WILEY | Hindawi

Research Article

An Improved Image Processing Based on Deep Learning Backpropagation Technique

Yang Gao[1] **and Yue Tian** [2]

[1]*Academy of Fine Arts, Shenyang University, Liaoning, Shenyang, China*
[2]*Shenyang Institute of Computing Technology Co Ltd, The Chinese Academy of Sciences, Liaoning, Shenyang, China*

Correspondence should be addressed to Yue Tian; tianyue@sict.ac.cn

In terms of image processing, encryption plays the main role in the field of image transmission. Using one algorithm of deep learning (DL), such as neural network backpropagation, increases the performance of encryption by learning the parameters and weights derived from the image itself. The use of more than one layer in the neural network improves the performance of the algorithm. Also, in the process of image encryption, randomness is an important component, especially when used by smart learning methods. Deep neural networks are related to pixels used to manipulate position and value according to the predicted new value given from a variable neural system. It also includes messy encrypted images used via applying randomness and increasing the key space in addition to using the logistic and Henon map for complexity. The main goal of any encryption method is to increase the complexity of the encrypted image to be difficult or impossible to decrypt the image without the proposed key. One of the important measurements for image encryption is the histogram and how it can be uniformed by the proposed method. Variables of randomness are used as features for the deep learning system, with feedback during iteration. An ideal image processing encryption yields high messy images by keeping the quality. Experimental results showed the backpropagation algorithm achieved better results than other algorithms.

1. Introduction

Image encryption is one of the classifications that can classify image security. Security is the most important issue in the digital computer world, and such security can be classified as steganography, watermark, and encryption [1]. Image processing is useful in many applications that accompany the terms data security, physical security, and digital security. These terms go hand in hand when it comes to data security, especially image security. They are related to national security, surveillance applications, identity authentication, and so on. Therefore, it is natural to use modern technologies, such as deep learning and the neural network algorithm, which use education to predict the next step. Encryption has a different term, which is focusing on challenging the hacker and the secret method presented in advance, while steganography and watermark hide the secret

through imperceptibility. This refers to secret communication used thousands of years ago in a way that cannot be read, except with the license from the sender [2]. This ensures that confidential information does not fall into the wrong hands. Images are the most important media for encryption because of not being easy to cover and more reliable. Given the rapid development in Internet technology, as well as security, images are considered one of the main sources of data security [3]. One of the most popular types of media on the Internet is images; therefore, they are always vulnerable to unauthorised hacking and manipulation. Images consist of an enormous number of cells called pixels, and each pixel has an internal relationship, such as colour and density, and an external relationship to the neighbouring pixels [4]. Chaotic cryptography has been considered for the past two decades, and more researchers are focusing on the fundamentals of chaos characteristics

and the sensitivity of the initial conditions. Beginning in 1998, many studies have investigated chaotic cryptography in relation to neural networks with built-in hidden layers [5]. The neural network always behaves like a nonlinear distribution of network parameters over the clusters. During unsupervised learning, the features extracted produce a great number of subfeatures simultaneously that help with image encryption.

There are three types of image security in the image processing technique; firstly, steganography aims to hide secrets inside the image in a manner that is not visible to the intruder [6]. Secondly, a watermark aims to hide secrets inside image media by increasing its imperceptibility. The secret message must be unseen in both steganography and watermark [7]. The third and last type is encryption of the image. In this case, the secret will be the image itself and would be challenging for the hacker to decrypt [8]. Figure 1 shows the three types of image security.

Watermark is responsible for embedding images within media, and the media includes images, text, sound, or protocol. Meanwhile, steganography is related to embedding text inside media, such as an image. Both steganography and watermark work in terms of imperceptibility, while encryption makes it challenging to find encrypted media.

Images are usually encrypted by using one chaotic sequence, but when using a neural network, this may change depending on the number of hidden layers. Thus, the batch encryption of images is used for an independent sequence. The chaos variables are responsible for the amount of complexity in encryption, which is often one. However, in modern methods, it is more than one. This is the first step; the next step will generate matrices, i.e., the second matrices by mixing together the generated shuffling matrix. This matrix determines the pixels' position in the newly encrypted image. Image encryption is known as a set of processes called techniques or algorithms, which convert an original or plain image into a coded image in a manner that no one can recover it, just the receiver with a certain key.

The randomness of the pixels reflects how the image and changing pixel position should be planned so it can be possible to recover it. Changing the correlation of pixels will be mapped by using the key generated for this purpose and in a function called the random function, which is supposed to be strong and more reliable to generate the key [9]. The confusion process is the process that describes how cipher images are strongly reflected by the security of the image.

A cipher key is an important factor of any encryption method because it is responsible for encryption and decryption. There are two types of cipher keys according to the proposed method and strategy of encryption. The symmetric key is used in two places by the sender and receiver during encryption and decryption and must be strong enough. The asymmetric key is different from the symmetric key and needs to be used by a sender or receiver as public and private keys as shown in Figure 2.

The manuscript is structured as the introduction section to illustrate the definition first, followed by exploring the existing methods in the literature review section; then the issue to be solved is mentioned in the problem statement
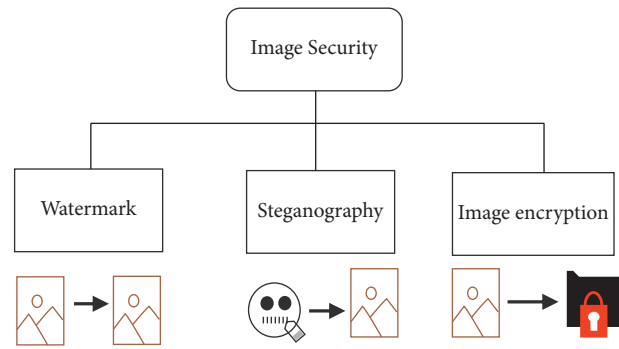

FIGURE 1: Type of image security as classified.

section. Details of deep learning are presented in the deep learning section and then proceeded by the proposed method in the method section. The experimental results are analysed in the results section to prove the proposed method. The last section is considered the conclusion section to summarise the manuscript.

2. Literature Review

Due to the importance of image encryption and using deep learning algorithms to solve their issues, there are so many existing research studies presented in the literature. The encryption of medical images presented by [10] used the Internet of Medical Things (IoMT) to connect many images of the human body to create a comprehensive image for treatment by doctors. There is an increase in the robustness of 2D and 3D for optical images and deep convolution neural networks, which are used for image encryption to stand against an attack [11]. Different encryption keys are used for encrypting medical images to increase the accuracy of the encrypted images under the deep residual networks [12] for learning. Deep neural networks are used to encrypt image pixels within positions by segmenting the pixels into groups and then updating the key simultaneously, with data augmentation considered in this technique [13]. The study by [14] attacks the chaos-based image encryption of deep learning used for low-dimensional features extracted from the pixels' behaviour.

2.1. Problem Statement. Using the conventional image that is produced from the encryption method for a high level of security is suitable. However, there are still many issues that control image encryption. Usually, image encryption includes the challenge of designing the random key generated that is used in both encryption and decryption [15].

The randomness of the pixels inside the image is controlled by a random number generator and must be unique and unpredictable due to its responsibility for the messiness of the encrypted image. To avoid a statistical attack, the random function must be robust against any changes or modifications [16].

The correlation of pixel distribution inside an image emphasises good encryption. The complexity of this distribution makes a conventional image have better
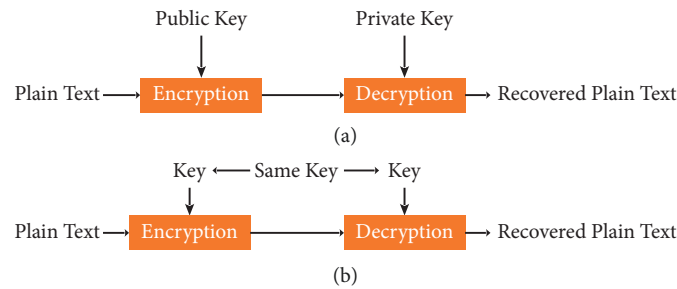
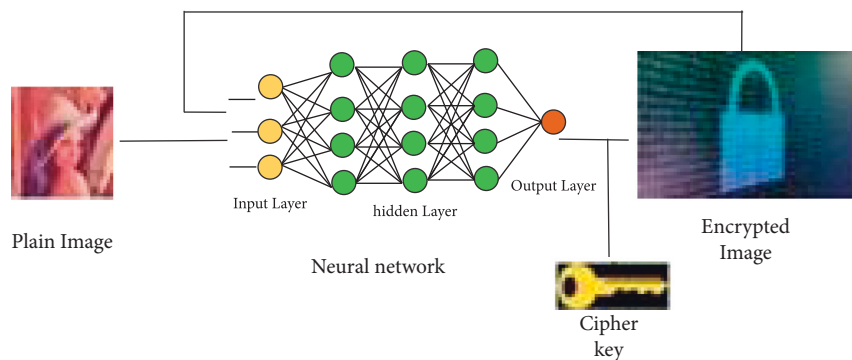FIGURE 2: Key types: (a) asymmetric key and (b) symmetric key.

FIGURE 3: Deep learning system of an encrypted image.

correlation and more randomisation of the pixels inside. The repositioning of the pixels allows the image to stop any type of attack.

The key space of the random method must be increased to achieve better security and reliability. Then, a 2D random key space makes a large initial size for confusion and diffusion and an image that gives more robustness and reliability [17]. This considers the main reference to find the novel idea, and it considers the core reference.

Considering the image histogram and entropy of a cipher image is needed because a statistical attack is sensitive to the entropy and equalisation of the uniform histogram, which leads to an increase in the entropy [18]. This is also necessary for avoiding differential attacks.

2.2. Deep Learning. With the development in data science and modern technology, such as big data (image pixels with high resolution), satellite image, and high-performance computers, there is an opportunity for machine learning for understanding data and its behaviour through complex systems [19]. Machine learning gives a machine the ability to learn in different algorithms without strict orders from certain programs or limited instructions [20].

Deep learning can be defined as a technique of machine learning to learn useful features directly from given images, sound, and text. Many layers are exploited by deep learning for nonlinear data processing of unsupervised or supervised feature extraction for classification and pattern recognition [21]. The deep learning motivation is greatly reduced by the Artificial Intelligence (AI) area, which simulates the ability

of the human brain in terms of analysis, making decisions, and learning [22]. Deep learning's goal is to emulate the approach of hierarchical learning of extracting features by the human brain directly from unsupervised data, such as a plain image.

The core of deep learning is that it is hieratically computed with the features and representation of information, such as the definition of the features starting from low-level to high-level [23]. Many applications are provided by machine learning [24]. With traditional image encryption or depleted coding, the standard techniques of machine learning do not work well when running directly because of ignoring the nature of the grid distribution of pixels. In deep learning, features are extracted automatically from a given image pixel's correlation. The characteristics of this method are considered one of the learning factors of the system.

The characteristics of the input image used as a feature are the key to the success of processing image pixels. There are limitations during encryption and decryption. For this reason, deep learning can be used with its feature extraction to resolve the limitations in such a field.

As mentioned before, the main difference between machine learning and deep learning is the features selection method [25], as shown in Figure 3.

The features of deep learning will be generated automatically to simulate the appropriate results. Different hidden layers participate in making decisions by using the feedback from the next layer to the previous one, or the resulting layer will be fed into the first layer [26]. DL enables computers to be able to perform complex calculations by relying on simpler calculations to optimise the computer's
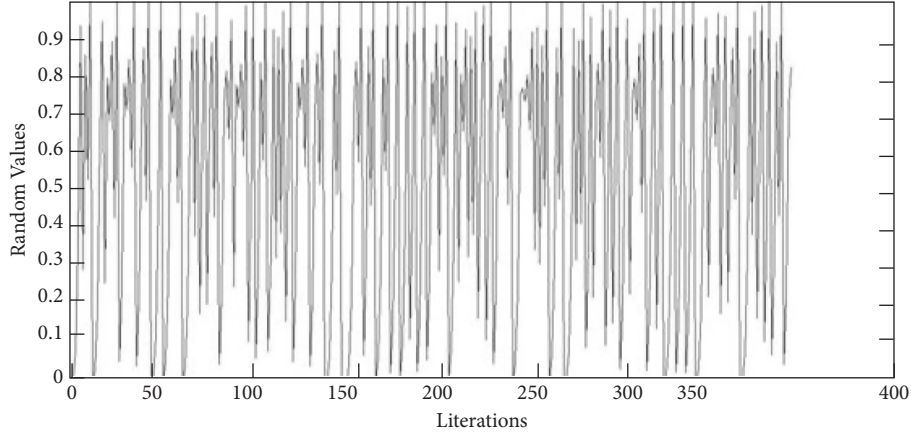
FIGURE 4: Behaviour of using a logistic map.

efficiency. It is difficult for a computer to understand complex data such as pixel correlation, thereby generating the confusion matrix and diffusion matrix, so deep learning algorithms are used instead of the usual learning methods [27]. The reason for using the deep learning technique is to improve the encryption that depends on the randomness of the selected pixels. The prediction of a new random map in encryption is the main part of using the deep learning technique.

3. Proposed Method

The process of image encryption using image processing techniques relies mainly on the power-generating key. Some existing methods depend on one key, and the rest depends on two keys for encryption. The proposed method used two chaotic maps, which are the Sensitive Logistic Maps (SLMs) and Henon Map. These were used to obtain randomness in the system for good criteria. The logistic map behaves as

$$X_{n+1} = rX_n(1 - X_n), \tag{1}$$

where $r \in (0.4)$ and $n = 1, 2, \ldots, n$, first value of X_1 in range $(0 < X_1 < 1)$. r for logistic map takes the range between 3.5699 and 4. Figure 4 illustrates the behaviour of the logistic map since $X_1 = 0.5$ and $r = 3.99$.

The second chaotic map is the Henon map which also increases the complexity of cryptography. To explain the details of the Henon map, the following equation is discussed:

$$\begin{aligned} X_{n+1} &= 1 - aX_n^2 + Y_n, \\ Y_{n+1} &= bX_n. \end{aligned} \tag{2}$$

X and Y are considered as the initial conditions, where a and b are control parameters for the cryptography system. Strong chaotic will be at $a = 1.4$ and $b = 0.3$ due to the Henon response for these two control parameters.

The encrypted image can be like a noisy image because of the random distribution of the pixel's loss and any helpful information presented visually. Therefore, removing noise that may affect the information of the image is necessary and

helpful. Noise is actually undesired data added to the image in a way that impacts the quality of the image. Many types of noise that images may be exposed to are salt and pepper, Gaussian, anisotropic, and shot noise. Gaussian noise is a famous one, whereby more probability affects the distribution of the image during encryption. For a better illustration, the Gaussian noise is presented in the following equation:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-(x-\mu)^2/2\sigma^2}, \tag{3}$$

where σ and μ are considered standard deviation with noise averaging and μ equals to Zero.

There are two important processes in each image encryption technique, i.e., the confusion and diffusion processes, as shown in Figure 5. The given image comes from a dataset, then starts preprocessing to normalise the image, and then prepares it for the confusion process.

Generating a random key includes considering the main issue in encryption due to scrambling of pixels based on randomness. Changing a pixel's position will change the view of an image, but the information is still not deleted. A pixel consists of two variable position coordinates (X, Y) and an intensity value. When changing the coordinate means changing position, the intensity value is still the same. Changing a pixel's position includes keeping track of the moving plan of the pixels. For randomness, the return value at the receiver side needs to be considered. For this reason, the algorithm followed by a sender (encryption) and receiver (decryption) is listed as follows.

Deep neural networks allow the selection of the row and column in a certain image. The algorithm of the chosen weight for each column or row has many hidden layers. Each layer is concluded from the weight derived according to the average of the intensity for a whole certain column or row, as shown in Figure 6.

Each feature that comes from a column or row will store the vector for manipulation, and each iteration will decide which column or row will be the next. The hidden layer plays the main role in a neural network system due to variable weights that take effect in this layer, and it is controlled when
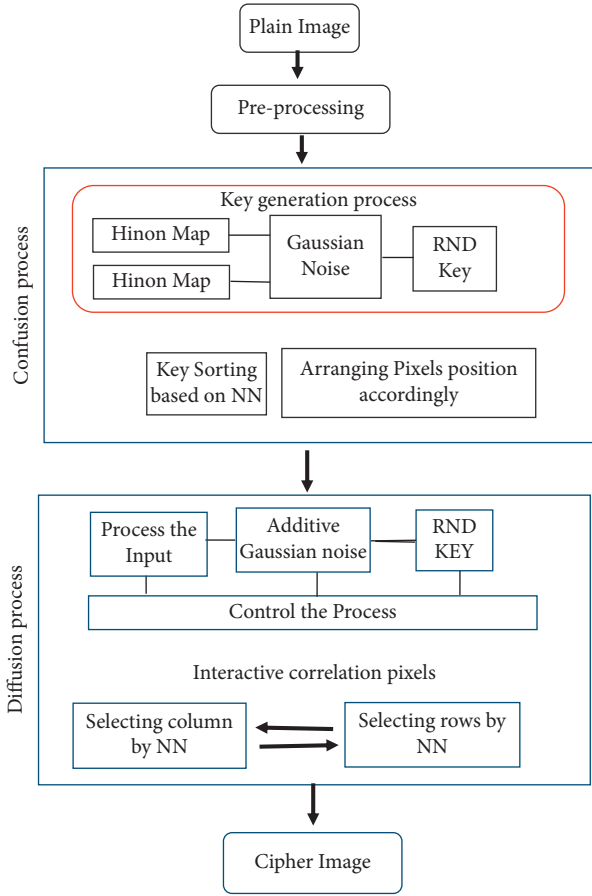
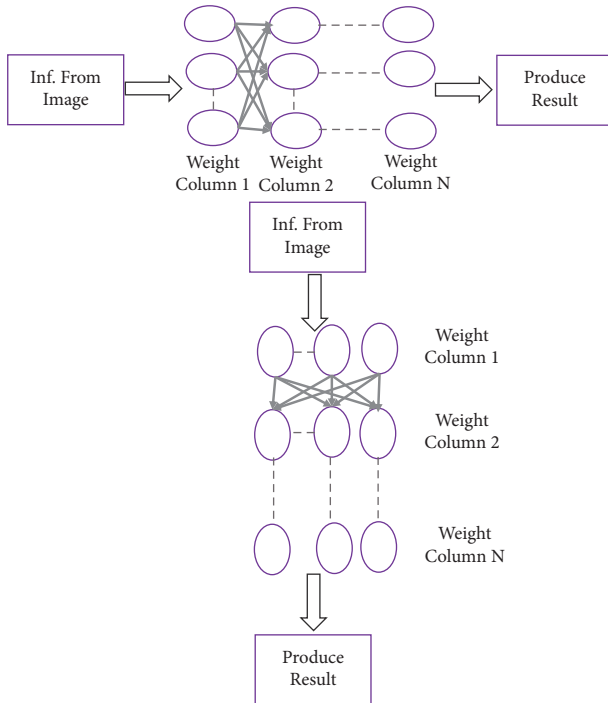FIGURE 5: A general overview of the proposed system.

FIGURE 6: Neural network strategy within pixel random position.

the training is finished until the desired results. During the confusion, the main issue of this process is the random number generated. This number is used to choose the next position for a pixel in a neural network and will increase the complexity of choosing the appropriate column or row. The random numbers will be for both X and Y during selection and are fed to a neural network to combine with the weight taken from the image's properties, as illustrated in the equation given as follows:

$$X.Y = \sum_{i=1}^{N} X_i \oplus \sum_{j=1}^{M} Y_j.$$ (4)

The coordinator of pixel (x, y) takes the first position from a random function and is updated by neural networks. During training, the system output position number may update the second time according to program predictions through feedback to hidden layers, for more complexity. In encryption, according to the proposed method, the image pixels will swap within column and row, and the alternative will be in both coordinate and value as shown in Figure 7.

The purpose of changing positions of all pixels in the image is to encrypt and confuse the hacker or intruder, as in Figure 7. So, the pixel value cannot be changed because it is valuable when decrypting at the receiver's side.

Confusion techniques rely first on a logistic map for swapping or repositioning pixels according to the correlation process. Changing the location of the pixel is necessary to stand against a statistical attack. Any encryption method suffers from statistical attacks. Thus, the application of the deep neural network of backpropagation is considered to make the correlation among pixels more robust in terms of horizontal and vertical swapping. To ensure the system is robust and the method is worthy, testing robustness is necessary by using the following equations:

$$Cor = \frac{cov(x.y)}{\sqrt{D(x)}\sqrt{D(y)}},$$ (5)

such as

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - x')^2,$$

$$D(y) = \frac{1}{N} \sum_{i=1}^{N} (y_i - y')^2,$$ (6)

$$cov(x.y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - x')(y_i - y').$$

These equations test the correlation among image pixels' neighbours in 8 neighbours (vertical, horizontal, and diagonal). The test includes an encrypted image, not a plain (original) image. There is another test that considers the relation between plain and cipher images and if there is a relationship or not. This test is presented in the following equations:
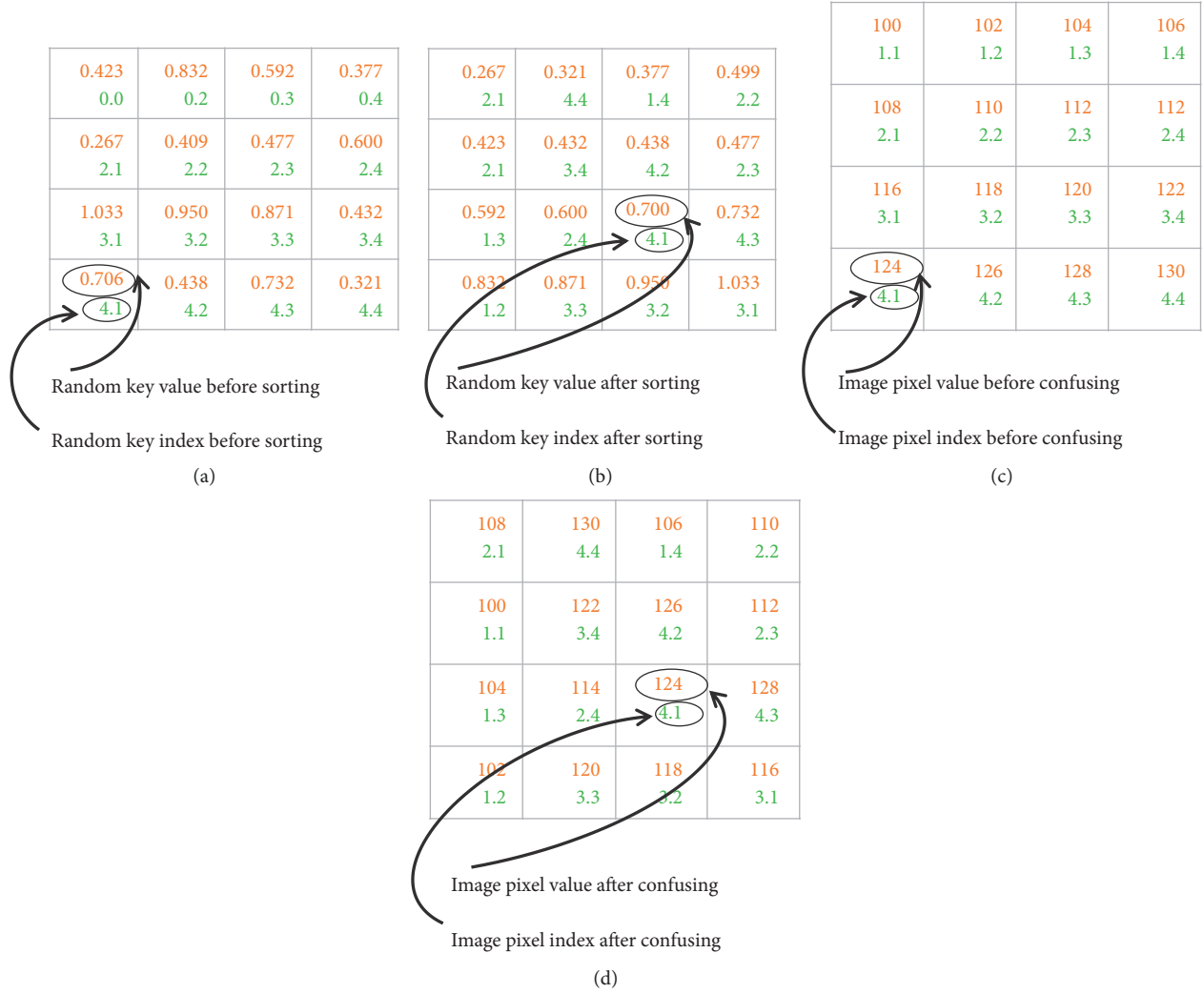
0.423 0.0	0.832 0.2	0.592 0.3	0.377 0.4
0.267 2.1	0.409 2.2	0.477 2.3	0.600 2.4
1.033 3.1	0.950 3.2	0.871 3.3	0.432 3.4
0.706 4.1	0.438 4.2	0.732 4.3	0.321 4.4

Random key value before sorting

Random key index before sorting

(a)

0.267 2.1	0.321 4.4	0.377 1.4	0.499 2.2
0.423 2.1	0.432 3.4	0.438 4.2	0.477 2.3
0.592 1.3	0.600 2.4	0.700 4.1	0.732 4.3
0.832 1.2	0.871 3.3	0.950 3.2	1.033 3.1

Random key value after sorting

Random key index after sorting

(b)

100 1.1	102 1.2	104 1.3	106 1.4
108 2.1	110 2.2	112 2.3	112 2.4
116 3.1	118 3.2	120 3.3	122 3.4
124 4.1	126 4.2	128 4.3	130 4.4

Image pixel value before confusing

Image pixel index before confusing

(c)

108 2.1	130 4.4	106 1.4	110 2.2
100 1.1	122 3.4	126 4.2	112 2.3
104 1.3	114 2.4	124 4.1	128 4.3
102 1.2	120 3.3	118 3.2	116 3.1

Image pixel value after confusing

Image pixel index after confusing

(d)

FIGURE 7: Changing pixel position during encryption.

$$\overline{A} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} A_{ij},$$

$$\overline{B} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} B_{ij}, \tag{7}$$

$$CC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(A_{ij} - \overline{A}\right)\left(B_{ij} - \overline{B}\right)}{\sqrt{\left(\sum_{i=1}^{M} \sum_{j=1}^{N} \left(A_{ij} - \overline{A}\right)\right)^2 \left(\sum_{i=1}^{M} \sum_{j=1}^{N} \left(B_{ij} - \overline{B}\right)\right)^2}},$$

where A is a plain image and B is a ciphered image, with dimensions of N and M, while CC considers the difference between cipher and plain images, which reflects the strength of the encryption.

One of the evaluations for image cryptography is the histogram, which gives the description of the frequency of pixels' behaviour and their values in the image. One of the criteria for the histogram is the difference between plain images and cipher images. A histogram still gives the same value even when scrambling the pixels. Therefore, a good

cipher image has a uniformed histogram so it can stop statistical attacks. The value of the pixels depicted by a histogram occurs between 0 (black pixel) and 255 (white pixel) for grey images. Figure 8 explains the behaviour of histograms.

The quantitative value of the image should be calculated, and the histogram of the cipher image should be uniform as in Figure 8; the following equation is used for testing uniformity:

$$Var(H) = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{\left(H_i - H_j\right)^2}{2}. \tag{8}$$

This is to estimate the pixels' value of the histogram. This test is used for a statistical attack to evaluate the cipher's image while there is another evaluation called entropy, which is used to measure random variables that are uncertain. Grey-scale images have 8 bits of entropy. Images produced from encryption must have their value of entropy the same as the grey image value. This entropy is also calculated using the following equation:
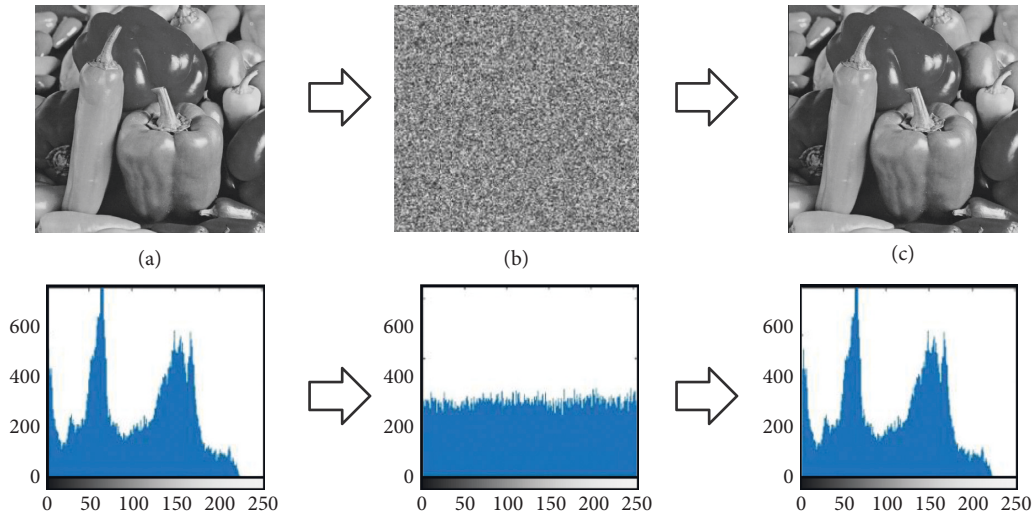
FIGURE 8: Histogram of plain and cipher image with the proposed method.

$$H(m) = \sum_{i=0}^{M-1} Pcv(m_i) \log_2 \frac{1}{P(m_i)}. \tag{9}$$

M is the number of pixels in the image, m_i is the possibility of occurrence, and *log* the base algorithm of 2 denotes the entropy result in binary mode. A perfect entropy is 8, which is for plain images, and for cipher images, it must be close to 8. When the entropy is 8, this means the image is safe, and the algorithm can face entropy-based attacks.

4. Experimental Results

For image encryption, many evaluation criteria can be used for evaluating the method. For the proposed method, there are more than five evaluation criteria. Most evaluations in this issue are to work on randomness and standing against attacks; the correlation of the image is important and correlation of pixels inside it. Evaluation takes the information from both plain and cipher images, and the evaluation process is achieved on the sender's side before sending it to the receiver. The plain image is processed and encrypted using keys similar to the process on the receiver's side, but on the contrary, as shown in Figure 9.

A plain image takes the process of encryption starting by using the information in the key, then producing a cipher image, and sending it to the other side to complete the process on the contrary. Encryption in the proposed method can work on both colour and grey images and images from a standard dataset used for evaluation and benchmarking. Figure 10 shows plain and cipher images of one image called Tiffany from a standard dataset.

The image after encryption looks messy, like in Figure 10 on the right, due to the distribution of the pixels being so messy and the value of each pixel transferred with it.

To evaluate the randomness of the proposed method according to the equation of the logistic map, a combination of the suggested random function with a Henon map in addition to white Gaussian noise implementation is shown in Table 1.
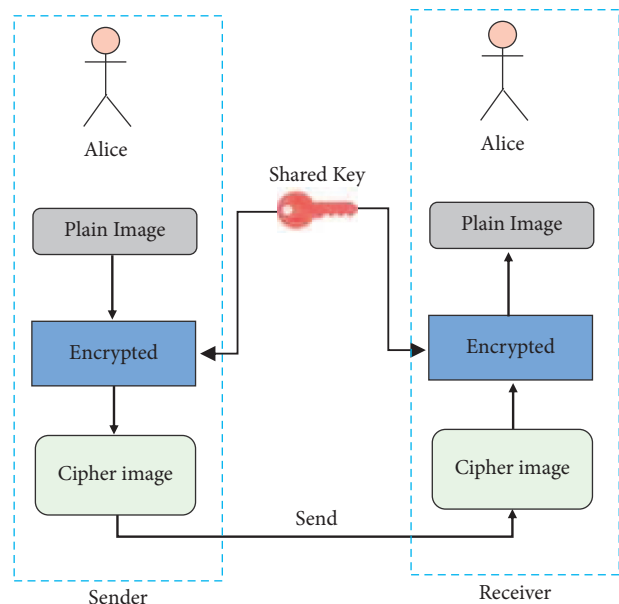

FIGURE 9: Protocol of encryption in the proposed method.

In the table, the P value with a proportion of the frequency of the pixels inside the image refers to an increase in the randomness of a random key generated by the proposed method. The listed results were achieved due to the method using three types of randomness, and the key space is increased.

The correlation of the pixels can also be evaluated when implementing the system. When using the correlation equation proposed method, choose 5000 pixels by random function and then the algorithm through the neural network with many iterations analyses these pixels in a manner of 8 neighbours: vertical, horizontal, and diagonal. Table 2 shows the correlation of the plain image with adjacent pixels to the image chosen from the SIPI dataset.

Correlation, as listed in the table, is very high due to the difference between the pixel value and corresponding

Figure 10: Tiffany's image and its cipher image.

Input: four (RND) vectors
Output: one (RND) vector
Begin
{**For** all RND vectors **do**
If Amended Bernoulli >0.34 **then** select element from Tinkerbell vector
If 0.34 = < Amended Bernoulli <0.67 **then** select element from Burger vector
Else the selected element is from Ricker vector }
End

Algorithm 1: Scrambling of pixels.

Table 1: Randomness measurement of the proposed method.

Statistical test	P value	Proportion
Frequency	0.98	0.99
Block frequency	0.73	1.00
Runs	0.96	0.99
Longest-run	0.62	0.99
Binary matrix run	0.98	0.99
FFT	0.54	0.99
Non-overlapping template	0.93	0.99
Overlapping template	0.87	0.99
Universal	0.99	0.99
Linear complexity	0.81	1.00
Serial	0.86	0.99
Approximate entropy	0.97	0.99
Cusum	0.64	0.99
Random excursions	0.95	0.99
Random excursions variant	0.96	0.99

Table 2: Correlation of adjacent pixels for a given image from SIBI dataset.

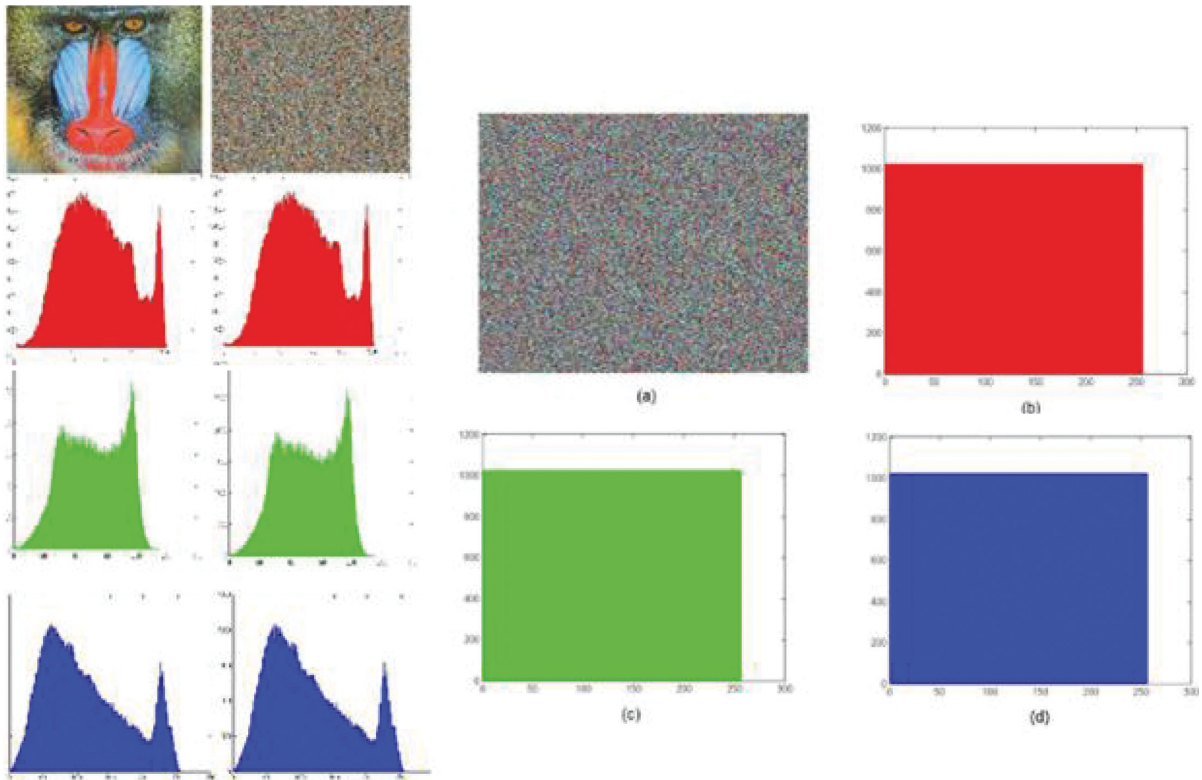| Image name	Image type	Size	Horizontal correlation	Vertical correlation	Diagonal correlation
Girl	RGB	256×256	0.9893	0.9688	0.9610
Tiffany	RGB	256×256	0.9426	0.9682	0.9945
Elaine	Grayscale	512×512	0.9519	0.9801	0.9724
Cameraman	Grayscale	256×256	0.9682	0.9583	0.8569
Lena	Grayscale	512×512	0.9785	0.9880	0.9855
Baboon	RGB	512×512	0.5119	0.6024	0.6876

FIGURE 11: Histogram of baboon image with their histogram after and before processing.

neighbour, which is small. This is the smooth area, while the difference increased when it reached the sharp area. Data in the table show that the smooth area in the image is greater than the sharp area. The last evaluation is based on the uniformity of the histogram. During encryption, data of the pixel value are still the same as changing will be on the position of pixels in the image. The histogram is rich in information about the image, and a powerful method is to try to decrease the peaks of the histogram to be uniform (a straight line), which was achieved in the proposed method as explained in Figure 11.

The proposed method achieved high results that will reflect the worth of the proposed method due to the aim of each study, which is to get high results. Maybe in the future, studies can reach perfect results in terms of encryption.

5. Conclusion

In this study, the process of encryption of an image using a random key and deep neural network is presented. The three random variables are the key space of randomness, logistic map, and the Henon map and contributed to the increase in the chaotic image. Encryption, in two terms, has been relied upon for changing the pixel location of the image and secondly the relationship between one pixel and its neighbours. The next pixel location selection is the responsibility of the deep neural network. This is done by using randomness as a feature, as well as the process of switching between columns and lines of the image. A histogram is used

as a perfect measurement for image cryptography, and its uniformity is evidence of the strength of the proposed method. The SIBI dataset is used for evaluating the proposed method via two types of images, grey and coloured images. The results achieved were satisfactory, and the reliability of the proposed method is proven by the efficiency of the system.

Data Availability

All data used to support the findings of this study are included within this article.

Conflicts of Interest

The authors confirm that there are no conflicts of interest regarding the study of this paper.

References

[1] M. A. Razzaq, R. Ahmed, M. Adnan, and A. Ahmed, "Digital image security: fusion of encryption, steganography and watermarking," *International Journal of Advanced Computer Science and Applications*, vol. 8, p. 5, 2017.

[2] S. Yadav and N. Tiwari, "Recent advancements in chaos-based image encryption techniques: a review," *Social Networking and Computational Intelligence*, Springer, Singapore, pp. 639–647, 2020.

[3] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework,"

Multiscale and Multidisciplinary Modeling, Experiments and Design, vol. 2, no. 4, pp. 233–248, 2019.

[4] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image encryption using Josephus problem and filtering diffusion," *IEEE Access*, vol. 7, pp. 8660–8674, 2019.

[5] N. Abdoun, S. El Assad, T. Manh Hoang, O. Deforges, R. Assaf, and M. Khalil, "Designing two secure keyed hash functions based on sponge construction and the chaotic neural network," *Entropy*, vol. 22, no. 9, p. 1012, 2020.

[6] Y. Liu, S. Liu, Y. Wang, H. Zhao, and S. Liu, "Video steganography: a review," *Neurocomputing*, vol. 335, pp. 238–250, 2019.

[7] O. Hosam, "Attacking image watermarking and steganography-a survey," *International Journal of Information Technology and Computer Science*, vol. 11, no. 3, pp. 23–37, 2019.

[8] S. R. Maniyath and V. Thanikaiselvan, "An efficient image encryption using deep neural network and chaotic map," *Microprocessors and Microsystems*, vol. 77, Article ID 103134, 2020.

[9] Y. Zhang, "The fast image encryption algorithm based on lifting scheme and chaos," *Information Sciences*, vol. 520, pp. 177–194, 2020.

[10] Y. Ding, "DeepEDN: a deep learning-based image encryption and decryption network for internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1504–1518, 2020.

[11] J. Chen, X.-W. Li, and Q.-H. Wang, "Deep learning for improving the robustness of image encryption," *IEEE Access*, vol. 7, pp. 181083–181091, 2019.

[12] W. Sirichotedumrong, Y. Kinoshita, and H. Kiya, "Pixel-based image encryption without key management for privacy-preserving deep neural networks," *IEEE Access*, vol. 7, pp. 177844–177855, 2019.

[13] W. Sirichotedumrong, T. Maekawa, Y. Kinoshita, and H. Kiya, "Privacy-Preserving deep neural networks with pixel-based image encryption considering data augmentation in the encrypted domain," in *Proceedings of the 2019 IEEE International Conference on Image Processing (ICIP)*, Taipei, Taiwan, September 2019.

[14] C. He, "A deep learning based attack for the chaos-based image encryption," p. 12245, 2019, https://arxiv.org/abs/1907.12245.

[15] P. G. Mante, H. R. Oswal, D. Swain, and D. Deshpande, "A symmetrical encryption technique for text encryption using randomized matrix based key generation," *Advances in Data Science and Management*, Springer, Singapore, pp. 137–148, 2020.

[16] Y. Wu, L. Zhang, T. Qian, X. Liu, and Q. Xie, "Content-adaptive image encryption with partial unwinding decomposition," *Signal Processing*, vol. 181, Article ID 107911, 2021.

[17] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 13841–13864, 2021.

[18] W. S. Sayed and A. G. Radwan, "Generalized switched synchronization and dependent image encryption using dynamically rotating fractional-order chaotic systems," *AEU-International Journal of Electronics and Communications*, vol. 123, Article ID 153268, 2020.

[19] C. He, T. Wu, C. Liu, and T. Chen, "A novel method of composite multiscale weighted permutation entropy and machine learning for fault complex system fault diagnosis," *Measurement*, vol. 158, Article ID 107748, 2020.

[20] Y. Hou, Z. Deng, and H. Cui, "Short-term traffic flow prediction with weather conditions: based on deep learning algorithms and data fusion," *Complexity*, vol. 2021, pp. 1–14, 2021.

[21] J. Wei, T. Ye, and Z. Zhang, "A machine learning approach to evaluate the performance of rural bank," *Complexity*, vol. 202110 pages, 2021.

[22] G. Sulong and A. Mohammedali, "Human activities recognition via features extraction from skeleton," *Journal of Theoretical and Applied Information Technology*, vol. 68, no. 3, 2014.

[23] H. Yang and X. Zhang, "Interactive multimodal television media adaptive visual communication based on clustering algorithm," *Complexity*, vol. 2020, pp. 1–9, 2020.

[24] G. Sulong and A. Mohammedali, "Recognition of human activities from still image using novel classifier," *Journal of Theoretical and Applied Information Technology*, vol. 71, no. 1, 2015.

[25] B. T. Atiyha, S. Aljabbar, A. Ali, and A. Jaber, "An improved cost estimation for unit commitment using back propagation algorithm," *Malaysian Journal of Fundamental and Applied Sciences*, vol. 15, no. 2, pp. 243–248, 2019.

[26] J. Fei and Y. Chen, "Fuzzy double hidden layer recurrent neural terminal sliding mode control of single-phase active power filter," *IEEE Transactions on Fuzzy Systems*, vol. 29, no. 10, pp. 3067–3081, 2020.

[27] V. K. Tanwar, B. Raman, A. S. Rajput, and R. Bhargava, "SecureDL: a privacy preserving deep learning model for image recognition over cloud," 2021.