IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 June 2024, accepted 18 July 2024, date of publication 23 July 2024, date of current version 23 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3432786

RESEARCH ARTICLE

Smart Pixels: Harnessing Deep Learning and Fibonacci Decomposition for Image Ciphering

YASMINE M. KHAZAAL[1,2,3], **ALI DOUIK**[3], **AND MONJI KHERALLAH**[4]
[1]National Engineering School of Sfax, University of Sfax, Sfax 3029, Tunisia
[2]Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad 7366, Iraq
[3]NOCCS Laboratory, National Engineering School of Sousse (ENISo), University of Sousse, Sousse 4000, Tunisia
[4]ATES-Laboratory, Faculty of Sciences of Sfax, University of Sfax, Sfax 3029, Tunisia

Corresponding author: Yasmine M. Khazaal (yasmine-mustafa-khazaal.al-tameemi@enis.tn)

ABSTRACT Due to the rapid and continuous growth of images in the digital environment, There are still concerns about the security and confidentiality of visual data. In this study, we will present a new, developed approach to securing digital images and maintaining their security by taking advantage of deep learning technology and Fibonacci decomposition. We used a deep neural network to generate random numbers, predict the optimal pixel position in the encrypted image, and apply Fibonacci decomposition to alter the pixel value (contrast). We trained the model on multiple images from a standard dataset to enhance its adaptability. The hidden layers in the neural network contributed to increasing the complexity of the generated numbers' randomness. The encryption key stores the method and functions of the encrypted image, enabling the recipient to decrypt it. We evaluated the research using the standard criteria from previous studies to compare the results. Deep learning helped prevent attacks, and Fibonacci analysis helped increase the image's security. This makes the proposed method a promising solution for digital image security. This study provides a promising solution that is adaptable to various types of images in the age of digital images.

INDEX TERMS Image encryption, deep learning, image security, Fibonacci decomposition, neural network.

I. INTRODUCTION

Image encryption is one of the types of classifications concerned with image security. In the digital computer world, security is considered a necessary priority and the most important issue. We classify security in digital images into three types: steganography, watermarking, and encryption [1]. In the realm of image processing, applications that manage digital images play a crucial role in various applications related to security, with physical and digital security being closely intertwined in various applications such as surveillance and identity verification [2]. This is why modern applications, particularly those in the field of artificial intelligence, such as deep learning and neural network algorithms, play a crucial role in predicting future treatments. The steganography technique hides information in an imperceptible and noticeable way, but the encryption process is a challenge, and the information cannot be extracted except through the secret key agreed upon between the two parties [3]. For the sake of information security, confidential information must not fall into the wrong hands, so that the matter does not become public. Image is considered one of the most important media for encryption due to its ease of handling and increased reliability. Images are a crucial consideration in the rapid development of information security and technology. Images are more common and widespread on the Internet, making them more vulnerable to hacking and manipulation of the information they contain. The image in general consists of a group of cells called pixels. Each pixel is composed of a color, density, and fixed location, and each pixel has a relationship with the remaining adjacent pixels [4].

The associate editor coordinating the review of this manuscript and approving it for publication was Jun Wang.

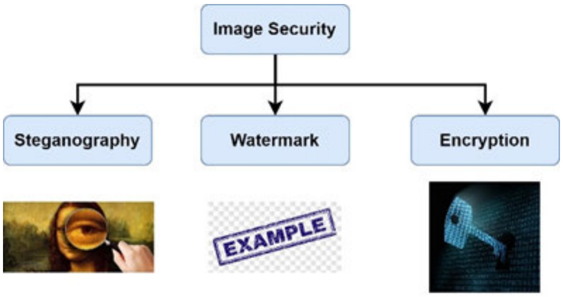


FIGURE 1. **Types of image security.**

During the past two decades, interest has been paid to chaos-based cryptography, and more and more researchers have focused on the basic properties of chaos and the sensitivity to the initial conditions that affect it [5]. Many studies focused on chaotic cryptography, which began in 1998 and involved the use of a neural network to control the hidden layers in it. The neural network always distributes information in a non-linear manner on the corpora, and through unsupervised learning, it produces a large number of extracted features, including many sub-features [6]. These features frequently aid in the encryption of digital images, which is the focus of our research. In image security technology, there are three types of image security. First, steganography, which aims to hide the secret inside an image in a way that it cannot be seen and is completely hidden [7], Secondly, the watermark is considered a method of hiding secret data inside the center of the image, in a way that increases incomprehension, and in such a way that the hidden information is completely invisible in the first and second types (steganography and watermark) [8]. The last and third type is image encryption, which itself is considered data, and the confidentiality in this case will be with the image, and it will be difficult to decrypt and a huge challenge. As depicted in Fig. 1. We use one or two chaotic sequences to encrypt the image. When employing a neural network, the chaotic sequence transforms into a sequence that relies on the neural network's structure and the quantity of hidden layers within it. Consequently, we employ the independent method to identify an appropriate chaotic sequence. The variables within the sequence equation are responsible for the complexity of the encrypted image. Modern methods use multiple variables to create a matrix, which is then binary-mixed to form a unique mixing matrix [9]. This matrix is responsible for changing the locations of the pixels in the encrypted image. A specific algorithm produces the encrypted image and sends it to the other party, but only the encryption key can decrypt it [10].

The random distribution of pixels within the image is what reflects the amount of chaos in the image, thus changing the locations of the pixels within the image, whose original arrangement cannot be restored except through the encryption key that contains information about the extent of the image's randomness. The encryption key changes and stores the correlation of pixels in the image, fulfilling its intended purpose. A robust and dependable random function generates the key [11]. The confusion process is the way through which the encryption process in images is accurately described and is reflected in the integrity of the image. The encryption method plays a crucial role in the encryption key's significance, as it handles both encryption and decryption, making its security paramount [12]. Both the sender and the recipient use the cipher key, which needs to be strong to prevent loss during or after the connection.

The contribution of this manuscript is to increase the security of the image by increasing the complexity of the distribution of pixels in the encrypted image and using several methods, including deep learning and generating more random numbers, in addition to manipulating the value of the pixels (contrast) by converting them to the Fibonacci decomposition. Increasing the randomness in the proposed method will increase the complexity of the encrypted image and reveal it as almost impossible.

The manuscript follows a structured format: an introduction establishes the work's principle and clarifies the overall concept, followed by a review of prior research in the literature to understand the fundamentals, pinpoint the primary issues of the subject, and devise solutions. A section delves into the intricacies of deep learning and provides a definition of the term. This is followed by a section that outlines the proposed method, including the specifics of its operation and the general algorithm. Next, a section dedicated to the results discusses the results and evaluations of the proposed method. The last section is the conclusion section, which mentions the conclusions reached in this manuscript.

II. RELATED WORK

Due to the widespread use of images in our time and the importance of encryption, especially the use of deep learning to solve its problems, a lot of research has been presented in the literature, including encryption of medical images and mechanisms for working on them using [13]. Medical staff used the Internet of Medical Things (IoMT) to build an integrated picture of the human body, facilitating treatment [14]. A deep convolutional neural network processes 2D and 3D optical images, contributing to rapid coding [15]. The study [16] discussed the importance of encryption keys and how deep neural networks use them to encrypt images. The study [17] employed deep learning to encrypt large-scale, high-resolution images, manipulate pixels, and intelligently divide a single pixel into multiple parts for storage in the encryption key. We employed deep learning to construct a chaotic encrypted image, leveraging previously extracted features from the image and forecasting pixel behavior during the encryption process [18]. Numerous studies have explored the function of deep learning in image encryption, encompassing key generation techniques that influence the intricacy of image encryption according to the pixel's role [19]. Researchers employed various techniques to alter the pixel value, thereby altering the image's

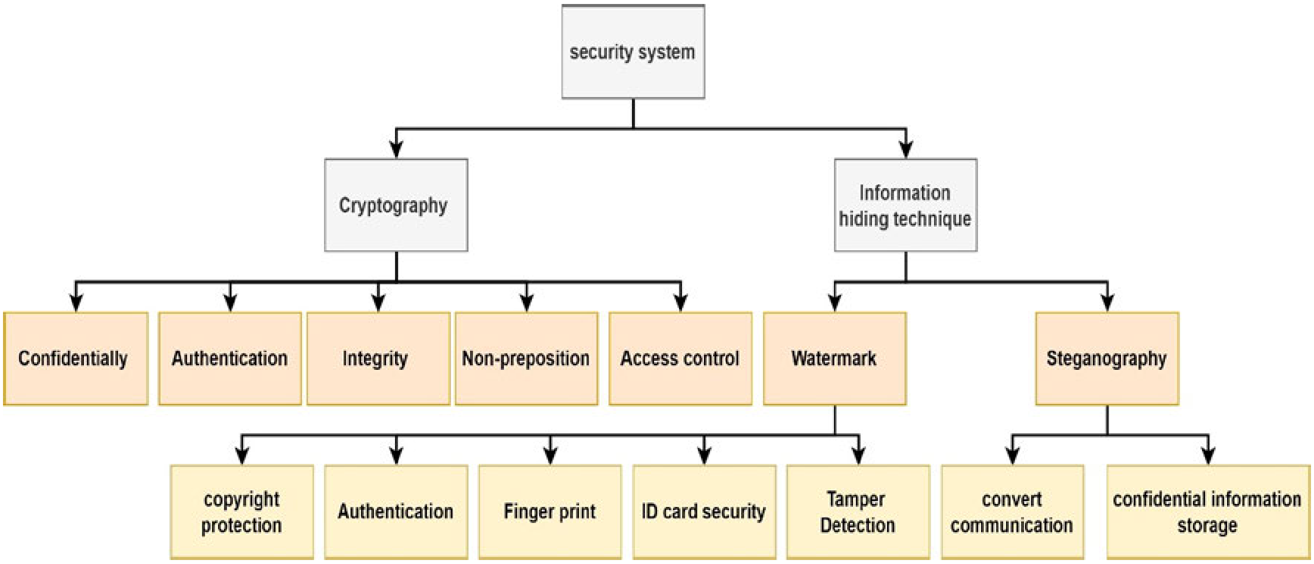


FIGURE 2. Types of image security.

content, and also transformed the pixel's value from binary to Fibonacci [20]. Proposed dynamic encryption, which evaluates the encryption key's accuracy to safeguard the encrypted image from potential attacks [21]. Deep learning has adopted and developed chaos management, the fundamental component of cryptography [22]. Cryptography employs a variety of systems, such as non-linear and chaotic systems, that utilize computational, random, and prediction properties [23]. To improve encryption accuracy, we generate keys in two ways: the first key, which establishes initial randomness, and the second key, which changes according to the leadership of the pixels and their distribution in the image. We propose a chaotic system based on the harmonic graph, which generates a random chaotic series for the screen's pixel distribution. The chaotic Arnold sequence, one of the sequences used in image encryption, relies on weakening the relationship between the original image and the encrypted image by generating a complex key that scatters the pixels' locations. One of the goals of the methods used in encryption is to prepare the image to be resistant to brute-force attacks, using chaotic maps that create the image in a complex manner [24]. In the past, there have been numerous attempts to transform a plain image into an encrypted one that can conceal the information it contains during the transfer process from sender to recipient. Because encryption is one of the branches of data security, the image must maintain the security of the data in it [25]. Confidentiality standards dictate that only authorized individuals can access the image's contents and view its information, thereby ensuring privacy. Much research has focused on the safety of information in images [26] and suggests ways to preserve privacy. Much research has proven that it is impossible to change the contents of an encrypted image by any means other than knowing the encryption key [27]. Some researchers focused their attention on the space key, striving to increase its complexity to prevent hacking through various methods such as statistical methods, artificial intelligence, and calculations [28]. Many researchers took into consideration the relationships between a single pixel and its neighbors and worked to complicate that correlation to protect against attacks on the image [29]. The most important research focuses on enhancing the image's randomness by developing the Henon map and increasing the complexity of generating the initial codes for the image [30]. Strong security systems must protect multimedia files, including text, images, and video, as they are more vulnerable to attacks. We can divide these security systems into two categories: data hiding and encryption. Steganography and watermarking, two types of data hiding, conceal information inside the cover media, while cryptography encodes the data. The design method, as shown in Fig. 2, is what distinguishes these systems.

A. PROBLEM STATEMENTS

We produce traditional encrypted images using high-level, high-security methods. However, there are still unresolved problems related to image encryption. Creating a random key that can both encrypt and decrypt is a crucial issue [31]. The random key controls the distribution of pixels in the image using a random number generator, which must be unique and difficult to predict. This helps avoid statistical attacks and ensures that the function responsible for generating random numbers is strong and unchangeable in any way [32]. The correlation and distribution of pixels within an image reflect the strength of good coding. The intricate arrangement of pixels enhances the image's correlation, while incorporating randomness into the distribution of pixels is beneficial. The complex change in pixels' position makes it possible to stand against attacks of various kinds [10].

TABLE 1. Most important studies in literature.

Authors	Method used	Advantage	Disadvantage
[33] 2021	Image encryption by cycle GAN	Improved GAN for encryption	Low diffusion issue
[34] 2019	Hiding information by steganography using GAN	Cover image transfer through communication	High image resolution is needed
[35] 2021	Diffusion with GAN	Improved diffusion for encryption	Diffusion used only XOR operation
[36] 2022	DNN with weight over the DCT	No need for training just and nonlinear technique	Not robust and histogram is not uniformly
[37] 2021	Use CNN in both diffusion and confusion	Useful for diffusion in encryption	Require two images to get encryption
[38] 2022	Key generating using DNN	Generate dynamic key	Not enough efficiency
[39] 2018	Using DNN and traditional techniques	Increase the security due to dynamic key	Weak decryption method need to improve
[40] 2022	Deep learning technique for iris image	Stand against brute force attack	Weak in general
[41] 2020	Using Chaotic Sequence and Deep Auto encoder	Auto encoder to keep scrambling for secure image	Weak histogram uniform

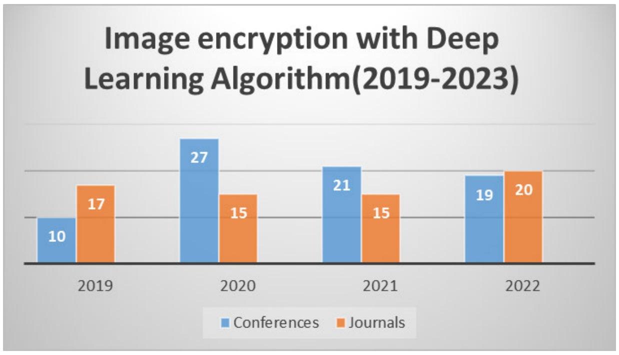


FIGURE 3. Publishing research in literature.

B. IMAGE ENCRYPTION WITH DEEP LEARNING

Traditional image encryption employed a variety of techniques, including chaotic sequence techniques, which served as the key to the encryption secret. The encryption system essentially alters the positions of the pixels in the encrypted image, as well as their numerical values [41]. Recently, researchers have employed artificial intelligence techniques, such as deep learning technology, to encode images. Figure 3 estimates the number of studies that considered deep learning in image encryption from 2018 to 2023, and efforts in this direction are still ongoing.

The regular image undergoes encryption through convolution. The chaotic sequences of a specific chaotic map update the convolution kernel, requiring no training for effective encryption. [42] The permutation process encodes images through the confusion and diffusion processes, creating the convolution kernel for the convolutional network and obtaining the necessary sequence for the scrambling process. XOR operations with chaotic sequences carry out the propagation process. In general, encryption consists of combination, switching, and diffusion. The large key space is one of the foundations of the encryption process's success [43]. Discrete Fourier transform (DCT) operations also yield the encrypted image, with chaotic operations playing a crucial role in this type of encryption. Encryption using deep learning sometimes requires a GAN cycle to create an encryption key. For certain images, the key is kept private through a network and 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 the bit locations of a single pixel and are often associated with deep learning algorithms. Table 1 summarizes the most important studies in the literature.

Encryption, a highly secure process for images, relies on advanced encryption standards [44]. The property of pseudo-randomness and the sensitivity of the initial value in the chaotic map, along with their interaction, are reliable properties in encryption. These chaotic maps generate the encryption key. 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. We utilize chaotic maps to blend the elements of the input image, thereby concealing them. For the mixing process, we employ novel and inventive methods for each technique, resulting in a map that the encryption key alone can decrypt.

III. DEEP LEARNING IN IMAGE ENCRYPTION

Deep learning has become one of the most popular artificial intelligence techniques recently. Many applications have used deep learning techniques, and these include image processing, such as image classification, object detection, and image transfer over networks. The structure of the neural network and its multiple layers assisted in correct prediction for a variety of applications. Deep neural networks have solved many complex functions that require deep calculations and nearly impossible derivations.

In image encryption, there are several operations that take place on the image in order for it to be encrypted. The most crucial step involves the random distribution of pixels within the image, where various functions and artificial intelligence technology generate random numbers. Generating random numbers is considered the basis of our study, which uses deep learning technology to work on hidden layers that produce data from one layer to the next. One of the most important features of a deep neural network is that layers at one level can refer data to layers at levels before the current one. Applications such as economic transactions [45], electricity [46], and pattern recognition [47], [48] can utilize deep learning or AI algorithms. Despite the technological development at the present time, working with large data, such as images with many pixels (with high resolution), is still difficult and complex, as in satellite images that require complex mathematical operations. In this case, the use of deep learning techniques is an urgent necessity to increase performance. This is necessary to enhance the efficiency of the work and boost the accuracy of the output. Deep learning is a modern technology that adopts the intermediate results of the hidden layers, or sometimes incorporates the final results into the output layer. Here, we process non-linear data through an unsupervised learning method, thereby creating new patterns. Deep learning emulates the human brain's capacity for deduction, working to anticipate future events and correct errors before they arise. An ordinary image is vulnerable to revealing information, but our method helps deep learning conceal the data with a strong and robust algorithm. Deep learning algorithms help insecure images make their information more robust and secure. The features extracted from the represented image, predetermined from the lowest to the highest level, form the basis of deep learning. Deep learning provides services to many applications, including image processing, which ignores any distribution of pixels in the image and thus redistributes in a more complex way. These are the features that form the basis of deep learning work.

The system considers the description of the entered image as the basic essence of the encryption process. There are restrictions during encryption and decryption that require careful consideration. Deep learning works to remove restrictions. The difference between machine learning and deep learning is in the process of selecting features. As in Figure 4.

Features are extracted automatically in deep learning and mimic the results that come out of the output layer. The hidden layers in the neural network play a significant role in making output decisions, and feeding takes place successively between the layers, from the input layer to the output layer, passing through the hidden layers. The program performs complex calculations based on the preliminary calculations, aiming to improve efficiency. The process of encrypting images involves complex calculations, including correlations between pixels, the diffusion matrix, and the generated confusion matrix. This led to the idea of using deep learning algorithms instead of regular ones. The foundation of encryption relies on deep learning technology to identify complex randomness in the distribution of pixels, and deep learning is responsible for predicting the optimal random map.

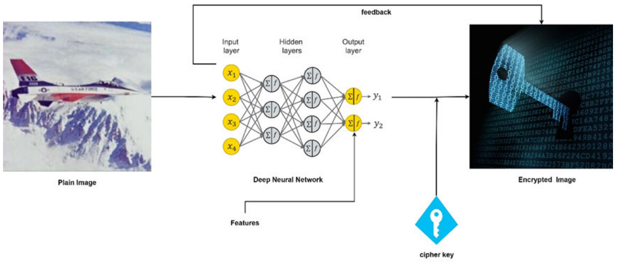


FIGURE 4. Encrypted image with deep learning.

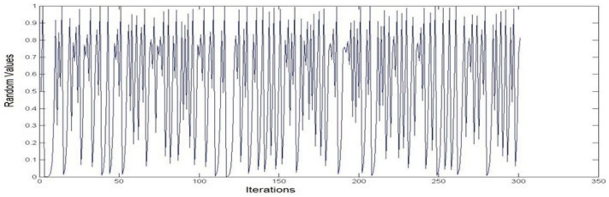


FIGURE 5. Behaviour of logistic map.

IV. PROPOSED METHOD

In image processing, encryption is very important and depends mainly on the random generation key. Some of the methods rely on one key, and the other section relies on two encryption keys. In the proposed method, we use two chaotic maps, Henon's map and Sensitive Logistic Maps (SLM). The main purpose of the existing algorithm in image encryption is to increase the mess of pixels inside the image to be more complex and secure [49]. In this case, complex randomness is obtained for good encryption standards. The general behavior of the logistic map is described by the following equations.

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

Consider $r \in (0.4)$ with $n = 1, 2, \ldots, n$, where X_1 is initial value such as $(0 < X_1 < 1)$. r for logistic map with range around 3.5699 and 4. Figure 4 shows the behavior of logistic map such as $X_1 = 0.5$ and $r = 3.99$.

In the proposed method, there is a second chaotic map, which is the Henon, which contributes to increasing the complexity of randomness, and the following equations explain the behavior of the map.

$$X_{n+1} = 1 - aX_n^2 + Y_n \tag{2}$$

$$Y_{n+1} = bX_n \tag{3}$$

where X and Y are initial conditions, and a and b control parameters used for cryptography. For strong chaotic will be at $a = 1.3$ and $b = 0.4$. this because of Henon response for these parameters.

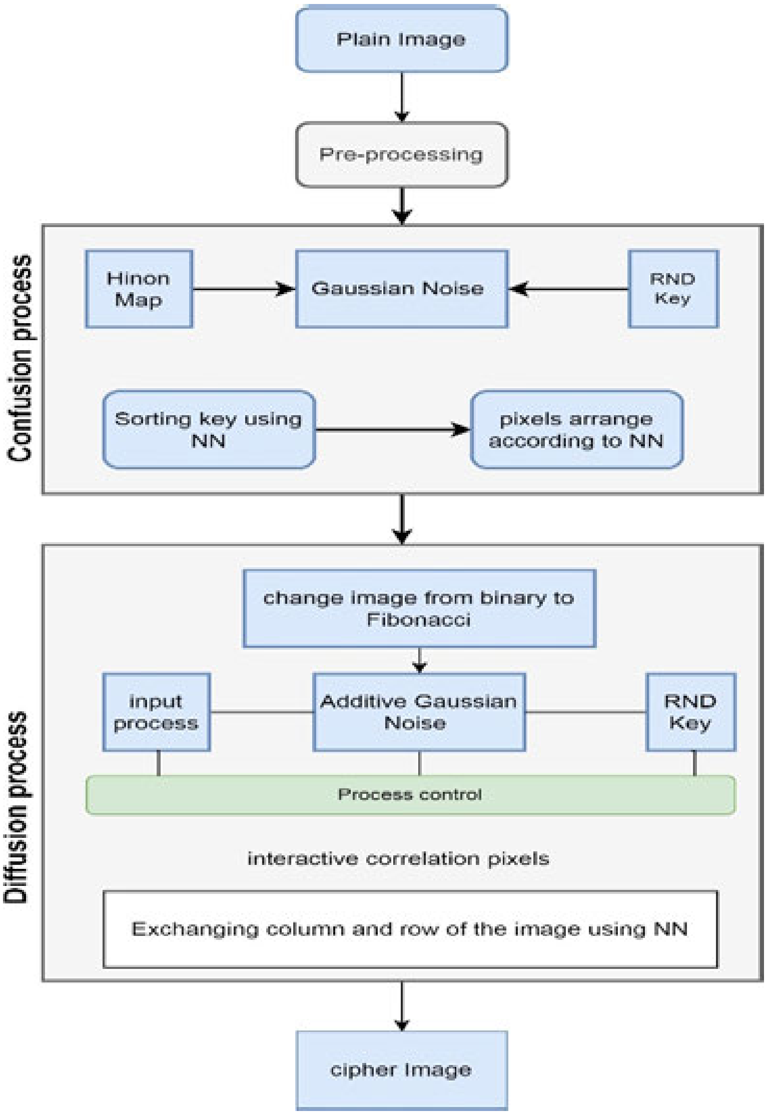


FIGURE 6. General framework for image encryption.

A feature of the encrypted image. Therefore, during encryption, those pixels distribute their useful information in a calculated manner, rendering it unreadable by an outsider. Adding noise to an image distorts the useful information, making it readable upon its removal. We define noise as the addition of unwanted data to the image, altering its quality and impacting the image's overall quality. There are several types of noise, including Gaussian noise, anisotropic noise, and salt and pepper noise, the most famous of which is Gaussian noise. The pixels in the image are significantly impacted by this noise. The following equations describe the Gaussian distribution.

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

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

Any encryption process in general consists of two main parts: confusion and the diffusion process. As in the Fig. 6, initially the original image goes through pre-processing operations in order to be prepared for subsequent processing operations.

The basic process in encryption is the method of making a random key, which is responsible for randomly distributing pixels within the image to be encrypted. Any change in the location of the pixels leads to a change in the visual image and it becomes a random, meaningless image. Regardless of the information stored in the pixels, it remains the same and the change occurs in the position only $P(x, y)$. The number and density of pixels do not change during encryption or the random distribution of pixels. The encryption key stores the pixel positions to aid in their restoration during the reception and decryption processes. The deep neural network will encode the image by randomly selecting rows and columns.

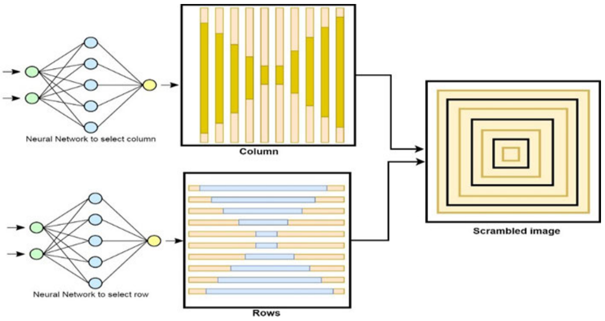


FIGURE 7. Scrambling rows and column by deep learning.

The number of pixels in the image determines the size of the rows and columns in a sequential descending or ascending manner. As a result, the process of replacing columns begins by choosing two random values for the number of columns in the image, and the replacement takes place between the two random numbers. The process continues until the number of columns reaches its limit, at which point the same mechanism applies to the rows in the image until the encrypted image is complete. As in Fig. 7.

The selection of columns and rows is one of the features that are extracted from the image and the number of pixels that make up each of the columns and rows. The decrease and increase in pixels is calculated through a deep neural network, and the hidden layers work to find the estimated number of pixels and the correct prediction in the number of columns and rows. The neural network is fed with the current $P(x, y)$ coordinates of the pixels, after which the new coordinates of the pixels are selected and predicted in the advanced stages.

Key space is the number of attempts necessary to guess a correct decryption key. Strong encryption should have an encryption key no smaller than 2100, with the exponent indicating the number of bits in the key. Large encryption keys provide greater security against brute-force attacks. In a good encryption system, the large key space indicates good resistance against brute force attacks. The use of a secret key for encryption produces strong encryption, as any change in the secret key produces another encrypted image. Secure image cryptosystems make use of secret keys to evaluate the robustness of an encryption scheme. In a cryptosystem, an image cannot be decrypted if there is any difference between the encryption and decryption keys.

A deep neural network coordinates the coordinates of pixels that result from hidden layers. Through the process of training the neural network, the coordinates are updated step by step until they reach the level of complexity required to replace their places through columns and rows. As shown in Fig. 8.

The main purpose of changing the sequence of pixel locations of an image is to encrypt it and confuse the intruder. Any change in the coordinates of the pixels in the image has nothing to do with changing the values of the pixels. The logistic map and the Henon map are used as a label in order to give the neural network a limit for the purpose of knowing the required degree of complexity. The degree of complexity of the proposed algorithm, which we will consider, can be tested through the following equations.

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

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

$$\bar{A} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}A_{ij} \tag{6}$$

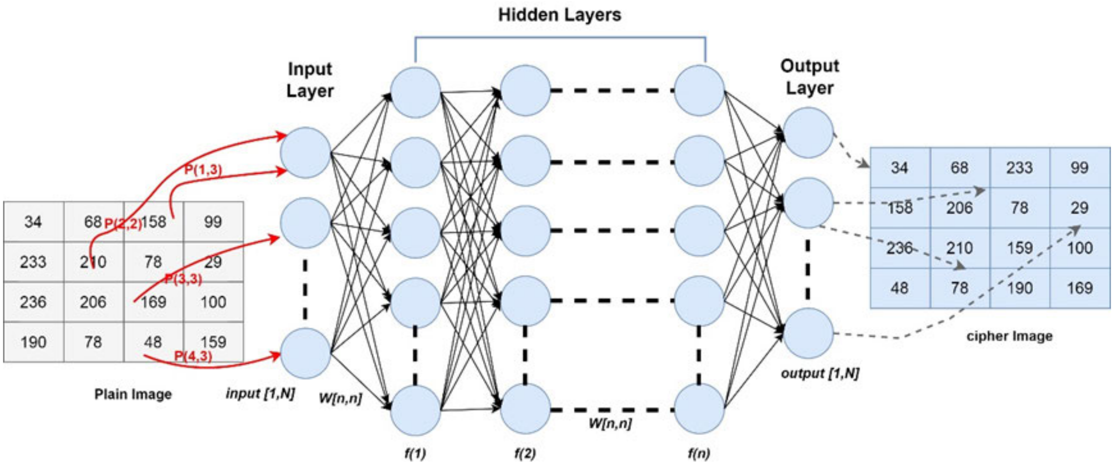
$$\bar{B} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}B_{ij} \tag{7}$$

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

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

After changing the locations of the pixels and manipulating their coordinates, we need to change the pixel values in order to increase the security of the image. Changing pixel values means destroying the information contained in the image and making it meaningless. In this case, we need to know the components of the pixel: it consists of two main parts, the first is the coordinates and the second is its value, i.e. the decimal number that includes the color contrast value in it. When processing the image, the decimal value is changed to a binary value of 0 and 1. The binary digital value is equal to 2^8, which achieves 8 orders of bits to give the highest color value of 256. Since the binary value is known to everyone, a formula that is unfamiliar to the hacker or intruder must be used.

Fibonacci is a 12-bits formula, not the 8-bits formula used with binary options. Its equation consists of adding the two bits to form the result in the third bit. During process, the decimal number in the image is converted to a Fibonacci analysis. In this case, the pixel value will have changed to a strange formula and it will remain part of the image and cannot be read in order to increase the security of the image. The Fibonacci analysis can be observed as in the Fig. 9. The main purpose of changing the sequence of pixel locations in an image is to encrypt it and confuse the intruder. Any change



34	68	158	99
233	210	78	29
236	206	169	100
190	78	48	159

34	68	233	99
158	206	78	29
236	210	159	100
48	78	190	169

FIGURE 8. Deep neural technique with image encryption.

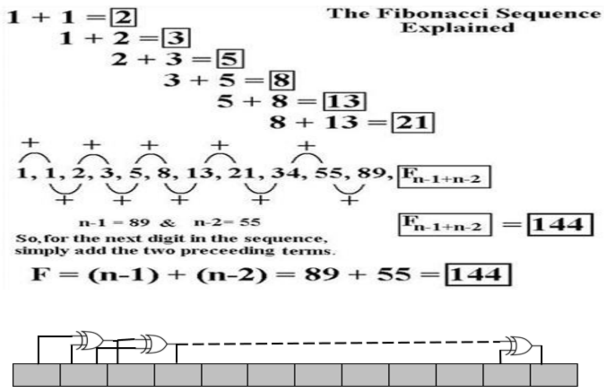

The Fibonacci Sequence Explained
1 + 1 = 2
1 + 2 = 3
2 + 3 = 5
3 + 5 = 8
5 + 8 = 13
8 + 13 = 21
1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, F n-1+n-2
n-1 = 89 & n-2 = 55
F n-1+n-2 = 144
So, for the next digit in the sequence, simply add the two preceeding terms.
F = (n-1) + (n-2) = 89 + 55 = 144

FIGURE 9. Mechanizem of fibonacii decomposition.

in the coordinates of the pixels in the image has nothing to do with changing the values of the pixels. The logistic map and the Henon map are used as labels in order to give the neural network a limit for the purpose of knowing the required degree of complexity. The degree of complexity of the proposed algorithm, which we will consider, can be tested through the following equations.

With Fibonacci, the impact of each bitplane of binary decomposition is equal to 2k where k represents the bitplane order (for example k=3 for bitplane number 3, k=7 for bitplane number 7 and so on). The impact of each layer in the binary representation increases with the next bits position. To explain the method of analysis of any pixel value from decimal representation to Fibonacci representation using Fibonacci sequence on this sequence, the general formula of the Fibonacci sequence is given as: $F1 = 1, F2 = 1, F3 = 1 + 1 = 2, F4 = 2 + 1 = 3, F5 = 3 + 2 = 5, \ldots, Fn = Fn - 1 + Fn - 2$

In general

$$F\left(n\right) = \begin{cases} 0, & if\ n = 0 \\ 1, & if\ n = 1 \\ F\left(n-1\right) + F\left(n-2\right), & if\ n > 1 \end{cases}$$

The Fibonacci sequence of numbers, each number is the sum of the previous two numbers. Fibonacci began the sequence not with 0, 1, 1, 2, as modern mathematicians do but with 1,1, 2, etc. He carried the calculation up to the thirteenth place (fourteenth in modern counting), that is 233, though another manuscript carries it to the next place: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377. Fibonacci did not speak about the golden ratio as the limit of the ratio of consecutive numbers in this sequence. Algorithm 1 shows the algorithm steps for Fibonacci number.

Algorithm 1 Fibonacci Number Representation

```
Input: An integer $n$ for $n^{th}$ Fibonacci number.
Output: n-th Fibonacci number.
FN[0]←0;
FN[1]←1;
for $i \leftarrow 2$ to $n - 1$ do
    $FN[i] \leftarrow FN[i-1] + FN[i-2]$;
    $i = i + 1$ ;
end
Return $FN[n-1]$
```

Three main reasons for using Fibonacci decomposition are:

1) Changing to Fibonacci decomposition improves the security due to difficulty in estimating the secret data by attacker.
2) Increase the robustness of the system because of using 12 bit-planes.
3) Difficult to recognize by visual attack because of heterogeneous data.

Each pixel in the image is represented by 8 physical bits, and the encoded image uses 12 logical bits. The conversion to the plain image is 8-bits, and the encrypted image is converted to 12-bits, as shown in the Fig. 10.

The main purpose of the diffusion process is to change the pixel's value for a uniform image histogram and more security. Thus, the Fibonacci decomposition changes the pixel

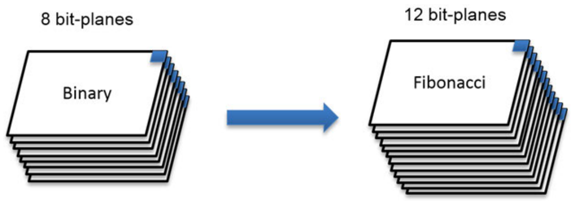


FIGURE 10. Decomposition of plain and encrypted image.

value without changing the information inside it because it is easy to recover if someone has a cipher key. The whole process is illustrated in Algorithm 2. As we will conclude in the next section of the result.

Algorithm 2 Process of Cyphering Image

```
Input: Images from dataset.
Output: Cypher images.
Read: image $(n)$; Preprocess image ;
Noise reduction $(n)$; Normalization $(n)$;
Confusion process;
Generating RND key; Applying Gaussian noise $(n)$;
  Applying Henon map;
for all image $(n)$ do
    Extracting $P(x; y)$ for each pixel;
    Store $P(x; y) \rightarrow$ Vector;
end
Construct NN; arrange Vector by NN;
Diffusion process;
Create Fibonacci $(n)$;
Apply Gaussian for image $(n)$;
Find correlation of 8-neighbors $(x, y)$;
for all image $(n)$ do
    By using RND key and NN;
    Change columns and rows in Vector;
end
Produce Cypher image (n)
```

V. RESULTS AND DISCUSSION

There are many criteria that are used to evaluate the encrypted image and determine the strength of the proposed method. In this study, we will take into consideration the most important standards used in previous studies in order to benchmark the results with them, in addition to trying to improve the proposed method to be a standard method and a comprehensive system for encrypting images. Encryption in general is a method of hiding information or an image in such a way that no one can reveal the original image except through the encryption key. The process of retrieving the image is almost impossible without the encryption key, which contains all the steps to solve the encryption. Encryption and decryption are two methods, one of which is the opposite of the other. The image is encrypted by the sender, and after sending it to the recipient, it is decrypted. As shown in Fig. 11.

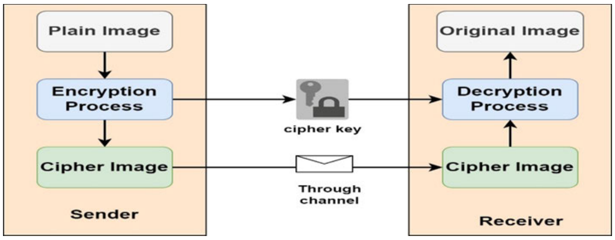


FIGURE 11. Encryption and decryption protocol.

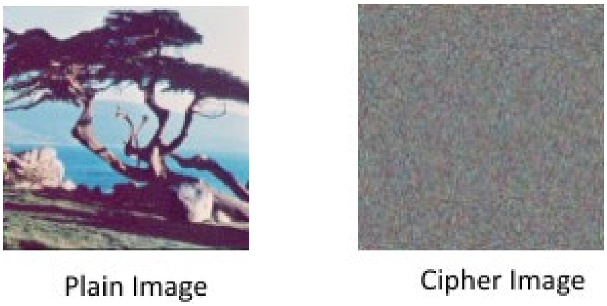


FIGURE 12. Original and encrypted image.

In the encryption process, the original image is prepared, which is called a plain image, after which the encryption process is applied according to the method followed, and the method information is stored in the encryption key, which is called the cipher key, and is agreed upon with the recipient. After encryption, a random image called a cipher image is generated and sent to the other party to begin the reverse process of extracting the original image and decrypting it with the help of the encryption key. The image (cipher image) sent to the recipient is a distorted image that is not clear and cannot be understood, as in Fig. 12.

Many criteria have been applied to measure the integrity of the encryption. The more complex the encryption, the more difficult it is to decrypt, and thus the security of the information inside it. There are many criteria used to measure the accuracy and difficulty of encryption, including:

Correlations help enhance the security of the encrypted image. By spreading the influence of individual pixels across neighboring pixels, correlation ensures that small changes in the input image result in significant alterations in the encrypted image, making it resistant to attacks. Histograms allow statistical analysis of pixel intensity distribution, which can inform the design of encryption systems. Through histograms, patterns and statistical properties of the image can be identified that can be exploited or manipulated to enhance cryptographic security. Uniform histograms reflect better encryption due to the inability to interpret the information of the pixels in the image, and randomness means that the selected pixels in the encrypted image change their location or value randomly. The increased randomness of the method allows the pixels not to be returned to their original places or to their initial values, which is the main purpose of encryption because it is not possible to know the contents of the image.

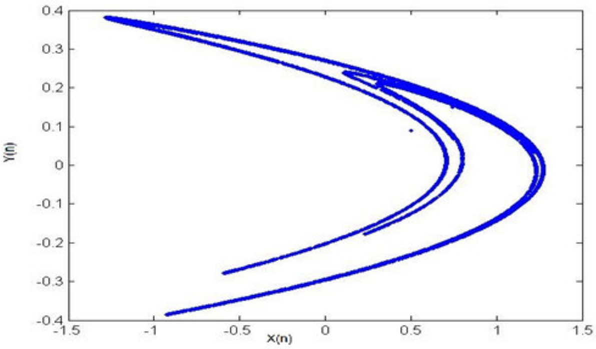


FIGURE 13. Behaviour of randomness in the system.

Henon map converges with a strange attractor through which randomness can be estimated in the form of two coordinates, as shown in the Fig. 13.

The image after encryption loses many features, especially after changing the coordinates of the pixels in the image or changing the pixel values. Because of the randomness in the image, which is considered complex due to the use of random functions and the noise added to the image, the image is therefore statistically evaluated after encryption to indicate the strength of the encryption for the method used, as in the following Table 2.

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

S-Value and P-Value are among the randomization tests provided by NIST and contain more than one test item. A large p-value means that the randomness is very good. If it is higher than 0.01, it means it is good and the tests are based on pseudo-randomness. The value of S is the randomness that connects the pixels to each other or to the pixel and its surroundings. It must also be high, more than 0.02, and the values here are less than the upper limit, which is 1. This test was used because it is used in previous methods and is approved.

Because of the change in pixel values, which affects the histogram and is considered one of the most important evaluation that reflects the strength of the diffusion process (changing pixels' value). The only way to know the strength of the diffusion is the histogram before and after encryption, as shown in the Fig. 14, which means that the distribution of pixel values in the image is on one level.

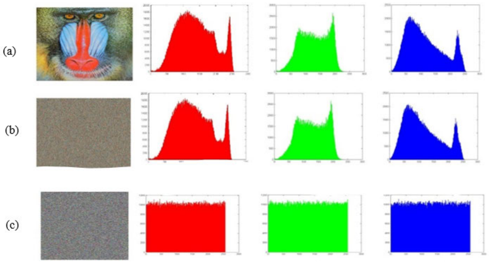
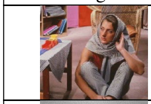
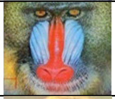


FIGURE 14. (a) histogram of plain image (b) histogram of encrypted image before diffusion (c) histogram of encrypted image after diffusion.

Fig. 14(a) reflects the histogram of three parts of image RGB and the distribution of the pixel value over several pixels in a certain image. (b) consider the histogram before diffusion which is the same as the original image and easy for the hacker to find, while section (c) represents the image after diffusion (change pixel value) and will get a uniform histogram and difficult for the hacker to discover the information of the encrypted image.

The pixel value with the proposed random value for the encryption strength is effective and gives more complexity with the three random methods used in addition to the key space. One of the important evaluations in image encryption is finding the strength of the correlation between pixels in a single image, or subjecting more than 5,000 pixels to a random equation in a deep neural network with a number of iterations determined by the neural network during training. Three correlations per pixel were taken into consideration: vertical, horizontal, and diagonal. Training was done on the standard SIPI dataset, which is widely used in previous research, so that we can compare the results obtained with previous studies. As shown in the Table 3.

TABLE 3. Illustrate the correlation of images with proposed method.

Image specification			Correlation		
Images	Image Type	Image size	Vertical	Horizontal	Diagonal
	RGB	512×512	0.962	0.951	0.921
	Grayscale	512×512	0.932	0.978	0.937
	RGB	1200×110	0.893	0.887	0.897
	RGB	512×512	0.932	0.936	0.976
	RGB	1200×110	0.973	0.978	0.938
	Grayscale	512×512	0.872	0.886	0.871

Through evaluations and practical results of the proposed method, the merit of the proposed method can be proven,

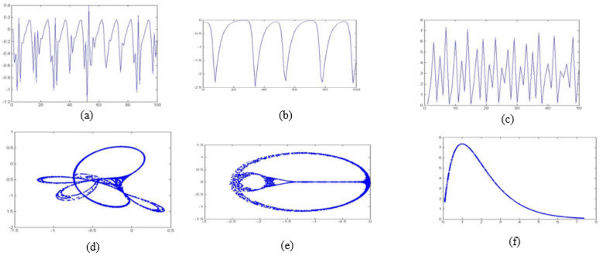


FIGURE 15. Different maps through the system with its combination.

given the goal of each study is to obtain good results. It is possible that we will achieve more ideal results in the future to encrypt images with a high degree of security.

Figure 15 illustrate the three kinds of map with corresponding behavior where (a) is the Henon map and (b) logistic map and (c) compline of the two maps during the system. The behavior of pixels distribution in image in the Fig. 15 (d and e) reflects the reason behind using and merging two algorithms, which is considered incomprehensible and therefore combining them, as in Fig. 15 (f), would be better.

During the training of the system confusion and diffusion behavior will be change through the training. Such as the behavior of the first iteration is totally different with embedding some improvement in the system. With Fibonacci decomposition will attach the final step of iteration and give strangeness to the system in term of randomness and security as shown in Fig. 16.

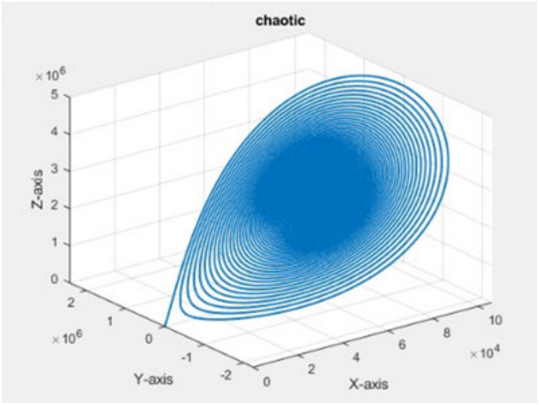


FIGURE 16. Chaotic of the system through Fibonacci decomposition.

As we notice the complexity of the outer shape is less than inner shape due to the complexity increase with increasing the bit-planes in the image. The outer shape represents the 20 while the center is 2^{12}.

In order to demonstrate the worth of the proposed method, we must compare it with modern methods in previous studies, and this is shown in Table 4. For existing methods, the numbers mentioned are the best values. For the proposed method, 2200 images from the dataset tested, and we considered the best value with the average for all images.

TABLE 4. Benchmark for low resolution image with existing method.

Author/year	Image Size/pixels	NPCR%	PSNR/ decibels (dB)	Entropy bit per pixel (b/p)
Kamal, S. T., et al (2021) [50]	128×128	99.678	76.8	6.7
Pourasad, Y., et al (2021) [51]	128×128	99.452	83.5	6.9
Sarosh, P.,et al (2022) [52]	128×128	99.762	99.1	7.3
He, D., et al (2023) [53]	128×128	—-	88.9	7.2
Ferdush, J.,et al (2021) [54]	128×128	99.518	78.9	——
Jun, W. J., & Fun, T. S. (2021) [55]	128×128	99.736	89.8	7.6
Proposed	128×128	99.836 av.: 99.429	99.3 av.: 99.01	7.7 av.: 7.1

The standard criteria that must be met in every measurement of the encrypted image include: NPCR, which is a Number of Pixels Change Rate, indicates the number of pixels change rate while one pixel of a plain image changes. Peak Signal to Noise Ratio (PSNR) is the ratio of the maximum value of the pixel to the noise (MSE) that affects the quality of the pixels. And entropy is a measure of the number of pixels required to encode image data.

VI. CONCLUSION

In this study, the image encryption process was presented using a random key and integrating the deep learning algorithm with Fibonacci analyses. The main goal of any encryption process is to increase randomness, so the Henon map and the logistic map were used to increase the complexity of the randomness, and thus increase the chaos of the image. Encryption in general consists of two main roles: first, changing the location of pixels in the image and the relationship of each pixel with its neighbors (confusion), and second, changing the value of the pixel (diffusion). The random selection comes from the deep neural network, which predicts the ideal position for the pixel, and the process of switching rows and columns was used according to complex randomness. Fibonacci analysis contributed to the image revision process and was evaluated using a histogram, degree of randomness, and strength of correlation using images from a standard database. Satisfactory results were obtained, which reflects the efficiency of the proposed method.

REFERENCES

[1] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, "An efficient image encryption technique based on two-level security for Internet of Things," *Multimedia Tools Appl.*, vol. 82, no. 4, pp. 5091–5111, Feb. 2023.

[2] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, "Digital image steganography: A literature survey," *Inf. Sci.*, vol. 609, pp. 1451–1488, Sep. 2022.

[3] M. S. Rathore, M. Poongodi, P. Saurabh, U. K. Lilhore, S. Bourouis, W. Alhakami, J. Osamor, and M. Hamdi, "A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108205.

[4] A. M. Fadhil, "Bit inverting map method for improved steganography scheme," Ph.D. thesis, Doctor Philosophy Comput. Sci., Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia, 2013.

[5] S. Zhou, Y. Qiu, G. Qi, and Y. Zhang, "A new conservative chaotic system and its application in image encryption," *Chaos, Solitons Fractals*, vol. 175, Oct. 2023, Art. no. 113909.

[6] A. M. Fadhil, H. N. Jalo, and O. F. Mohammad, "Improved security of a deep learning-based steganography system with imperceptibility preservation," *Int. J. Electr. Comput. Eng. Syst.*, vol. 14, no. 1, pp. 73–81, Jan. 2023.

[7] A. Kumar, R. Rani, and S. Singh, "A survey of recent advances in image steganography," *Secur. Privacy*, vol. 6, no. 3, May 2023, Art. no. e281.

[8] H. Caballero, V. Muñoz, and M. A. Ramos-Corchado, "A comparative study of steganography using watermarking and modifications pixels versus least significant bit," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 6, p. 6335, Dec. 2023.

[9] X. Wang, Y. Su, M. Xu, H. Zhang, and Y. Zhang, "A new image encryption algorithm based on Latin square matrix," *Nonlinear Dyn.*, vol. 107, no. 1, pp. 1277–1293, Jan. 2022.

[10] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik*, vol. 272, Feb. 2023, Art. no. 170316.

[11] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "A novel pixel-split image encryption scheme based on 2D salomon map," *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 118845.

[12] Y. Alghamdi and A. Munir, "An image encryption algorithm based on trivium cipher and random substitution," *Social Netw. Comput. Sci.*, vol. 4, no. 6, p. 713, Sep. 2023.

[13] Priyanka and A. K. Singh, "A survey of image encryption for healthcare applications," *Evol. Intell.*, vol. 16, no. 3, pp. 801–818, Jun. 2023.

[14] T. A. Khan, A. Fatima, T. Shahzad, Atta-Ur-Rahman, K. Alissa, T. M. Ghazal, M. M. Al-Sakhnini, S. Abbas, M. A. Khan, and A. Ahmed, "Secure IoMT for disease prediction empowered with transfer learning in healthcare 5.0, the concept and case study," *IEEE Access*, vol. 11, pp. 39418–39430, 2023.

[15] Q. Zhou, X. Wang, M. Jin, L. Zhang, and B. Xu, "Optical image encryption based on two-channel detection and deep learning," *Opt. Lasers Eng.*, vol. 162, Mar. 2023, Art. no. 107415.

[16] R. Montero-Canela, E. Zambrano-Serrano, E. I. Tamariz-Flores, J. M. Muñoz-Pacheco, and R. Torrealba-Meléndez, "Fractional chaos based-cryptosystem for generating encryption keys in ad hoc networks," *Ad Hoc Netw.*, vol. 97, Feb. 2020, Art. no. 102005.

[17] S. R. Maniyath and V. Thanikaiselvan, "An efficient image encryption using deep neural network and chaotic map," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103134.

[18] L. Zhang, R. Xiong, J. Chen, and D. Zhang, "Optical image compression and encryption transmission-based ondeep learning and ghost imaging," *Appl. Phys. B, Lasers Opt.*, vol. 126, no. 1, pp. 1–10, Jan. 2020.

[19] F. Wang, R. Ni, J. Wang, Z. Zhu, and Y. Hu, "Invertible encryption network for optical image cryptosystem," *Opt. Lasers Eng.*, vol. 149, Feb. 2022, Art. no. 106784.

[20] S. Panchikkil and V. M. Manikandan, "A machine learning based reversible data hiding scheme in encrypted images using Fibonacci transform," in *Proc. Int. Conf. Innov. Trends Inf. Technol. (ICITIIT)*, Feb. 2022, pp. 1–6.

[21] J. Zheng and Q. Zeng, "An image encryption algorithm using a dynamic S-box and chaotic maps," *Appl. Intell.*, vol. 52, no. 13, pp. 15703–15717, Oct. 2022.

[22] S. Zhou, Z. Zhao, and X. Wang, "Novel chaotic colour image cryptosystem with deep learning," *Chaos, Solitons Fractals*, vol. 161, Aug. 2022, Art. no. 112380.

[23] A. C. H. Chen, "Post-quantum cryptography neural network," in *Proc. Int. Conf. Smart Syst. Appl. Electr. Sci. (ICSSES)*, Jul. 2023, pp. 1–6.

[24] R. Verma, N. Dhanda, and V. Nagar, "Enhancing security with in-depth analysis of brute-force attack on secure hashing algorithms," in *Proceedings of Trends in Electronics and Health Informatics*. Kanpur, India: Springer, 2021, pp. 513–522.

[25] M. Z. Salim, A. J. Abboud, and R. Yildirim, "A visual cryptography-based watermarking approach for the detection and localization of image forgery," *Electronics*, vol. 11, no. 1, p. 136, Jan. 2022.

[26] D. Zhang, L. Ren, M. Shafiq, and Z. Gu, "A privacy protection framework for medical image security without key dependency based on visual cryptography and trusted computing," *Comput. Intell. Neurosci.*, vol. 2023, pp. 1–11, Jan. 2023.

[27] Y. Khazaal, Y. Aydi, and M. Abid, "Secure image transmission through differential chaos shift keying communication system," *Int. J. Comput. Digit. Syst.*, vol. 14, no. 1, pp. 457–467, Aug. 2023.

[28] Y. Liu, Z. Jiang, X. Xu, F. Zhang, and J. Xu, "Optical image encryption algorithm based on hyper-chaos and public-key cryptography," *Opt. Laser Technol.*, vol. 127, Jul. 2020, Art. no. 106171.

[29] A. P. Kari, A. H. Navin, A. M. Bidgoli, and M. Mirnia, "Image cryptosystem based on plain image correlation rate and selective chaotic maps," *Multimedia Tools Appl.*, vol. 81, no. 15, pp. 20483–20508, Jun. 2022.

[30] Y. Chen, S. Xie, and J. Zhang, "A hybrid domain image encryption algorithm based on improved Henon map," *Entropy*, vol. 24, no. 2, p. 287, Feb. 2022.

[31] S. De, J. Bhaumik, and D. Giri, "A secure image encryption scheme based on three different chaotic maps," *Multimedia Tools Appl.*, vol. 81, no. 4, pp. 5485–5514, Feb. 2022.

[32] D. Wei, M. Jiang, and Y. Deng, "A secure image encryption algorithm based on hyper-chaotic and bit-level permutation," *Expert Syst. Appl.*, vol. 213, Mar. 2023, Art. no. 119074.

[33] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, "DeepEDN: A deep-learning-based image encryption and decryption network for Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1504–1518, Feb. 2021.

[34] Z. Zheng, H. Liu, Z. Yu, H. Zheng, Y. Wu, Y. Yang, and J. Shi, "EncryptGAN: Image steganography with domain transform," 2019, *arXiv:1905.11582*.

[35] Z. Bao and R. Xue, "Research on the avalanche effect of image encryption based on the cycle-GAN," *Appl. Opt.*, vol. 60, no. 18, p. 5320, 2021.

[36] C. Wang and Y. Zhang, "A novel image encryption algorithm with deep neural network," *Signal Process.*, vol. 196, Jul. 2022, Art. no. 108536.

[37] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons Fractals*, vol. 152, Nov. 2021, Art. no. 111318.

[38] Y. Ding, F. Tan, Z. Qin, M. Cao, K. R. Choo, and Z. Qin, "DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 9, pp. 4915–4929, Sep. 2022.

[39] X. Li, Y. Jiang, M. Chen, and F. Li, "Research on iris image encryption based on deep learning," *EURASIP J. Image Video Process.*, vol. 2018, no. 1, pp. 1–10, Dec. 2018.

[40] Y. Sang, J. Sang, and M. S. Alam, "Image encryption based on logistic chaotic systems and deep autoencoder," *Pattern Recognit. Lett.*, vol. 153, pp. 59–66, Jan. 2022.

[41] J. Zhou, J. Li, and X. Di, "A novel lossless medical image encryption scheme based on game theory with optimized ROI parameters and hidden ROI position," *IEEE Access*, vol. 8, pp. 122210–122228, 2020.

[42] S. P. Praveen, V. S. Suntharam, S. Ravi, U. Harita, V. N. Thatha, and D. Swapna, "A novel dual confusion and diffusion approach for grey image encryption using multiple chaotic maps," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 8, pp. 971–984, 2023.

[43] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Arch. Comput. Methods Eng.*, vol. 27, no. 1, pp. 15–43, Jan. 2020.

[44] A. Altigani, S. Hasan, B. Barry, S. Naserelden, M. A. Elsadig, and H. T. Elshoush, "A polymorphic advanced encryption standard—A novel approach," *IEEE Access*, vol. 9, pp. 20191–20207, 2021.

[45] N. K. Abed, A. Shahzad, and A. Mohammedali, "An improve service quality of mobile banking using deep learning method for customer satisfaction," *AIP Conf. Proc.*, vol. 2746, no. 1, 2023, Art. no. 090001.

[46] B. T. Atiyha, S. Aljabbar, A. Ali, and A. Jaber, "An improved cost estimation for unit commitment using back propagation algorithm," *Malaysian J. Fundam. Appl. Sci.*, vol. 15, no. 2, pp. 243–248, Apr. 2019.

[47] G. Sulong and A. Mohammedali, "Human activities recognition via features extraction from skeleton," *J. Theor. Appl. Inf. Technol.*, vol. 68, no. 3, pp. 645–650, 2014.

[48] G. Sulong and A. Mohammedali, "Recognition of human activities from still image using novel classifier," *J. Theor. Appl. Inf. Technol.*, vol. 71, no. 1, pp. 115–121, 2015.

[49] S. B. Mamia, P. Puteaux, W. Puech, and K. Bouallegue, "From diffusion to confusion of RGB pixels using a new chaotic system for color image encryption," *IEEE Access*, vol. 11, pp. 49350–49366, 2023.

[50] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021.

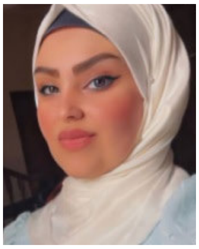
[51] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, no. 3, p. 341, Mar. 2021.

[52] P. Sarosh, S. A. Parah, and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimedia Tools Appl.*, vol. 81, no. 5, pp. 7253–7270, Feb. 2022.

[53] D. He, R. Parthasarathy, H. Li, and Z. Geng, "A fast image encryption algorithm based on logistic mapping and hyperchaotic Lorenz system for clear text correlation," *IEEE Access*, vol. 11, pp. 91441–91453, 2023.

[54] J. Ferdush, M. Begum, and M. S. Uddin, "Chaotic lightweight cryptosystem for image encryption," *Adv. Multimedia*, vol. 2021, pp. 1–16, May 2021.

[55] W. J. Jun and T. S. Fun, "A new image encryption algorithm based on single S-box and dynamic encryption step," *IEEE Access*, vol. 9, pp. 120596–120612, 2021.



YASMINE M. KHAZAAL was born in Baghdad, Iraq, in 1995. She received the B.Sc. degree in software engineering, in 2017, and the M.Sc. degree in computer engineering from the College of Engineering, Iraqi University, Baghdad, in 2021. Her research interests include computer security, image processing, FPGA's and Xilinx system generator, chaotic modulation, and digital signal processing.

ALI DOUIK was born in Tunis, Tunisia. He received the B.S., M.S., and Ph.D. degrees in electrical engineering from ENSET, Tunis, in 1988, 1990, and 1996, respectively, and the HDR degree in electrical engineering from the University of Monastir, Monastir, Tunisia, in 2010. He was at the National Engineering School of Monastir, from September 1991 to September 2014. He is currently a Full Professor with the Department of Industrial Computing, National Engineering School of Sousse. His research interests include digital image processing, artificial intelligence, machine learning, deep learning, automatic control, optimization, and evolutionary algorithms.

MONJI KHERALLAH was born in Sfax, Tunisia. He received the Dip.-Ing., Ph.D., and HU degrees in electrical engineering from the ENIS, University of Sfax, in 1989, 2008, and 2012, respectively. For fourteen years ago, he was an Engineer at the Biotechnology Center, University of Sfax. He is currently a Professor with the Faculty of Science, University of Sfax. He is also the Founder of a professional master's degree: "Metrology and Industrial Instrumentation," Faculty of Sciences, University of Sfax. His research interest includes signal and image processing.