|---|---|---|---|---|---|---|---|
| Image name | Size | Type | Fouda et al. [51], Pareek et al. [4] | | Proposed scheme | Fouda et al. [51], Pareek et al. [4] | | Proposed scheme |
| Girl (Lenna) | 512 × 512 | Gray | −0.0017 | −0.0003 | −3.2825*e* − 005 | 7.9992 | 7.9952 | 7.9994 |
| Baboon | 512 × 512 | Gray | −0.0024 | — | −2.0137*e* − 004 | 7.9991 | — | 7.9993 |
| Peppers | 200 × 200 | Gray | — | −0.0012 | 6.2295*e* − 004 | — | 7.9844 | 7.9992 |

Table 2: Correlation coefficients and entropy information between the gray image and corresponding cipher image of several USC-SIPI images databases and some medical images. The encryption has been done using the secret key "234211004529726043091008812970 41."

| File name | File description | Size | Correlation coefficients | Entropy information |
|---|---|---|---|---|
| 4.1.01 | Girl | 256 × 256 | −3.1456*e* − 004 | 7.9975 |
| 4.1.05 | House | 256 × 256 | 6.5647*e* − 004 | 7.9975 |
| 5.1.12 | Clock | 256 × 256 | −8.5321*e* − 004 | 7.9971 |
| 4.2.04 | Girl (Lenna) | 512 × 512 | −3.2825*e* − 005 | 7.9994 |
| 4.2.03 | Baboon | 512 × 512 | −2.0137*e* − 004 | 7.9993 |
| Elaine. 512 | Girl (Elaine) | 512 × 512 | 2.6659*e* − 004 | 7.9993 |
| 4.2.07 | Peppers | 512 × 512 | 9.5657*e* − 004 | 7.9992 |
| Boat. 512 | Fishing Boat | 512 × 512 | −4.6505*e* − 004 | 7.9993 |
| 7.1.01 | Truck | 512 × 512 | 2.4855*e* − 004 | 7.9994 |
| — | Toxoplasma gondii | 512 × 512 | −3.1456*e* − 004 | 7.9993 |
| — | *Taenia saginata* | 512 × 512 | −7.7169*e* − 004 | 7.9993 |
| — | *Entamoeba coli* | 512 × 512 | −5.1410*e* − 004 | 7.9993 |
| — | Plasmodium falciparum | 512 × 512 | −3.3624*e* − 005 | 7.9958 |
| — | *Cryptosporidium* sp. *oocysts* | 512 × 512 | 1.6842*e* − 004 | 7.9994 |
| 5.3.03 | Man | 1024 × 1024 | −6.8554*e* − 004 | 7.9998 |

Table 3: Correlation between various decrypted images shown in Figure 4.

| Correlation coefficient between various decrypted images shown in Figure 4 | |
|---|---|
| Figures 4(a) and 4(b) | 8.7604*e* − 004 |
| Figures 4(a) and 4(c) | 1.5835*e* − 004 |
| Figures 4(a) and 4(d) | 0.0030 |
| Figures 4(b) and 4(c) | 8.1398*e* − 004 |
| Figures 4(b) and 4(d) | −0.0041 |
| Figures 4(c) and 4(d) | 0.0034 |

the proposed image cipher with respect to the key, encrypted image corresponding to plain image is decrypted with a slightly different key compared to the original one. Further, we calculate correlation coefficient between the encrypted image and the image decrypted using a slightly different key. This procedure is described as follows.

(a) The encrypted image (Figure 3(b)) is decrypted by making a slight modification in the original key "234211004529726043091008**8**2297041" and the resultant encrypted image is shown in Figure 3(a).

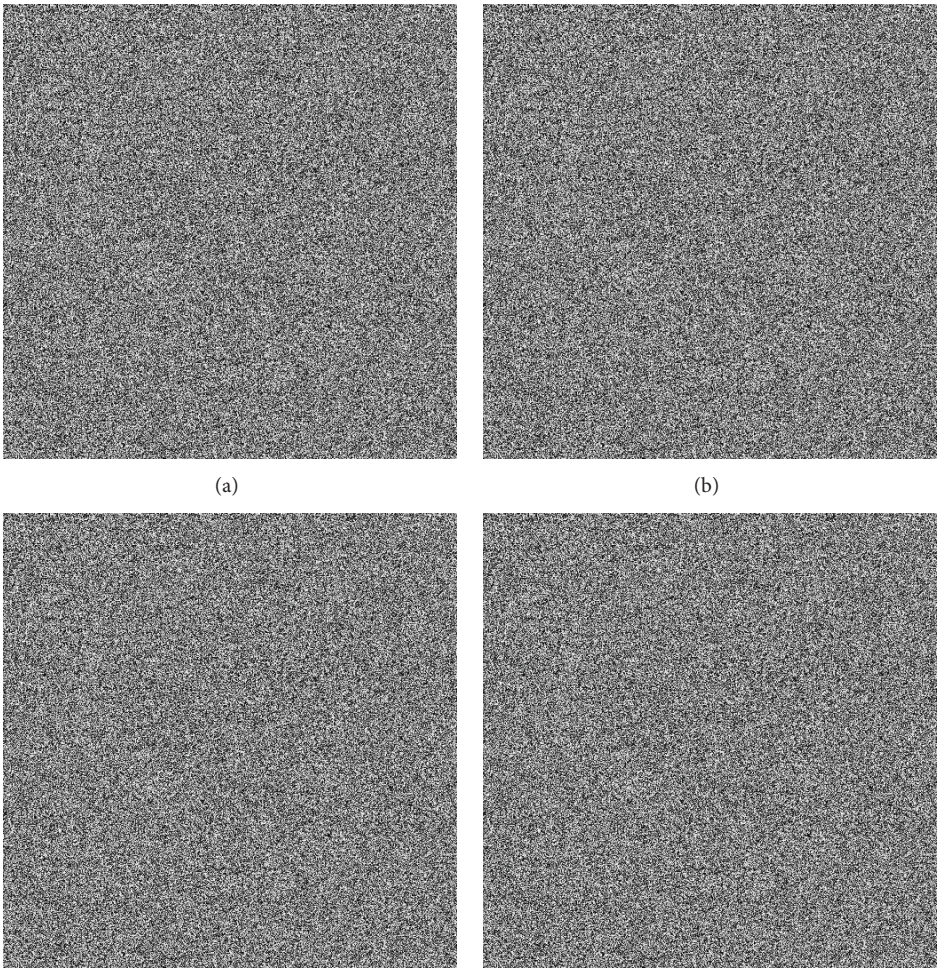
(b) The encrypted image (Figure 3(b)) is decrypted by making a slight modification in the original key "234211004529726043091008812970**8**1" and the resultant encrypted image is given in Figure 3(b).

(c) The encrypted image (Figure 3(b)) is decrypted by making a slight modification in the original key "**23521**1004529726043091008812970 41" and the resultant encrypted image is depicted in Figure 3(c).

(d) The encrypted image (Figure 3(b)) is decrypted by making a slight modification in the original key "23421**1045**29726043091008812970 41" and the resultant encrypted image is reported in Figure 3(d).

With a slight change in the key, one is unable to find any clue about the original image from the decrypted image. To compare the decrypted images, we have calculated the correlation coefficient. The results are given in Table 3. We conclude from this table that one cannot find any clue about the plain image even if there is a little change in the key. The correlation coefficient is negligible. Having the right pair of secret key is an important part while decrypting the image, as a slight change in the secret key will not retrieve the exact original image. The above example shows that the decryption of the encrypted image with the wrong secret key will not reveal any information about the original image. These results confirm the effectiveness of the proposed algorithm.

*3.2.2. Statistical Analysis.* Statistical analysis on the proposed image encryption algorithm shows superior confusion and diffusion properties which strongly resist statistical attacks.



(a) (b) (c) (d)

Figure 4: Frames (a)–(d) show the decrypted images from the encrypted image of Figure 3(b) using slightly different keys compared to the key used for encryption.

Table 4: Correlation coefficients of two adjacent pixels in original and encrypted images.

| Images | HC | VC | DC |
|---|---|---|---|
| Girl | $-1.8772e-004$ | $-0.0015$ | $-0.0015$ |
| House | $-9.1631e-004$ | $-9.2734e-004$ | $-0.0033$ |
| Clock | $9.4186e-004$ | $-1.4436e-004$ | $-0.0102$ |
| Girl (Lenna) | $5.4435e-004$ | $3.2131e-004$ | $-4.4382e-004$ |
| Baboon | $3.6478e-004$ | $4.3778e-004$ | $-0.0028$ |
| Girl (Elaine) | $8.7529e-004$ | $3.7196e-004$ | $-7.3646e-004$ |
| Peppers | 0.0020 | $-9.5121e-005$ | 0.0040 |
| Fishing Boat | 0.0011 | $-5.4823e-004$ | 0.0020 |
| Truck | $3.6615e-004$ | $-4.0810e-004$ | $7.0184e-004$ |
| Toxoplasma gondii | $-6.8938e-004$ | $-2.2139e-004$ | $-0.0013$ |
| *Taenia saginata* | $-0.0010$ | $2.7169e-004$ | 0.0019 |
| Plasmodium falciparum | $-1.6999e-004$ | $1.4880e-005$ | $2.7926e-004$ |
| *Cryptosporidium* sp. *oocysts* | $-7.2488e-004$ | $-9.9171e-004$ | $-0.0018$ |

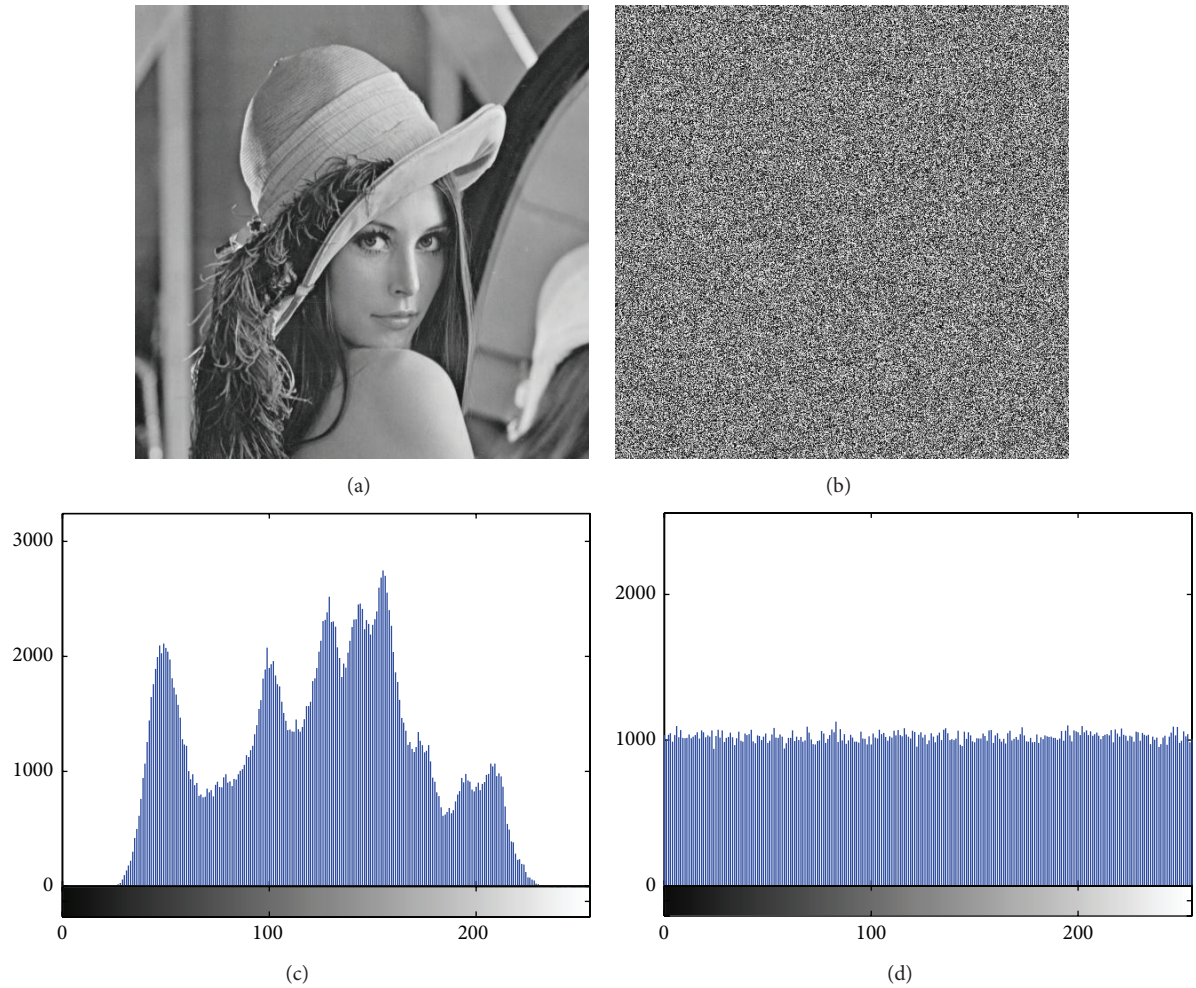



Figure 5: Histogram analysis: frames (a) and (b) show a plain image "Lenna" and its corresponding cipher image, respectively. Frames (c) and (d) show histograms of images shown in frames (a) and (b), respectively.

This can be shown by a test on the histograms of the enciphered images and on the correlations of adjacent pixels in the ciphered image [36] as described in the next paragraph.

*Histograms of Encrypted Images*. Statistical analysis of Lenna images and their encrypted images yielded their gray-scale histogram given in Figure 5. This figure shows that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. Also, it demonstrates that the encryption algorithm has covered up all the characters of the plain image.

*Correlation of Two Adjacent Pixels*. To test the correlation between two adjacent pixels in plain image and ciphered image, the following procedure was carried out. First, randomly select all pairs of two adjacent (in horizontal, vertical, and diagonal directions) pixels from an image. Then, referring to [1], calculate the correlation coefficient of each pair by (18). The results for horizontal, vertical, and diagonal directions were obtained and are shown in Table 4. These correlation analyses prove that the proposed encryption technique satisfies zero cocorrelation property; thus its robustness against statistical attacks is proved.

*3.2.3. Entropy Information Analysis.* Information entropy, introduced by Pareek et al. [4], is a common criterion that shows the randomness of the data. The expression of entropy information is given by

$$H(S) = -\sum_{i=0}^{N-1} P(S_i) \log_2 \left( \frac{1}{P(S_i)} \right), \tag{19}$$

where $N$ is the number of gray levels in the image and $P(s_i)$ shows the probability of appearance of the symbol $s_i$. In the case of 256 gray-scale images, truly random image entropy is equal to eight [51], which is the ideal value. The entropy of a practical source generating random messages is smaller than the ideal one. However, the entropy of encrypted messages should be equal to eight; otherwise there exists a certain degree of predictability which threatens its security. Table 2 gives the entropy of images encrypted by the proposed scheme. It appears that the entropy of ciphered images is

Table 5: NPCR and UACI of some ciphered images.

| Images | Girl (Lenna) | Baboon | Girl (Elaine) | Peppers | Toxoplasma gondii | *Toxocara canis* |
|---|---|---|---|---|---|---|
| NPCR | 99.6128 | 99.6206 | 99.6018 | 99.6125 | 99.6022 | 99.6204 |
| UACI | 33.4203 | 33.4405 | 33.5032 | 33.48025 | 33.5120 | 33.4365 |

almost close to eight. We can conclude that the proposed encryption method is robust against entropy attack.

*3.2.4. Differential Attacks.* Another desirable property for the proposed cipher is its sensitivity to small changes in the plain image (single bit change in plain image). To test the influence of one-pixel change on the plain image encrypted by the proposed cipher, two common measures may be used, number of pixels change rate (NPCR) and unified average changing intensity (UACI) [22, 51], which are calculated. Therefore, if $A(i, j)$ and $B(i, j)$ are the pixels in row $i$ and column $j$ of the encrypted images $A$ and $B$, with only one-pixel difference between the respective plain images, then the NPCR is calculated by using the following formula:

$$\text{NCPR} = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\%, \tag{20}$$

where $W$ and $H$ are the width and height of $A$ or $B$. $D(i, j)$ is produced by the following way:

$$D(i, j) = \begin{cases} 1 & \text{if } A(i, j) \neq (i, j) \\ 0 & \text{ortherwise.} \end{cases} \tag{21}$$

The second number (UACI) measures the average intensity of differences between the plain image and the encrypted image calculated by the following formula:

$$\text{UACI}(A, B) = \frac{1}{W \times H} \left[ \sum_{i,j} \frac{|A(i, j) - B(i, j)|}{255} \right] \times 100\%. \tag{22}$$

Computing values of NPCR and UACI for a few images are shown in Table 5. According to the values of the NPCR over 99.60% for all images, the encryption scheme is very sensitive with respect to small changes in the plain image. The UACI in all cases is found close to the ideal values of 33.33% indicating that the rate of influence due to one-pixel change is very large. Generally, these obtained results for NPCR and UACI obtained after only one round encryption show that the proposed algorithm is very sensitive with respect to plain image (plain images have only one-pixel difference).

## 4. Conclusion

In this paper, a robust gray image encryption scheme based on chaotic logistic map combined with artificial neural network has been proposed. In the proposed image encryption scheme, an external key of 128 bits, two chaotic logistic maps, and multilayer perceptron have been used to confuse the relationship between the cipher image and the plain image. The main feature of this algorithm is that it is easily implementable and hence more suitable for image encryption applications. Computing results using experimental data and security analysis have shown that our proposed scheme provides better performance than some recent results of literature.

## Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

## References

[1] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, no. 9, pp. 926–934, 2006.

[2] V. Patidar, N. K. Pareek, G. Purohit, and K. Sud, "Modified substitution-diffusion image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 10, pp. 2755–2765, 2010.

[3] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[4] N. K. Pareek, V. Patidar, and K. K. Sud, "Diffusion-substitution based gray image encryption scheme," *Digital Signal Processing*, vol. 23, no. 3, pp. 894–901, 2013.

[5] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," *Optics Communications*, vol. 284, no. 12, pp. 2775–2780, 2011.

[6] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Optics Communications*, vol. 284, no. 22, pp. 5290–5298, 2011.

[7] C.-C. Chang, M.-S. Hwang, and T.-S. Chen, "A new encryption algorithm for image cryptosystems," *Journal of Systems and Software*, vol. 58, no. 2, pp. 83–91, 2001.

[8] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[9] L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 759–765, 2005.

[10] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 372, no. 15, pp. 2645–2652, 2008.

[11] B. S. Wong, K. Kwok, and L. Wing-Shing, "A fast image encryption scheme based on chaotic standard map," *Physics Letters*, pp. 2645–2652, 2008.

[12] S. Li, C. Li, G. Chen, and K.-T. Lo, "Cryptanalysis of the RCES/RSES image encryption scheme," *Journal of Systems and Software*, vol. 81, no. 7, pp. 1130–1143, 2008.

[13] G. Alvarez and S. Li, "Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 11, pp. 3743–3749, 2009.

[14] C. Li, S. Li, G. Chen, and W. A. Halang, "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," *Image and Vision Computing*, vol. 27, no. 8, pp. 1035–1039, 2009.

[15] H. Cheng, "Partial encryption of compressed images and videos," *IEEE Transactions on Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.

[16] J. C. Yen and J. I. Guo, "An efficient hierarchical chaotic image encryption algorithm and its VLSI realization," *IEE Proceedings-Vision Image Processing*, vol. 147, pp. 167–175, 2000.

[17] K. Wang, W. Pei, L. Zou, A. Song, and Z. He, "On the security of 3D Cat map based symmetric image encryption scheme," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 343, no. 6, pp. 432–439, 2005.

[18] G. Chen and S. T. Liu, "On generalized synchronization of spatial chaos," *Chaos, Solitons and Fractals*, vol. 15, no. 2, pp. 311–318, 2003.

[19] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[20] F. Sun, S. Liu, Z. Li, and Z. Lü, "A novel image encryption scheme based on spatial chaos map," *Chaos, Solitons and Fractals*, vol. 38, no. 3, pp. 631–640, 2008.

[21] F. Sun and S. Liu, "Cryptographic pseudo-random sequence from the spatial chaotic map," *Chaos, Solitons and Fractals*, vol. 41, no. 5, pp. 2216–2219, 2009.

[22] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Optics Communications*, vol. 284, no. 19, pp. 4331–4339, 2011.

[23] S. A. Parah, J. A. Sheikh, A. M. Hafiz, and G. M. Bhat, "Data hiding in scrambled images: a new double layer security data hiding technique," *Computers and Electrical Engineering*, vol. 40, no. 1, pp. 70–82, 2014.

[24] L. Y. Zhang, C. Li, K.-W. Wong, S. Shu, and G. Chen, "Cryptanalyzing a chaos-based image encryption algorithm using alternate structure," *Journal of Systems and Software*, vol. 85, no. 9, pp. 2077–2085, 2012.

[25] X.-J. Tong, "The novel bilateral—diffusion image encryption algorithm with dynamical compound chaos," *The Journal of Systems and Software*, vol. 85, no. 4, pp. 850–858, 2012.

[26] S. T. Liu and F. Y. Sun, "Spatial chaos-based image encryption design," *Science in China, Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 2, pp. 177–183, 2009.

[27] X. Zhang, L. Shao, Z. Zhao, and Z. Liang, "An image encryption scheme based on constructing large permutation with chaotic sequence," *Computers and Electrical Engineering*, vol. 40, no. 3, pp. 931–941, 2014.

[28] X. Wang and G. He, "Cryptanalysis on a novel image encryption method based on total shuffling scheme," *Optics Communications*, vol. 284, no. 24, pp. 5404–5407, 2011.

[29] I. Darkiran and K. Danisman, "Artificial neural network based chaotic generator for cryptology," *The Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 18, pp. 744–753, 2010.

[30] N. Bigdeli, Y. Farid, and K. Afshar, "A robust hybrid method for image encryption based on Hopfield neural network," *Computers and Electrical Engineering*, vol. 38, no. 2, pp. 356–369, 2012.

[31] N. Bigdeli, Y. Farid, and K. Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks," *Engineering Applications of Artificial Intelligence*, vol. 25, no. 4, pp. 753–765, 2012.

[32] T. Gao, Q. Gu, and S. Emmanuel, "A novel image authentication scheme based on hyper-chaotic cell neural network," *Chaos, Solitons & Fractals*, vol. 42, no. 1, pp. 548–553, 2009.

[33] A. Kassem, H. A. H. Hassan, Y. Harkouss, and R. Assaf, "Efficient neural chaotic generator for image encryption," *Digital Signal Processing: A Review Journal*, vol. 25, no. 1, pp. 266–274, 2014.

[34] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1773–1783, 2009.

[35] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," *Chaos, Solitons and Fractals*, vol. 42, no. 3, pp. 1745–1754, 2009.

[36] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.

[37] P. Manjunath and K. L. Sudha, "Chaos image encryption using pixel shuffling," *CS and IT*, vol. 2, pp. 169–179, 2011.

[38] H. H. Nien, W. T. Huang, C. M. Hung et al., "Hybrid image encryption using multi-chaos-system," in *Proceedings of the 7th International Conference on Information, Communications and Signal Processing (ICICS '09)*, pp. 1–5, 2009.

[39] K.-W. Wong, B. S.-H. Kwok, and C.-H. Yuen, "An efficient diffusion approach for chaos-based image encryption," *Chaos, Solitons & Fractals*, vol. 41, no. 5, pp. 2652–2663, 2009.

[40] C. Fu, B.-B. Lin, Y.-S. Miao, X. Liu, and J.-J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, no. 23, pp. 5415–5423, 2011.

[41] G. J. Zhang and Q. Liu, "A novel image encryption method based on a skew tent map," *Optics Communications*, vol. 284, 2011.

[42] X. Wang, J. Zhao, and H. Liu, "A new image encryption algorithm based on chaos," *Optics Communications*, vol. 285, no. 5, pp. 562–566, 2012.

[43] L. Teng and X. Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive," *Optics Communications*, vol. 285, no. 20, pp. 4048–4054, 2012.

[44] Z. Eslami and A. Bakhshandeh, "An improvement over an image encryption method based on total shuffling," *Optics Communications*, vol. 286, no. 1, pp. 51–55, 2013.

[45] J. Liu, H. Jin, L. Ma, Y. Li, and W. Jin, "Optical color image encryption based on computer generated hologram and chaotic theory," *Optics Communications*, vol. 307, pp. 76–79, 2013.

[46] S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin, "Image encryption based on the Jacobian elliptic maps," *The Journal of Systems and Software*, vol. 86, no. 9, pp. 2429–2438, 2013.

[47] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "Image encryption based on the jacobian elliptic maps," *Image and Vision Computing*, vol. 27, pp. 1371–1381, 2009.

[48] G. Bhatnagar and Q. M. Wu, "Selective image encryption based on pixels of interest and singular value decomposition," *Digital Signal Processing*, vol. 22, no. 4, pp. 648–663, 2012.

[49] X. Wang, D. Luan, and X. Bao, "Cryptanalysis of an image encryption algorithm using Chebyshev generator," *Digital Signal Processing: A Review Journal*, vol. 25, no. 1, pp. 244–247, 2014.

[50] S. Bahrami and M. Naderi, "Image encryption using a lightweight stream encryption algorithm," *Advances in Multimedia*, vol. 2012, Article ID 767364, 8 pages, 2012.

[51] J. S. Fouda, J. Y. Effa, S. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 3, pp. 578–588, 2014.

[52] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 3998–4006, 2010.

[53] T. Chen and J. Cai, "A novel remote user authentication scheme using interacting neural network," in *Advances in Natural Computation*, vol. 3610 of *Lecture Notes in Computer Science*, pp. 1117–1120, Springer, Berlin, Germany, 2005.

[54] Y. Hu, C. Zhu, and Z. Wang, "An improved piecewise linear chaotic map based image encryption algorithm," *The Scientific World Journal*, vol. 2014, Article ID 275818, 7 pages, 2014.

[55] R. Boriga, A. C. Dăscălescu, and A.-V. Diaconu, "A new one-dimensional chaotic map and its use in a novel real-time image encryption scheme," *Advances in Multimedia*, vol. 2014, Article ID 409586, 15 pages, 2014.