

Research Article

Yasmine M. Khazaal*, Mohanaed Ajmi Falih, and Abbas Hamid Majeed

Design a new scheme for image security using a deep learning technique of hierarchical parameters

<https://doi.org/10.1515/eng-2024-0016>

received February 16, 2024; accepted March 17, 2024

Abstract: With the continued exponential growth of digital images, concerns about the security and confidentiality of visual data have increased. In this session, a new developed approach was presented for image security and confidentiality by taking advantage of deep learning (DL) technology and producing data hierarchies. Due to the development taking place in the field of images and the large circulation of them through modern applications, it has become necessary to maintain their security. DL technology was used to encrypt and decrypt images, and based on hierarchical variables to complicate the encryption process. Convolutional neural networks are used in automatic learning to extract hierarchical features from an image, and to ensure adaptability, the model is trained on a variety of images. In order to encrypt the image, multi-layered hierarchical processes are used, and there are layers added during the work for complexity and to thwart attacks. Manipulating the layers of the neural network in a hierarchical manner to benefit from the outputs of the layers in feedback reflects the importance of the contributions here. Likewise, scattering the columns and rows of the image in a descending or ascending manner increases the efficiency of the contribution in this study. The use of hierarchical parameters facilitates encryption and decryption for authorized users. The evaluation of the research was conducted using established picture metrics and compared to pre-existing encryption techniques. The experimental findings substantiated the efficacy of the proposed approach in upholding image security, with the inclusion

of hierarchical information further bolstering its ability to thwart attacks. Consequently, it emerges as a very promising strategy for ensuring image security. The proposed method is a significant advancement in creating an image security strategy using DL and a hierarchical variable creation process. The study provides a good and adaptable solution to evolving image security challenges in the digital age.

Keywords: deep learning, image encryption, hierarchical parameters, image security, histogram

1 Introduction

Despite the tremendous growth of digital images today and the many applications that use these images, the security and integrity of information security must be highlighted as a priority in the digital environment [1]. The various advances in image processing technology, which are spread through social media and data transmission processes, were either medical or any other field with an urgent need to maintain their security. This study presents a new image encryption system based on deep learning (DL), based on hierarchies of random values in encryption.

Traditional image encryption methods have relied, for a long time, on traditional encryption algorithms. The effectiveness of these algorithms has diminished over time and in the face of increasingly sophisticated cyber threats [2]. In response to this, our proposed scheme takes a serious step forward by harnessing one of the artificial intelligence (AI) algorithms, namely, DL algorithms, and it is considered a model that has proven unparalleled success in various tasks, especially for applications that rely on images such as recognition and analysis [3]. Many media are circulated on the Internet, and information is transmitted through or through them. Pictures have become one of the most important media nowadays, especially since the spread of social media. The security of images is a must, as it is the most important means of transferring

* **Corresponding author: Yasmine M. Khazaal**, Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad, Iraq, e-mail: yasmin.m.khazaal@aliraqia.edu.iq

Mohanaed Ajmi Falih: Directorate General of Education in Babylon, Hillah, Iraq, e-mail: mohanaedajmi@gmail.com

Abbas Hamid Majeed: Directorate General of Education in Babylon, Hillah, Iraq, e-mail: abbbham6@gmail.com

confidential data. Therefore, the security of images is the basic matter in our current study.

In our proposed approach lies the strategic integration of hierarchical parameters that are generated and derived from a deep neural network (DNN). These parameters depend on complex image features and analyze them at multiple levels of abstraction, starting from the lowest pixel level up to the semantic structure level. The hierarchical process leads to increased complexity in the encryption process and also enhances security by addressing features that are publicly visible. These features have one thing in common, which is to reveal an encrypted image that is very secure.

It is clear that DL plays an effective role in maintaining image security in various fields. Many applications include detecting forged and potentially tampered images. In addition to protecting copyrights in some cases, the process of revealing confidential information contained in the image, and in some cases diagnosing the image, leads to revealing a lot of information. DL helps hide the basic identity of images and the integrity and security of the information inside them, in addition to detecting potential attacks and verifying the authenticity of the digital content in the image. Through this, we see the importance of deep education in maintaining image security. For this reason, the researchers in the literature considers the image security in AI algorithms.

In our modern era, there has been a rapid increase in the transmission of digital images *via* the Internet. In this regard, the sender expects the transmission channel to be secure in transmission and free of any security threat that may occur to the image, but it is not possible to predict the reliability of the transmission [4]. The increase in automated education technologies has led to increased concerns about data security in various fields [5]. In terms of privacy, the world has become in need of protecting the security of its data, and the more data there is, the greater its security responsibility. Digital images contain large data, represented by data related to the juxtaposition of pixels. Traditional encryption techniques such as Data Encryption Standard and Advanced Encryption Standard (AES) are not suitable [5].

In order to protect the personal data of individuals passing through communication networks, many efforts have been made to find solutions that provide image security, and this protection is through many different techniques of encryption, shorthand, and image authentication. Recently, DL has played a vital role in this issue in terms of discovery and segmentation: images, style transfer, image reconstruction, and image compression [6]. Of all the above, image security using DL has captured the attention of

researchers and has achieved significant progress in this field.

Traditional encryption systems rely mainly on chaos, according to the known characteristics of encryption. Initially, the chaotic cryptosystem was first proposed by Matthews in 1989 [7]. After that, several designs for image encryption systems based on chaos [8,9] were proposed. Then, many techniques that depend on chaos and DNA coding were encrypted: wavelet transforms, *etc.* Encryption systems are a combination of propagation and switching rounds. The arrangements of pixel locations are arranged randomly, which is useful to avoid statistical attacks. In this case, the image is in the form of a scatter and does not contain any information, and then, the pixel values are modified using secret keys, which is the basis of the encryption process [10].

DL includes a lot of characteristics in its non-linear structure and its ability to learn [11]. Much effort has been made in the past to link DL to encryption, especially digital images. It is still in its infancy, which is why it encouraged researchers in this direction. This article summarizes some important works in the literature related to DL and image encryption systems and understanding their similarities. This study also describes the development of DL used in image encryption, summarizes a good portion of that research, compares the methods used, and mentions the pros and cons of each of the methods [12].

In this study, an image encryption system based on a new chaotic map using DL and key generation is proposed. Through a deep convolutional neural network (CNN), a public key for a new chaotic map was generated, and the new contributions of the proposed study can be confirmed as follows:

A new method for generating encryption keys using CNN has been proposed.

A new sequence of the chaotic map was proposed using hierarchical variables produced through a DNN.

2 Related work

Image security is extremely important in protecting images and not tampering with them except by authorized parties. Among the security systems is encryption, which is considered the basis for image security due to the sensitivity of images. Images enter a wide range of fields and applications, so researchers are interested in the security of this information. Images are important in the medical, military, and financial fields, so security measures must be taken, and this is what has been suggested in the literature to protect the security of digital images. Many techniques

have been used to maintain the security of images, including traditional methods, including statistical methods, and many algorithms proposed in the past, but among the most important of these methods are the methods that rely on AI and its algorithms, including DL algorithms.

Many researches have been proposed in the literature regarding DL and its role in image encryption. [13] They proposed a secure method for generating keys that has a relatively lower latency than its counterparts, and it worked well. They used variable methods to change the pixel value in the image and used Fibonacci to fool the hacker into the value inside the pixel [14]. A dynamic authentication method was proposed by Sathyadevan *et al.* [15], which adopted dynamic encryption and a precision measure in producing the security key. A combination of DNA sequencing and DL is used to generate an encryption key that increases the security of the process and also increases the chaos of the encrypted image [16]. Nonlinear systems such as chaotic systems have also been used to encode images using their unique computational properties, unpredictability, and randomness. In terms of key generation [17], a new seed generator was adopted based on the sensor and to increase the accuracy of the encryption, which allowed the combination of a hybrid graph and an algorithm that works to increase the chaos of the image. A very chaotic system based on beta functions was proposed, which was used to create a complete chaotic chain that mixes the locations of pixels in the image, leading to the loss of the relationship between the original image and the encoded image [18]. The Arnold chaotic sequence was also used to create the private encryption key and thus was used to encrypt the image, using the improved AES algorithm and the keys that were used to generate the chaotic system [19]. An algorithm has been proposed to stand up to brute force attacks, which works to generate random numbers to increase the complexity of encryption in the image and chaotic mapping, as the key that is generated with a large area helps in designing a very false environment [20]. A method based on repeated random generation controlled by a DL algorithm was proposed to find the best encryption key generation sequence [21]. The best algorithms use multiple patterns that are close to mathematical formulas, which produces an encrypted image that is complex but at the same time consuming time and computer resources [22].

2.1 Research gap

The research gap in determining the use of DL in maintaining data security is identifying previous techniques and areas where methodologies may be deficient and

need further development. One of these gaps is that DL is able to detect image security manipulation faster and more accurately, especially complex images that are vulnerable to attacks and forgery, which traditional methods may not be able to keep up with. In addition, DL has proven itself in many fields due to its ability to predict through training and testing, so it is worthwhile to develop a method to deal with image security. Another important gap is that DL is able to give more reliable and reliable results, especially when developing and hybridizing DL algorithms.

2.2 Image encryption with DL

Many techniques were used in traditional image encryption, including chaotic sequence techniques, which were used as a key to the encryption secret. The encryption system basically consists of changing the positions of pixels in the encrypted image as well as changing the value of the pixel as a numerical value [23]. Recently, AI techniques have been used, including DL technology, to encode images. According to Figure 1, the number of studies that considered DL in image encryption is estimated, from 2018 until 2023, and efforts are still continuing in this direction.

Encryption of the image is carried out by convolution of the regular image. The convolution kernel is updated through the chaotic sequences of a specific chaotic map, and this work does not require training for the encryption to be effective [24]. Confusion and diffusion process through which images are encoded by the permutation process, and the convolution kernel for the convolutional network is created and the sequence required for the scrambling process is obtained. Thus, the propagation process is carried out through XOR operation with chaotic sequences. Encryption, in general, consists of combination, switching, and diffusion. The large key space is one of the basics of the success of the encryption process [25]. The encrypted image is also

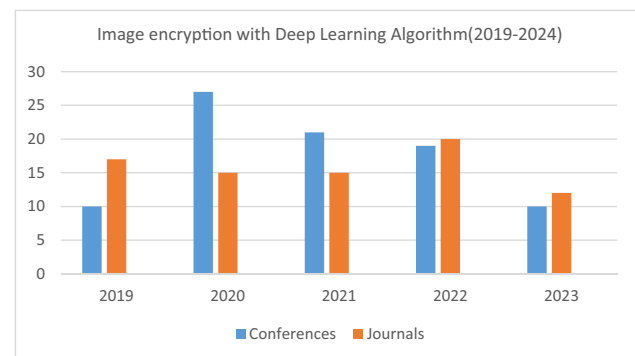


Figure 1: Publishing research in the literature.

Table 1: Most important studies in the literature

References	Method used	Advantage	Disadvantage
[26] 2020	Image encryption by cycle GAN	Improved GAN for encryption	Low diffusion issue
[27] 2019	Hiding information by steganography using GAN	Cover image transfer through communication	High-resolution image is needed
[28] 2021	Diffusion with GAN	Improved diffusion for encryption	Diffusion used only XOR operation
[29] 2022	DNN with weight over the DCT	No need for training just and nonlinear technique	Not robust and histogram is not uniform
[30] 2021	Use CNN in both diffusion and confusion	Useful for diffusion in encryption	Require two images to get encryption
[31] 2021	Key generating using DNN	Generate dynamic key	Not enough efficiency
[32] 2020	Using DNN and traditional techniques	Increase the security due to dynamic key	Weak decryption method need to improve
[33] 2018	DL technique for iris image	Stand against brute force attack	Weak in general
[34] 2022	Using chaotic sequence and deep auto encoder	Auto encoder to keep scrambling for secure image	Weak histogram uniform
[35]	Hybrid approach for DNN and attention-based recurrent neural network	Decrease the rate of misclassifications by resampling	Lake in big data management special for social media

obtained through discrete Fourier transform (DCT) operations, and in this type of encryption, chaotic operations are the main key in the encryption process. Encryption using DL sometimes requires a generative adversarial network (GAN) cycle to create an encryption key. For certain images, the key is private through a network and with the help of XORed with the original image. In this case, encryption is the best means of defense against brute force attacks. XOR operations are well known on bit locations of a single pixel and are often associated with DL algorithms. Table 1 summarizes the most important studies in the literature.

Encryption is an effective process for images and is considered highly secure, and there are AESs that are relied upon [36]. There is a reliable property in encryption, which is the property of pseudo-randomness, and the sensitivity of the initial value in the chaotic map as well as the interaction, and the chaotic maps are the sequences that generate the key for encryption. Many researchers have proposed methods for encrypting various types of images such as medical, military, and engineering. The main stages that image decryption goes through are the mixing stage and the masking stage. Chaotic maps are used to mix the components of the input image and thus hide them, and as for the mixing, it is carried out in new innovative ways for each approach and thus works to create a map that can only be solved by the encryption key.

2.3 DL

The progress in analyzing information and contemporary technology, including big data (high-quality image pixels),

satellite imaging, and powerful computing devices, has facilitated the development of algorithms that use machine learning (ML) to understand complex systems and their information patterns [27]. ML allows machines to acquire information through diverse means, while being limited by likely developers or constrained rules [28].

DL is a sort of ML that focuses on obtaining useful data out of images, audio, and texts. DL refers to a method that uses multiple layers to analyze complicated information and extract features, either with or without supervision. This allows for precise identification and classification of structures [29]. The discipline of AI greatly reduces the need for ML by imitating the human brain's ability to analyze, make decisions, and learn [30]. The goal of DL is to mimic the hierarchical learning mechanism of the brain of a person, which entails obtaining characteristics directly from unstructured data, such as raw photos. DL utilizes hierarchical features computing to represent information in the desired manner, including the progressive choice of characteristics from lowest to greater levels. ML is extensively utilized for multiple applications, such as encryption, where it excels in terms of its exceptional accuracy and speed in comparison with conventional methods of encryption. At first, DL techniques do not produce adequate outcomes as they necessitate a training period to encompass all the pixels in a picture, even in cases of high-resolution images where the pixels are scattered randomly. DL automatically extracts features by analyzing the associations between pixels in the image. This pertains to the DL technique and the specific attributes it depends on for encoding images. AI techniques are essential for the advancement of technology and are widely applied in several scientific domains, such as pattern recognition and

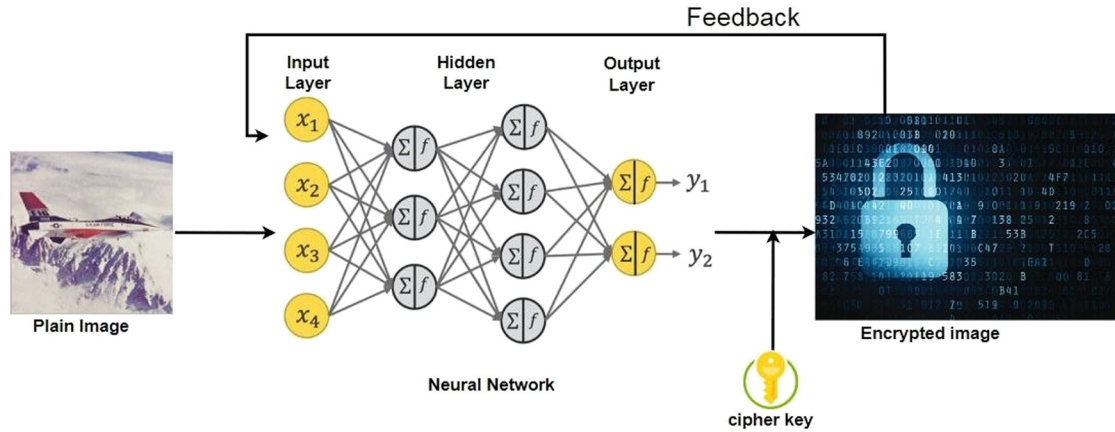


Figure 2: DL with encryption process.

computational power. The user's text is a reference to a specific range of numbers, specifically previous studies [37,38].

The precise representation of the image being input, used as a feature, is the basis for the efficient processing of image pixels, regardless of their amount. Both decryption and encryption entail distinct limitations. Therefore, DL approaches can be utilized to extract unique features that are used to overcome restrictions in many domains.

The primary distinction between ML and DL is in the approach to feature selection [38], as depicted in Figure 2.

To simulate appropriate results, features are automatically created in DL. Hidden layers help in making the right decisions by transferring information from a previous layer to a subsequent layer, but sometimes decisions are made based on information from the subsequent layer and returning data to the layer before it. So sometimes the previous layer is fed from the outputs of the next layer. This is what distinguishes DL and deducing immediate decisions. DL allows the computer to perform complex operations that require a large amount of time through simpler calculations to exploit the computer's efficiency. Understanding some complex data, such as correlations of pixels in an image, the confusion matrix, and the diffusion matrix, these concepts are difficult for a computer. This is why for using DL techniques, which improves encryption based on the randomization of image pixels. Completely predicting the proposed new randomly map for encryption is the basis for using DL [39].

3 Proposed method

In terms of image processing, the encryption process relies on a power key. There are some methods that use one key,

and there are methods that use two keys for encryption. In the suggested technique, two maps of chaotic were used, namely, sensitive logistic maps and Hannon map [40]. It is useful for increasing random chaos in system and for better standards. The behavior of the logistic map can be described by Equation (1) [16]:

$$X_{n+1} = rX_n(1 - X_n). \quad (1)$$

Consider $r \in (0.4)$ with $n = 1, 2, \dots, n$, where X_1 is the initial value such as $(0 < X_1 < 1)$. r is used for logistic function with a range around 3.5699 to 4. Then, Figure 3 shows the logistic behaviors such as $X_1 = 0.5$ and $r = 3.99$.

Henon map is the second chaotic map in the proposed method, which, in turn, increases the process of code complexity. The behavior of the Henon map can be explained as in the following equations [7]:

$$X_{n+1} = 1 - aX_n^2 + Y_n, \quad (2)$$

$$Y_{n+1} = bX_n. \quad (3)$$

where X and Y are the variables that represent the initial conditions, and $(a$ and $b)$ consider as control parameters used for cryptography. Chaotic events that are excellent for $a = 1.3$ and $b = 0.4$. This is because of Henon map that responds to these parameters.

The encrypted image is in the form of a random distribution of pixels and is noisy due to this distribution of pixels, and this is reflected in the useful information of the visual image. Therefore, removing noise from the image is necessary, whether this noise is artificial or caused by work. Noise considers unwanted data that is embedded to image in a certain way to affect the image quality. Images are exposed to several types of noise, including Gaussian noise, salt and pepper noise, anisotropic noise, and gunshots. The most famous type of noise is Gaussian noise, which has a significant impact on the encoded image

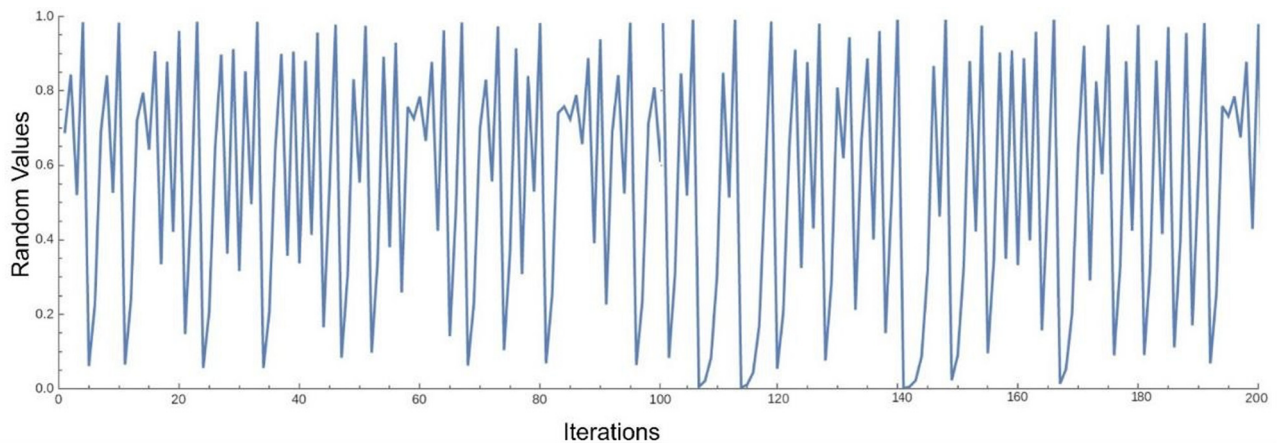


Figure 3: Logistic map behavior.

during the distribution of pixels. The Gaussian distribution can be described by the following Equation [7]:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}, \quad (4)$$

where σ and μ are considered standard deviations with averaging noise where $\mu = \text{Zero}$.

Image encryption technology contains two very important processes, which are the confusion process and the diffusion process. As shown in Figure 4, the image comes in the form given data and is followed by pre-processing in order to normalize the image, and then, it is prepared of confusion process.

One of the most important problems facing encryption in images is how to create a random key that scrambles the pixels of the image randomly. Changing the locations of the pixels leads to changing the visual image to a random image, but the information contained in the pixels does not change, and the change is only in the title. Changing the locations of pixels is a change in the pixel coordinates of the image, because the pixel density does not change in the random order of the image. The new arrangement of pixels in the image must save the locations in order for the recipient to rearrange to obtain the original image, which is stored in the encryption key.

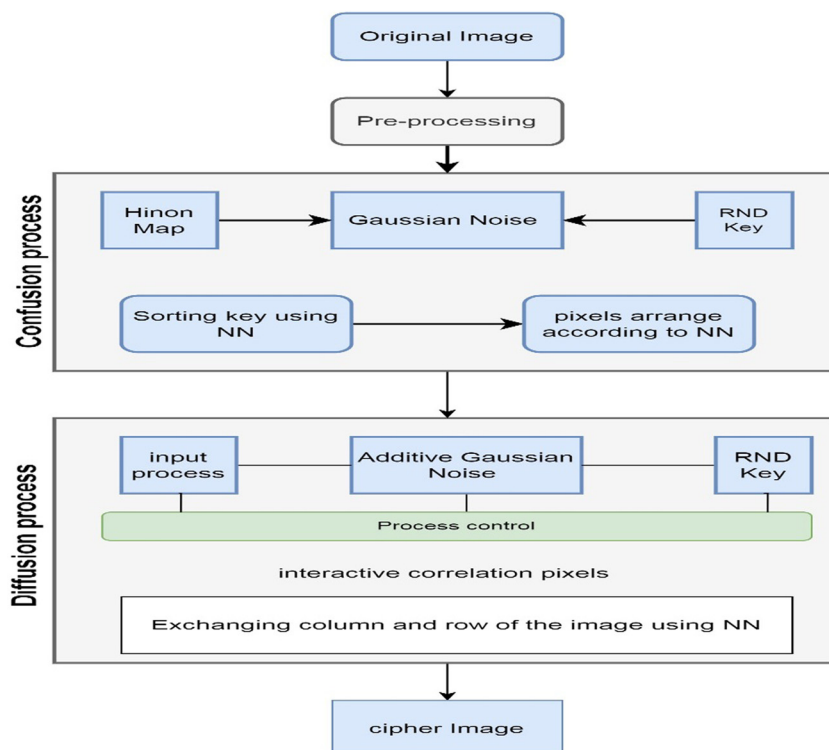


Figure 4: Main process in the encryption proposed method.

In DNN, the row and column are selected hierarchically from the original image. The column or row borders are chosen from the outside to the inside in a hierarchical manner, as the particular image is in the form of a decreasing border from the outer sides. The hidden layers are the ones that deduce which columns are to be replaced or which columns should be replaced. The changing values of the hidden layers, especially the layers that feedback from the later layers, have an impact on the encryption process, as shown in Figure 5.

The features come from choosing the column and the number of pixels that make up this column. At each reduction, it stores the number of pixels of the decrease in one vector and repeats the process until the number of pixels reaches half. The hidden layer plays a role in choosing the number of pixels and the length of the column, and the training process plays a role in the possibility of choosing the sections of the column and the amount of part that will be replaced with the corresponding column. The complexities of choosing a column or choosing a line using the same principle are complicated at first, but during the training process, they become better and simpler. The neural network is fed the coordinates of the pixels (X, Y) of the columns and lines, and thus, the coordinates are chosen in the advanced stages.

The pixel coordinator enters a random function to be updated by a DNN. Through training, the coordinates of the pixels in the image are updated. The predictions produced by the hidden layer increase in complexity with each training session, and then, the randomness of the image increases. The pixels that are replaced are compatible with the replacement between the line and the column, as shown in Figure 6.

The main purpose of changing the position of all pixels in the image is to encrypt, change the sequence and confuse the intruder. Repositioning the image using coordinates shows the values stay constant, which is critical for decoding. Confusion is a technique that relies on the logistic map to shift or change pixel coordinates, disentangling old pixel associations and creating new ones. Changing position is necessary to stand against statistical attack. This is one of the benefits of applying DL and feedback algorithms to find new coordinates for image pixels through the horizontal and vertical hierarchical formation of the image. The strength of the proposed algorithm can be detected by solving the following equations:

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

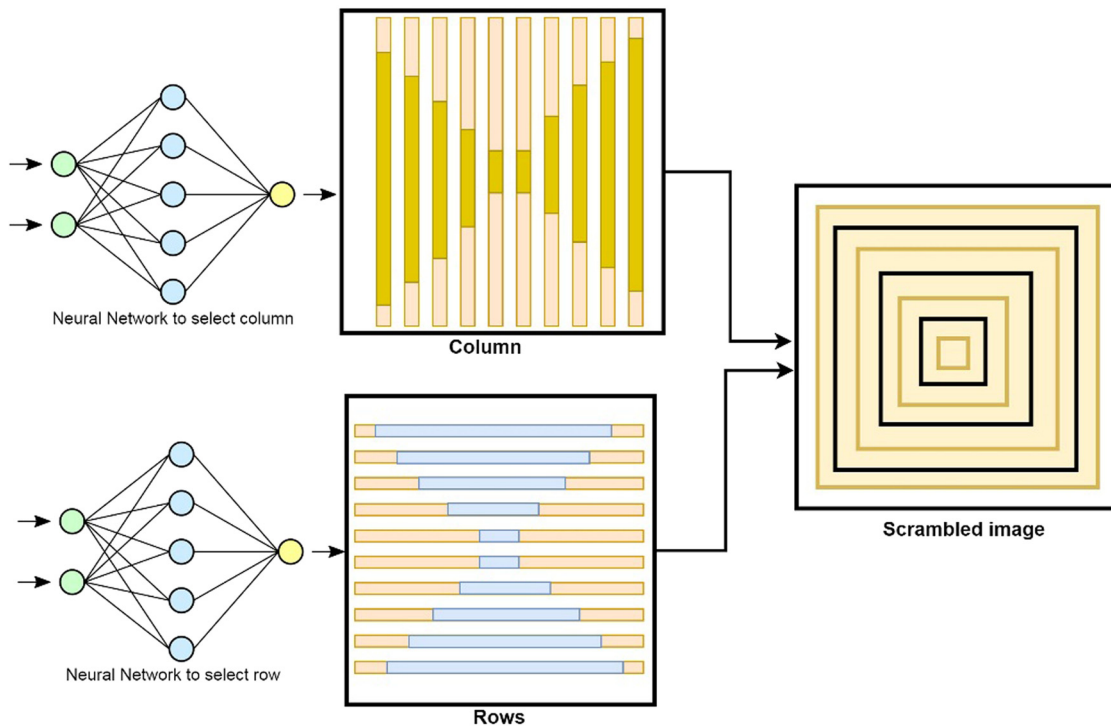


Figure 5: DNN with hierarchical selection.

1,1 0.23	1,2 0.54	1,3 0.72	1,4 0.37
2,1 0.53	2,2 0.45	2,3 0.82	2,4 0.79
3,1 0.54	3,2 0.87	3,3 0.47	3,4 0.56
4,1 0.47	4,2 0.61	4,3 0.65	4,4 0.73

Original Image

4,4 0.73	1,2 0.54	1,3 0.72	1,4 0.37
2,1 0.53	2,2 0.45	4,1 0.47	2,4 0.79
3,1 0.54	3,2 0.87	3,3 0.47	3,4 0.56
2,3 0.82	4,2 0.61	4,3 0.65	1,1 0.23

encrypted Image

Figure 6: Encryption by scrambling.

where $D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - x')^2$ for horizontal correlation, $D(y) = \frac{1}{N} \sum_{i=1}^N (y_i - y')^2$ for vertical correlation, and $\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - x')(y_i - y')$ for diagonal representation.

These equations test the correlations of pixels in the image based on their horizontal, vertical, and diagonal neighbors. This test aims at the encrypted image whose features are unknown, and the other complementary test is the relationship between the encrypted image and the original plain image, which is what the following improved equations do:

$$\bar{A} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N A_{ij}, \quad (6)$$

$$\bar{B} = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N B_{ij}, \quad (7)$$

$$CC = \frac{\sum_{i=1}^M \sum_{j=1}^N (A_{ij} - \bar{A})(B_{ij} - \bar{B})}{\sqrt{\left(\sum_{i=1}^M \sum_{j=1}^N (A_{ij} - \bar{A})^2 \right) \left(\sum_{i=1}^M \sum_{j=1}^N (B_{ij} - \bar{B})^2 \right)}}, \quad (8)$$

where A is the plain image (original) and B is the ciphered image (encrypted) that share dimensions both N and M , and CC is the difference between them, which gives the strength of encryption.

All the parameters that are related to feedback within iterations and weighted variables are generated due to improvement in the DL technique in addition to vectors

through scrambling, while standard parameters such as pixels and for random techniques are fixed and come from used techniques.

4 Experimental results

Image encryption is an important and sensitive topic in which many criteria and evaluation methods can be used. This study will address a set of criteria that are considered the most important for evaluating the proposed method. The important evaluation here is the standing against attacks, randomness, and correlations in the image, whether between pixels or the image as a whole. First, we must know that encryption is the process of hiding information in a way that can only be solved by the encryption key, which contains the method for returning the image. The encrypted image is transmitted from the sender who encrypted it to the recipient who will decrypt it. Encryption and decryption are two methods, one opposite to the other. The work sequence is shown in Figure 7.

The encryption process consists of several stages. The plain image is prepared to change its information using the encryption key, after which the components of the image are changed in a random sequence, and it becomes an encrypted (cipher) image. It is then sent to the last

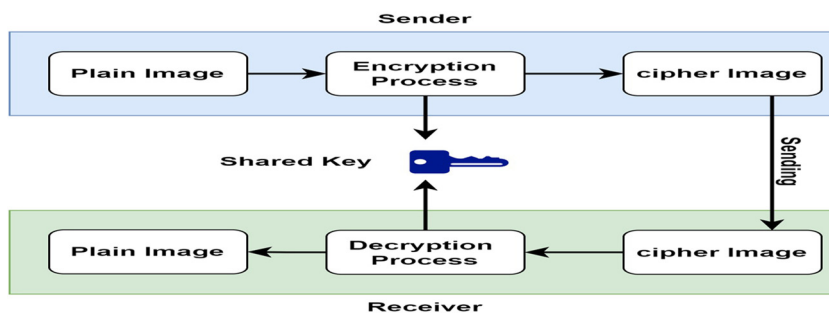


Figure 7: Encryption strategies through network.



Figure 8: Difference between original and encrypted images.

receiving side, so that the reverse process takes place by rearranging the image components according to the encryption key, thus producing the original (plain) image without losing its important information. Figure 8 shows the difference between plain image and encrypted image (cipher) that are difficult to recognize that contains it.

The image after encryption is missing features due to the pixels in the image being randomly distributed and thus changing the spatial pixel values. Among these distributions is randomness, which is important to measure the amount of randomness of the distribution of pixels, which distinguishes one method from the other. According to the logistic map, the random function proposed here, as well as Henon map, is the one that gives complex randomness in the image and is difficult to guess, as well as the white Gaussian noise, which can also be measured. The randomness evaluation is illustrated in Table 2.

Here, the p -value with s -value reflects the randomness and the power of encryption that are effected by processing in the proposed method. The achieved results come from the method that used the three types of randomness in additional key space of it. One of the most important evaluations in this study is the correlation of pixels in a single image. When implementing the program, the collision equation and the randomness of the hierarchical

random distribution are studied through columns and lines. More than 5,000 pixels are subjected to a random equation, and through the DNN in the number of iterations during training, the three correlations are analyzed. The SIPI database provides a good environment for measurement because it is used by many researchers to be a good standard for benchmarking, as shown in Table 3.

The strength of the correlation varies from one pixel to another and also according to the value. It is not possible for a correlation to be weak horizontally and at the same time strong vertically. Therefore, the homogeneity and strength of the link is evidence that the encrypted image is good and undetectable. The correlation is greater in images with a soft nature, as well as for areas with high color frequencies and edges. The evaluation can also be based on the histogram and a measure of the number of pixels in the image along with the color intensity of each pixel. The histogram is often rich in useful information about the image, and the peaks on the graph provide distinct and clear information. In order to hide information, the histogram must be in the form of a straight line. This reflects the strength of the encryption method, as shown in Figure 9.

Through evaluations and practical results of the proposed method, the merit of the proposed method can be proven, given the goal of each study is to obtain good results. It is possible that it will achieve more ideal results in the future to encrypt images with a high degree of security.





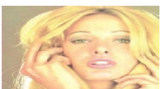

The main problem facing encryption or data security, in general, is how to ensure that the image is secure and protects against attacks. This basis lies with the encryption process and the amount of randomness in the encrypted image, which is the basis of the strength of the encryption method. The proposed method proved its worth because DL helped in randomly selecting pixels in the image, which increases the complexity of the method.

DL is one of the AI algorithms that relies on prediction at work, and this issue may be useful in the process of encrypting images and maintaining their security. Choosing the locations of pixels or areas in the image that are more changeable than others is performed through strong randomness predicted by the algorithm in order to increase the complexity of the random process in the image. In previous studies, the influencing element in the image was neglected. If it changes, what does it affect and the sequence of the subsequent effect of any pixel in the image? The hierarchical sequential effect of the change in the image cannot be calculated except through DL, which predicts the good result, thus moving to another level of work, and so on.

Table 2: Randomness evaluation

Statistic evaluation	p -value	s -value
Runs	0.92	0.96
B-matrix	0.95	0.98
Longest run	0.72	0.89
Frequency	0.96	0.98
FFT	0.59	0.86
Linear complexity	0.85	0.99
Entropy	0.96	0.99
Random excursions	0.96	0.99
Random variant	0.95	0.98

Table 3: Correlation of images with the proposed method

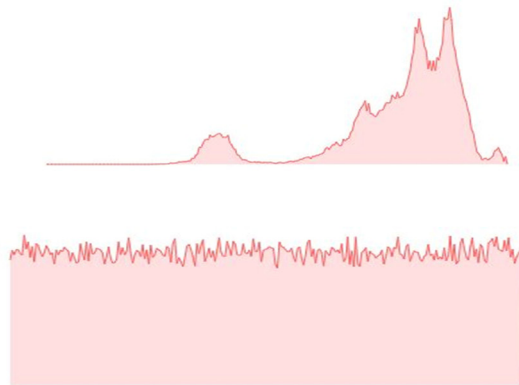
Images	Image type	Image size	Correlation		
			Vertical	Horizontal	Diagonal
	RGB	512 × 512	0.962	0.951	0.921
	Grayscale	512 × 512	0.932	0.978	0.937
	RGB	1,200 × 110	0.893	0.887	0.897
	RGB	512 × 512	0.932	0.936	0.976
	RGB	1,200 × 110	0.973	0.978	0.938
	Grayscale	512 × 512	0.872	0.886	0.871



Plain Image



cipher Image

**Figure 9:** Plain and cipher images with corresponding histogram.

5 Conclusion

The image encryption process was presented in this study using a random key and a DNN. The goal of encryption is to increase the randomness of the logistic map and the Henon map, which effectively contributes to increasing the chaos of the image. The encryption process, in general, depends on two terms: changing the location of a pixel and the relationship between the pixel and its neighbors. The random selection of pixels comes from a neural network prediction, and this is used in the process of switching columns and rows hierarchically and sequentially according to

the encryption key. The histogram, the strength of the correlation, and the degree of randomness were chosen to evaluate the work, and a standard dataset was used. The results were satisfactory, and the reliability of the proposed method was adopted to increase the system's efficiency.

Due to the development in data security, encryption methods are very useful in various fields, such as the military and medical fields, where encryption is performed to prevent image manipulation, and in the financial and correspondence fields. The work can be developed in a more professional manner based on the proposed method, which is the basis for any future work by researchers in

the field of data security, especially images. Since the development in the field of information technology and digital images can extend the work with the contribution made to an extent that can guarantee the safety of the image against attacks, researchers move to developing the work, on the other hand, and not stopping at attacks and intrusion on the security of images.

Funding information: Authors state no funding involved.

Author contributions: All authors have accepted responsibility for the entire content of this manuscript and consented to its submission to the journal, reviewed all the results and approved the final version of the manuscript. YMK and MAF designed the model and the computational framework, and analyzed the data. YMK and AHM carried out the implementation, worked out almost all of the technical details and performed the numerical calculations for the suggested experiment. YMK performed the calculations. YMK and MAF wrote the manuscript with input from all authors, devised the project, the main conceptual ideas, and proof outline. YMK and AHM conceived the study and were in charge of overall direction and planning. MAF assisted measurements with AHM that helped to carry out the simulations. All authors discussed the results, contributed to the design, implementation of the research, to the analysis of the results, and to the writing of the manuscript.

Conflict of interest: The authors state no conflict of interest.

Data availability statement: Most datasets generated and analyzed in this study are comprised in this submitted manuscript. The other datasets are available on reasonable request from the corresponding author with the attached information.

References

- [1] Korać D, Boris D, Dejan S. A model of digital identity for better information security in e-learning systems. *J Supercomput.* 2022;78:1–30.
- [2] Fadziso T, Thaduri UR, Dekkati S, Ballamudi VK, Desamsetti H. Evolution of the cyber security threat: an overview of the scale of cyber threat. *Digit Sustain Rev.* 2023;3(1):1–2.
- [3] Gupta N, Gupta SK, Pathak RK, Jain V, Rashidi P, Suri JS. Human activity recognition in artificial intelligence framework: A narrative review. *Artif Intell Rev.* 2022 Aug;55(6):4755–808.
- [4] Roman'kov V. Multi-recipient and threshold encryption based on hidden multipliers. *J Groups Complexity Cryptol.* 2023 Mar;14:1–12.
- [5] Sood R, Harpreet K. A literature review on RSA, DES and AES encryption algorithms. *Emerg Trends Eng Manag.* 2023;10:57–63.
- [6] Fadhil AM, Jalo HN, Mohammad OF. Improved security of a deep learning-based steganography system with imperceptibility preservation. *Int J Electr Comput Eng Syst.* 2023;14(1):73–81.
- [7] Panwar K, Kukreja S, Singh A, Singh KK. Towards deep learning for efficient image encryption. *Procedia Comput Sci.* 2023 Jan;218:644–50.
- [8] Zolfaghari B, Koshiba T. Chaotic image encryption: state-of-the-art, ecosystem, and future roadmap. *Appl Syst Innov.* 2022;5(3):57.
- [9] Zia U, McCartney M, Scotney B, Martinez J, AbuTair M, Memon J, et al. Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. *Int J Inf Secur.* 2022 Aug;21(4):917–35.
- [10] Benaissi S, Noureddine Chikouche RH. A novel image encryption algorithm based on hybrid chaotic maps using a key image. *Optik.* 2023;272:170316.
- [11] Kim J, Kim T, Love D, Brinton C. Robust non-linear feedback coding via power-constrained deep learning. *arXiv preprint arXiv:2304.13178;* 2023 Apr.
- [12] Abed NK, Shahzad A, Mohammedali A. An improve service quality of mobile banking using deep learning method for customer satisfaction. *AIP Conference Proceedings.* Vol. 2746, No. 1. AIP Publishing; 2023.
- [13] Zhou M, Wang C. A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. *Signal Process.* 2020;171:107484.
- [14] Mohamed K. Dynamic S-boxes and spiral permutation function on Fibonacci sequence for secure block cipher. Diss. Shah Alam, Malaysia: Universiti Teknologi MARA (UiTM); 2022.
- [15] Sathyadevan S, Achuthan K, Doss R, Pan L. Protean authentication scheme—a time-bound dynamic KeyGen authentication technique for IoT edge nodes in outdoor deployments. *IEEE Access.* 2019 Jul;7:92419–35.
- [16] Elizalde-Canales FA, Rivas-Camero ID, Rebolledo-Herrera LF, Camacho-Bello CJ. Pseudo-random bit generator using chaotic seed for cryptographic algorithm in data protection of electric power consumption. *Int J Electr Comput Eng.* 2019 Apr;9(2):1399.
- [17] Chang H, Wang E, Liu J. Research on image encryption based on fractional seed chaos generator and fractal theory. *Fractal Fract.* 2023;7(3):221.
- [18] Erkan U, Toktas A, Toktas F, Alenezi F. 2D er-map for image encryption. *Inf Sci.* 2022 Apr;589:770–89.
- [19] Lin CH, Hu GH, Chan CY, Yan JJ. Chaos-based synchronized dynamic keys and their application to image encryption with an improved AES algorithm. *Appl Sci.* 2021 Feb;11(3):1329.
- [20] Audhkhasi R, Povinelli ML. Generalized multi-channel scheme for secure image encryption. *Sci Rep.* 2021;11(1):22669.
- [21] Harlianto PA, Adji TB, Setiawan NA. Dislocated time sequences—deep neural network for broken bearing diagnosis. *Open Eng.* 2023 Mar;13(1):20220402.
- [22] Reddy MI, Siva Kumar AP. A modified advanced encryption standard algorithm. *J Mech Continua Math Sci.* 2020;1:112–117.
- [23] Zhou J, Li J, Di X. A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position. *IEEE Access.* 2020;8:122210–122228.
- [24] Praveen SP, Suntharam VS, Ravi S, Harita U, Thatha VN, Swapna D. A novel dual confusion and diffusion approach for grey image encryption using multiple chaotic maps. *Int J Adv Comput Sci Appl.* 2023;14(8):971.

- [25] Kaur M, Kumar V. A comprehensive review on image encryption techniques. *Arch Comput Methods Eng.* 2020;27:15–43.
- [26] Ding Y, Wu G, Chen D, Zhang N, Gong L, Cao M, et al. DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. *IEEE Internet Things J.* 2020 Jul;8(3):1504–18.
- [27] Zheng Z, Liu H, Yu Z, Zheng H, Wu Y, Yang Y, et al. Encryptgan: Image steganography with domain transform. *arXiv preprint arXiv:1905.11582*; 2019 May.
- [28] Zhenjie B, Xue R. Research on the avalanche effect of image encryption based on the Cycle-GAN. *Appl Opt.* 2021;60(18):5320–34.
- [29] Wang C, Zhang Y. A novel image encryption algorithm with deep neural network. *Signal Process.* 2022;196:108536.
- [30] Man Z, Li J, Di X, Sheng Y, Liu Z. Double image encryption algorithm based on neural network and chaos. *Chaos Solitons Fractals.* 2021 Nov;152:111318.
- [31] Ding Y, Tan F, Qin Z, Cao M, Choo KK, Qin Z. DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption. *IEEE Trans Neural Network Learn Syst.* 2021 Mar;33(9):4915–29.
- [32] Maniyath SR, Thanikaiselvan V. An efficient image encryption using deep neural network and chaotic map. *Microprocess Microsyst.* 2020;77:103134.
- [33] Kamil WF, Mohammed IJ. Deep learning model for intrusion detection system utilizing convolution neural network. *Open Eng.* 2023 Aug;13(1):20220403.
- [34] Sang Y, Sang J, Alam MS. Image encryption based on logistic chaotic systems and deep autoencoder. *Pattern Recognit Lett.* 2022;153:59–66.
- [35] Kuang M, Safa R, Edalatpanah SA, Keyser RS. A hybrid deep learning approach for sentiment analysis in product reviews. *Facta Univ Series: Mech Eng.* 2023 Oct;21(3):479–500.
- [36] Altigani A, Hasan S, Barry B, Naserelden S, Elsadig MA, Elshoush HT. A polymorphic advanced encryption standard—a novel approach. *IEEE Access.* 2021 Jan;9:20191–207.
- [37] Sulong G, Mohammedali A. Human activities recognition via features extraction from skeleton. *J Theor & Appl Inf Technol.* 2014;68:3.
- [38] Atiyha BT, Aljabbar S, Ali A, Jaber A. An improved cost estimation for unit commitment using back propagation algorithm. *Malays J Fundam Appl Sci.* 2019 Apr;15(2):243–8.
- [39] Sulong G, Mohammedali A. Recognition of human activities from still image using novel classifier. *J Theor Appl Inf Technol.* 2015;71:1.
- [40] Zamfirache IA, Precup RE, Petriu EM. Q-learning, policy iteration and actor-critic reinforcement learning combined with metaheuristic algorithms in servo system control. *Facta Univ Series: Mech Eng.* 2023 Dec;21(4):615–30.