A Secure and Efficient Optimized Image Encryption Using Block Compressive Sensing and Logistic Map Method

Qutaiba Kadhim Abed[1,*] and Waleed Ameen Mahmoud Al-Jawher[2]

[1] *Informatics Institute for Postgraduate Studies, Iraqi Commission for Computers and Informatics, Baghdad, Iraq*
[2] *Uruk University, Baghdad, Iraq*
E-mail: phd202130682@iips.edu.iq; profwaleed54@gmail.com
[*] *Corresponding Author*

Received 15 December 2023; Accepted 22 May 2024

Abstract

Recently, multimedia has developed and become very important for transferring images securely through public networks. This paper uses the COOT optimization algorithm with compressive sensing (CS) for image encryption. A good method was proposed for encryption using compressive sensing with COOT optimization and chaos to encrypt images and obtain optimal encryption with the least correlation between pixels. This method will strengthen the encryption against various types of attacks. The natural image was sparsed using discreet wavelet transform (DWT) and the FAN transform. The image is divided into several blocks, and CS is applied to each block. The best measurement matrix was obtained using a COOT-optimized algorithm. All blocks are masked to get the compressed image, and the pixels are quantified. Next, the COOT optimization is used to Shuffle the image pixels to achieve the minimum correlation between the pixels. Then, a logistic map will be used to uniform the image pixel values by diffusion to get the final encrypted image. Chen's chaotic and logistic map initial values are obtained from the

Journal of Cyber Security and Mobility, Vol. 13_5, 983–1006.
doi: 10.13052/jcsm2245-1439.1358

input image after its division into four parts by taking a value from each part. The evaluation results obtained for this algorithm showed that it performs highly compared to other conventional methods. The average PSNR for the reconstructed images was 35.244, the average NPCR and UACI were 90.53 and 29.54, respectively, and the average correlation was (D = 0.0018, V = 0.0031, H = 0.0039). The results proved that the method is strong enough and very efficient to withstand attacks.

Keywords: COOT optimization algorithm, BCS, Chen chaos system, Logistic map, DWT.

1 Introduction

There has been a great interest in information security since the beginning of the information era. Images have abundant data. The images are vulnerable to attacks during transmission or while saving on the Internet; hence, encryption has become very important to protect images. Traditional text encryption algorithms cannot be applied to images because they do not consider the size of images, the strong correlation between pixels, and other properties. Image encryption is a process to obtain a protected image and eliminate the correlations between pixels. There is a proposal for image encryption [1]. The mechanism that has been used for encryption includes scrambling and diffusion of images [2, 3]. Based on this, many algorithms were proposed, such as DNA coding [4] and optical encryption [5] Chaos systems are unpredictable, uncertain, and non-repeatable, which enhances the ability of the encryption system to encrypt images. Chaos systems can encrypt the image, and some encryption methods have been proposed successfully [6]. Redundant information in the image is a significant challenge for the transfer image. Simply encryption does not handle the increase in data size for images. Transferring and storing images is restricted due to the redundant data inside the images [7–11]. Compressive Sensing (CS) is a method [12–19] different from the Nyquist sampling method. It is considered a symmetric encryption system and has gotten interested in recent years.

In image encrypting, the Compressive Sensing combines compression and encryption. Therefore, Compressive Senescing reduces redundant data and improves the transmission process. From a cryptography perspective, the sparse signal, measurement matrix, and sensing matrix in CS technology correlate to the plaintext, secret key, and ciphertext in the cryptosystem. This makes the CS technology a variation on symmetric encryption. Furthermore, Rachlin et al. [20] noted that the computational security of the CS-based cryptosystem is high enough to fend against brute force attacks and ciphertext assaults. The sensing matrix is nonetheless susceptible to known and selected plaintext attacks because it was created by applying linear projection to the sparse data [21, 22]. Researchers have therefore developed a variety of image protection methods by integrating CS with encryption approaches, for example, chaos method [23–25], coding technology [26, 27], cellular automata [28, 29], neural network [30, 31], and so on. For instance, Huang [32] presents a parallel image compression-encryption technique. His method involves splitting the plain image into some smaller images, which are then linearly compressed using one-dimensional compressive sensing. Some quantized measurement value matrix operations, including substitution, permutation and block-wise XOR, produce the final encryption image. However, Huang's technique necessitates transmission loads and additional storage space due to the Gaussian random matrix utilized as the secret encryption keys. Therefore, a key-controlled partial Hadamard matrix [48, 50] was used to solve this problem. The simple image is compressed using the chaos-based measurement matrix [22, 33, 34], structurally random matrix [35], and weighting matrix [36]. Additionally, as various plain images correlate to distinct key streams, the counter mode [37, 38], hash function [22, 39], and plaintext eigenvalue [40] are used in the encryption phase to defend against plaintext analysis-based security attack models. The CS-based image encryption scheme stated above can prevent image data from leaking but cannot offer visual protection. Therefore, provided a workable framework for concurrent steganography and encryption, known as an encryption-embedding system [41]. The plain image is first encrypted using an already-in-use encryption technique to produce a cipher image that resembles noise or texture. The meaningless cipher image is then broken down and inserted using the lifting wavelet transform (IWT) into a host image accessible to the general public. Without the compression stage, a meaningful cipher image has a four times higher resolution than a plain image, increasing the needless expense of storage and transmission. Later, some enhanced visually relevant image encryption methods [42–46] were successively presented. For instance, in [47], First, a block-wise compressive sensing technique and a coefficient random scrambling strategy are used to encrypt and compress the plain image. Then, using the resilient singular value decomposition embedding approach, the worthless cipher image is inserted into a cover image. Furthermore, the encryption keys are updated by the counter mode to protect against specific plaintext attacks.

Through the above discussion, in this paper, an encryption mechanism was designed to compress and encrypt the images. The initial values of the chaos are calculated by dividing the image into four parts, and from each part, calculate one value, which can be used as keys for the algorithm. The encryption operations are related to the plain image. Sparse the image by DWT, then use FAN transform to shuffle all pixels. The original image was divided into blocks. Compress each block by using BCS. The COOT optimization algorithm is used to generate the best MM. Through this, the Compressive sensing was improved. The blocks are masked to one image and shuffled using the COOT optimization algorithm. Finally, uniform pixel value by diffusion is used to get the final encrypted image. The following points can describe the contribution of the proposed encryption system: –

- Designing highly efficient Block Compressive Sensing increases the reconstruction speed and decreases complexity.
- Using COOT optimization in scrambling to get the minimum correlation between pixels to increase security.
- Generating the initial keys from the four parts division of the image (one key from each part) will give different keys for each image so that it will give different encryption for each image.

The remains of this paper are as follows: Section 2 describes Block Compressive Sensing (BCS), Section 3 represents the logistic map, Section 4 describes Chen's chaotic system, and Section 5 the COOT optimization algorithm is described. Section 6 presents the proposed CS algorithm, Section 7 demonstrates the evaluation result obtained, and the conclusion of this research is given in Section 8.

2 Block Compressive Sensing (BCS)

The main idea of Compressive Sensing is to take fewer samples than required by the Nyquist-Shannon method. The signal sparsity and low correlation are necessary for CS performance. After sampling, the original signal can be reconstructed in the receiver. At first the signal N × 1 sparsely can be represented as linear combination of $\Psi = [\Psi 1, \Psi 2, \Psi 3 \ldots \Psi N]$ by

$$X = \Psi s \tag{1}$$

Where Ψ is a transform matrix, s is a sparse vector with several nonzero values. When sprsing the signal in the transforming domain, the y vector can be obtained.

$$\mathrm{y} = \Phi \mathrm{x} = \Phi \Psi \mathrm{s} = \mathrm{As} \tag{2}$$

The measurement matrix (MM) is key for the CS. MM and transforming matrix are incoherent [20]. Retrieve the original signal from y turned to the convex problem as

$$\mathrm{Minimize} \|s\| 1 \quad \text{subject to } \mathrm{y} = \Phi \Psi \mathrm{s} \tag{3}$$

Due to the large size of the image, traditional compressive sensing is complex and slow in processing, so it uses BCS [40].

3 The Logistic Map (LM)

Chaos is helpful for image encryption by generating random numbers. The dimension logistic map is defined as:

$$\mathrm{M}_{\mathrm{n}+1} = \mathrm{M}_{\mathrm{n}} \times \mathrm{u} \times (1 - \mathrm{M}_{\mathrm{n}}) \tag{4}$$

Where u ∈ [0, 4] and n is the chaos iteration, and $3.5690 < \mathrm{u} \leq 4$, Mn is the chaos number.

The logistic map can get the chaotic state quickly and easily. The random numbers were generated by the logistic map used for the diffusion process.

4 Chen Chaotic System

In this system can calculate the random numbers by the following equations:

$$\left.\begin{array}{c} \mathrm{X} = \alpha \times (\mathrm{Y} - \mathrm{X}) \\ \mathrm{Y} = (\delta - \alpha) \times \mathrm{X} - \mathrm{X} \times \mathrm{Z} + \delta \times \mathrm{Y} \\ \mathrm{Z} = \mathrm{X} \times \mathrm{Y} - \beta \times \mathrm{Z} \end{array}\right\} \tag{5}$$

Using these system equations, an image encryption sequence of random integers is obtained, where $\alpha = 35$, $\beta = 3$, and d = 28 are the control parameters.

5 Coot Optimization Algorithm

The COOT water bird belongs to the rail family; there are several behaviours and movements in the water for the coot bird. The bird behaviour in the water is used for a new optimization algorithm. The coot bird behaviour in the water includes two movements: a disordered movement and a synchronized movement. The coot performs a chain of movements on the water's surface, and every coot goes through the coot in front of it. The whole group heads towards the goal (food) by a group of leaders. So, the coots have four different movements in the water, as the following [48]:

A. Random movement between the right and left side

A new random location can be obtained within the search space through Equation (6), and move the coots toward the random location to perform this movement.

$$\mathrm{q} = \mathrm{Rand}(1, \mathrm{d}) \times (\mathrm{ub} - \mathrm{lb}) + \mathrm{lb} \tag{6}$$

ub is the upper bound, lb is the lower bound, Rand is the function for generating a random number

If the algorithm suffers from getting stuck in the local optimal, this will avoid getting stuck in the local optimal. The location of the new coot can be calculated from the following equation:

$$\mathrm{CCPos(i)} = \mathrm{CCPos(i)} + \mathrm{AA} \times \mathrm{RR2} \times (\mathrm{qq} - \mathrm{CCPos(i)}) \tag{7}$$

Where RR2 is a number within [0, 1], Equation (8) calculates AA.

$$\mathrm{AA} = 1 - \mathrm{LL} \times (1/\mathrm{itr}) \tag{8}$$

Where itr is the max iteration, and LL is the present iteration.

B. The Chain Movement

The mean (average) distance between one coot and another can be used to apply this movement, and the new location can be calculated through the following equation.

$$\mathrm{CCPos(i)} = 0.5 \times (\mathrm{CCPos(i-1)} + \mathrm{CCPos(i)}) \tag{9}$$

CCPos(i) is the new position, CCPos(i-1) is the old position

C. Improving the location of coots depending on the location of the leaders

A number of coots lead the groups in front of them, and the other members improve their position depending on the location of the leaders. Equation (10) is applied to determine the leader through which the position is updated

$$k = 1 + mod(1, NL) \tag{10}$$

Depending on the k, the location can be updated using the following equation

$$\begin{aligned}\mathrm{CCPos(i)} &= \mathrm{LLPos(k)} + 2 \times \mathrm{RR1} \times \cos(2 \times \mathrm{RR} \times \pi)\\ &\quad \times (\mathrm{LLPos(k)} - \mathrm{CCPos(i)})\end{aligned} \tag{11}$$

where π is 3.144, RR1 and RR are numbers inside [0, 1], CCPos (i) and LLPos (k) represent the coot and leader positions, respectively.

D. Leaders lead the group to the optimal location.

Lead the group to the best location. As a result, the leaders' group shifts their orientation in relation to the target. Equation (9) is used for updating the leader position. Sometimes, Leaders should move away to find a better location.

$$\mathrm{LLPos(i)} = \left\{\begin{matrix} \mathrm{BB} \times \mathrm{RR3} \times \cos(2 \times \mathrm{RR} \times \pi) \times (\mathrm{gbest} - \mathrm{LLPos(i)}) \\ \quad + \mathrm{gbestRR4} < 0.5 \\ \mathrm{BB} \times \mathrm{RR3} \times \cos(2 \times \mathrm{RR} \times \pi) \times (\mathrm{gbest} - \mathrm{LLPos(i)}) \\ \quad - \mathrm{gbestRR4} >= 0.5 \end{matrix}\right\} \tag{12}$$

Where the best position is LLPos, RR3 and RR4 are numbered within [0, 1], and BB is found by Equation (13).

$$\mathrm{BB} = 2 - \mathrm{L} \times (1/\mathrm{itr}) \tag{13}$$

We are eliminating local optimal because 2 × R3 makes more significant movements. Cos(2Rπ) to search for the best solution with another radius to get a better solution.

6 The Proposed Optimized Encryption System

This algorithm uses the COOT algorithm to find the best measurement matrix (MM). The original image's discreet wavelet transform (DWT) is calculated and scrambled using the FAN transform. Lorenz chaos is used to generate two matrices with FAN transform. The sparsed image was separated into blocks size 64 × 64. A mask is made for all blocks to get one compressed image. Quantify the compressed image. Use a logistic map to generate sequence chaos numbers for diffusing the image. Divide the original image into four parts and take the first five pixels from each part to compute the initial values

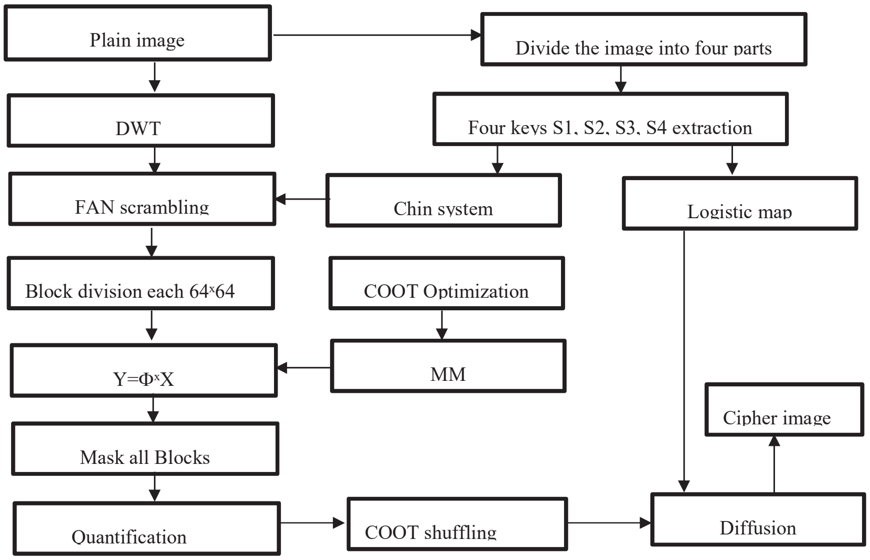


Figure 1 Represent the block diagram of the encryption system.

S1, S2, S3, and S4 for chin chaotic and logistic maps. This will be explained in the following procedure: –

1. Obtain the natural image size 256×256 pixels
2. Sparse the natural image by DWT

$$\mathrm{ImgSp} = \Psi \times \mathrm{image} \times \Psi' \tag{14}$$

3. Threshold the sparsed image by the following equation

$$Imgth(abs\ (imgSp) <= 20 \tag{15}$$

4. Generate two random matrices using chin chaotic to scramble the sparsed image using FAN transform.

$$\mathrm{ImgF} = \mathrm{FAN\ transformation\ (Imgth)} \tag{16}$$

5. Divide the sparsed image into blocks, each size of 64×64 pixels.
6. Find the optimal solution for the MM(measurement matrix) by using the COOT optimization algorithm using the following objective function:

$$\mathrm{max{:}\ (E) = entropy\ (MM)} \tag{17}$$

Where the MM represents the solution from the COOT algorithm

7. Compress each block of the image by using the MM to get the compressed block as the following equation:

$$\mathrm{Y} = \Phi \times \mathrm{ImgF} \tag{18}$$

8. Mask all blocks to get one compressed image.
9. Quantify the compressed image to get pixel values between [0-255].

$$\mathrm{img\_en} = \mathrm{round}\ (255 \times (\mathrm{Y} - \mathrm{Ymin})/(\mathrm{Ymax} - \mathrm{Ymin})) \tag{19}$$

10. Shuffling the image by COOT algorithm as the following

    a. Convert the image to one dimension.
    b. Generate the initial population for COOT by Equation (6).
    c. Take a vector from the COOT algorithm size equal to the image size.
    d. Sort ascending the solution vector from COOT and take its index as a vector
    e. Scramble the image by using the index to get the scrambled image.
    f. Check the image correlation to select the best solution from the COOT algorithm by the following objective function.

$$\mathrm{Min}\ (\mathrm{z}) = \mathrm{correlation}(\mathrm{Y}) \tag{20}$$

    g. Update the locations of each member to get a better solution by Equations (7), (9), (11) and (12).
    h. Continue until the end of iterations.
    i. Get the optimal solution for the COOT optimization.
    j. Scramble the image by using the optimal solution from the COOT optimization algorithm.

11. Obtain the four keys for chin chaotic and logistic map as the following steps:

    a. Divide the original image into four parts
    b. Take the first five pixels from each part
    Pi = [Pi1, Pi2, Pi3, Pi4, Pi5] decimals values
    c. convert the value of each pixel to binary
    d. B= [Pi1,1, Pi1,2, Pi1,3,. . . Pi2, 1, Pi2,3, . . . Pi5,7, Pi5,8] binary
    e. Compute the keys S1, S2, S3 and S4 by the following equation

$$S_k = \frac{p_{i1,1}{}^{\times}2^{39} + p_{i1,2}{}^{\times}2^{38} + \cdots + p_{i2,2}{}^{\times}2^{31} + \cdots p_{i5,6}{}^{\times}2^{2} + p_{i5,8}{}^{\times}2^{0}}{2^{40}} \tag{21}$$

Where k is 1, 2, 3, and 4

7 Decryption Process

During the decryption process, encryption operations are carried out but in reverse, where the keys generated in the encryption process are exchanged to generate keys during decryption. Chaos numbers are generated using the logistic map to decrypt the diffusion. Then, the confusion is decrypted through the same sequence done in encryption using the COOT optimization algorithm. MM Matrix is received from the transmitter to be used with the OMP algorithm to reconstruct the image and recover the shuffled image using the FAN Transform. Finally, apply the IDWT to retrieve the image.

8 Efficiency Evaluation

This part presents practical experiments. The process was done using Win 11 with the MATLAB 2021 platform. Orthogonal Matching Pursuit (OMP) is the algorithm for recovering compressed images in decryption. The compression ratio is 0.5, and the size of each block is 64×64, while the size of all images is 256×256.

8.1 The Results of The Encryption and Decryption

Five grayscale images of size 256×256 were used. All images are compressed to half-size after the encryption process. The cipher is in the form of noise that is not similar to the original image. In addition to that, the images that are decrypted are identical to the original images without noise.

Peak Signal-to-Noise Ratio (PSNR) can be calculated through the following equation:

$$\mathrm{PSNR} = 10 \times \log 10[255^2/\mathrm{sqr}\ (\mathrm{MSE})] \tag{22}$$

Where (MSE) is the mean square error and a high-quality image has a minimal MSE value. The following equation can compute it:

$$\mathrm{MSE} = (1/\mathrm{M}^{\mathrm{x}}\mathrm{N}) = \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} [\mathrm{PP}(\mathrm{i},\mathrm{j}) - \mathrm{DD}(\mathrm{i},\mathrm{j})]^2 \tag{23}$$

Where PP represents the input image, DD represents the reconstructed image, the height is M, and the width is N. The following equation can calculate the similarity between the images.

$$SSIM(PP, DD) = \frac{2uPP^{\mathrm{x}}uDD + CC1}{u^2PP + u^2DD + CC1}$$

$$\times \frac{2\sigma PP^{\mathrm{x}}\sigma DD + CC2}{\sigma^{2}PP + \sigma^{2}DD + CC2}$$

$$\times \frac{\sigma PPDD + CC3}{\sigma PP\sigma DD + CC3} \tag{24}$$

$$MSSIM(PP, DD) = \frac{1}{w} \times \sum_{i=1}^{w} SSIM(PPi, DDi) \tag{25}$$

Where W = 64, PP is an input image, DD is the retrieved image, μPP is the average of PP, μDD is the mean of PP, σDD is the variance of DD, σPP is the variance of PP, the covariance between PP and DD is σPPDD. Also, CC1, CC2, CC3 are three constants CC1 = (K1 × L)2, CC2 = (K2 × L)^{2}, CC3 = CC2/2, LL = 255, KK1 = 0.01 and KK2 = 0.03.

In Table 1, the PSNR was greater than 30 dB and MSSIM was greater than 0.90; from this, the method has a good effect on image recovery. Table 2 shows the comparison with other methods.

8.2 Keyspace Analysis

Keyspace is the probabilities of the keys to protect data against different types of attacks. The range of the key should be equal to more than 2^{100}. The keys include the parameters μ, S1, S2, S3, and S4 for chaos. The accuracy is 10^{-15}, and the critical space is 2^{249}. The essential space is more significant than 2^{100}, in Table 3. The proposed system is better than the methods because it has a more significant key space.

Table 1 Show the comparison with other methods

	MAP	PSNR	MSSIN
Lena image	194.9949	35.2873	0.9898
Cameraman image	245.4678	35.0474	0.9931
House image	123.0511	36.4442	0.9925
Peppers image	162.7851	35.4095	0.9847
Aircraft image	284.5353	34.0322	0.9828

Table 2 The PSNR results compared with other methods

Ref. [49]	Ref. [40]	Ref. [50]	Ref. [22]	Proposed
34.55600	33.22990	33.84620	23.36080	35.28730

Table 3 Show the comparison with other methods

	Ref. [50]	Ref. [47]	Ref. [51]	Proposed
Keyspace	2^{149}	2^{197}	2^{232}	2^{249}

Table 4 Measurement for the encrypted images

Keys	(NPCR)	(UACI)
correct-key	0	0
S1+10-15	90.1886	26.8148
S2+10-15	91.4215	28.0129
S3+10-15	90.0513	31.9315
S4+10-15	90.9302	29.3813
μ+10-15	90.0787	31.5661

8.3 The Sensitivity of the Key

The encrypted image can be changed to a different image through a slight change in the key. Therefore, this method is compassionate, especially if there is a slight difference between the wrong and right keys. The image cannot be retrieved with a different key.

$$NPCR = \frac{1}{M \times N} \times \sum_{i=1}^{M} \sum_{j=1}^{N} D(x, y) \times 100\% \tag{26}$$

$$UACI = \frac{1}{N \times M} \times \sum_{x=1}^{M} \sum_{y=1}^{N} \frac{|CC1(x, y) - CC2(x, y)|}{255} \times 100\% \tag{27}$$

$$\mathrm{DD(x, y)} = \begin{Bmatrix} 1, & CC1(x, y) \neq CC2(x, y) \\ 0, & CC1(x, y) = CC2(x, y) \end{Bmatrix}$$

Where NPCR is Number of Pixels Change Rate and UACI is Unified Average Changing Intensity.

8.4 Histogram Analysis

The original image carries redundant information, so the histogram is volatile. The best image that withstands attacks is the one that has a uniform distribution of histograms. As in Figure 2, despite the difference in the original images, all the encrypted images have the same distribution of histograms. This means that the encrypted image does not have any helpful information and enables it to withstand statistical attacks.

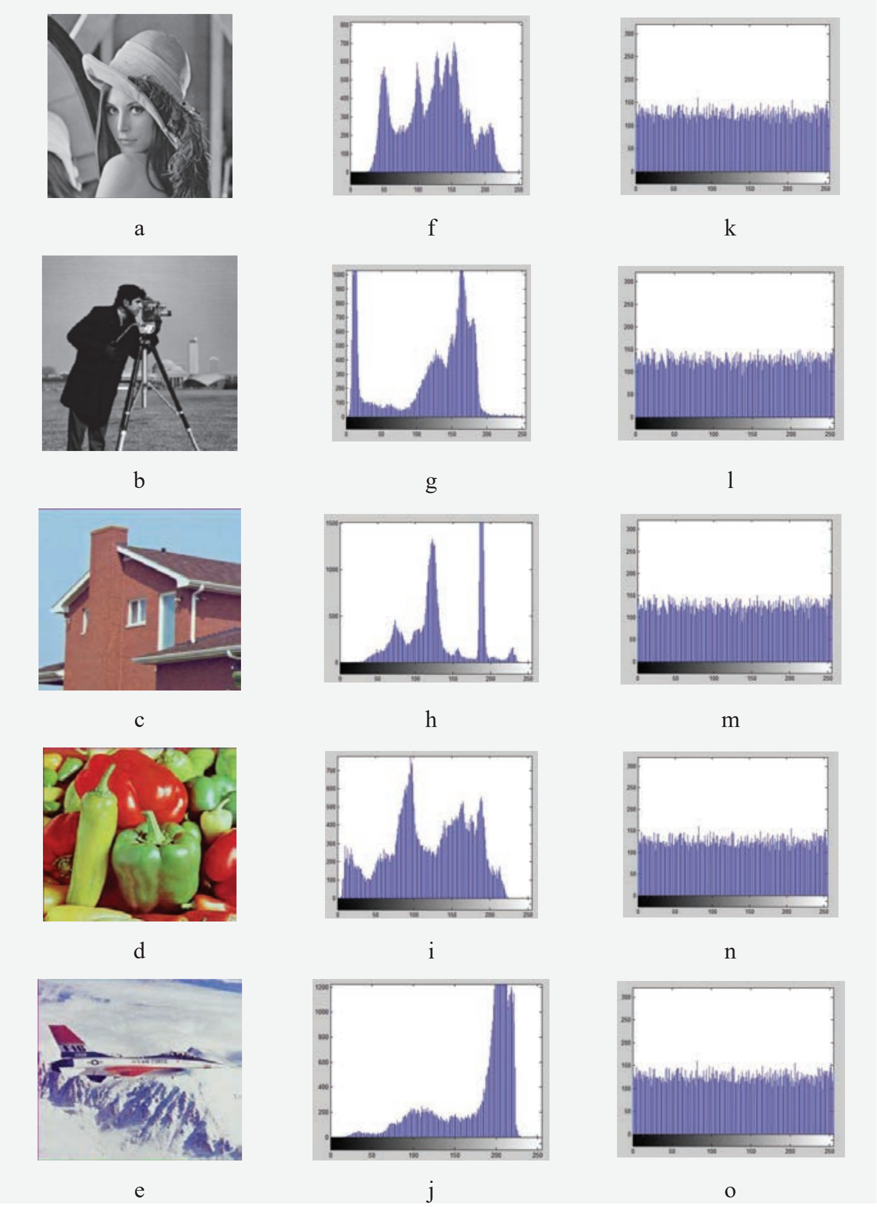


Figure 2 The original images are a, b, c, d, and e; the distribution of the original image are f, g, h, i, and j; the cipher images distribution is k, l, m, n, and o.

Table 5 The correlation coefficient between adjacent pixels

	H		V		D	
	Original	Cipher	Original	Cipher	Original	Cipher
Lena image	0.9456	−0.0026	0.9727	0.0040	0.9213	−0.0009
Cameraman image	0.9544	0.0068	0.9726	0.0059	0.9326	−0.0013
House image	0.9782	0.0025	0.9529	−0.0010	0.9361	0.0026
Peppers image	0.9639	−0.0070	0.9709	−0.0041	0.9373	0.0004
Aircraft image	0.9369	−0.0007	0.9307	0.0009	0.8830	0.0038

Table 6 The correlation coefficient compared with other algorithms

Algorithms	H	V	D
Ref. [50]	0.0018**0**	0.0014**0**	0.0034**0**
Ref. [40]	−0.0029**0**	0.0058**0**	−0.0025**0**
Ref. [33]	−0.0016**0**	0.0010**0**	−0.0015**0**
proposed	−0.0026**0**	0.0040**0**	−0.0009**0**

8.5 Correlation Coefficient Analysis

The perfect encryption algorithm breaks the correlation between pixels. It is used to evaluate the correlation between pixels. It can be calculated from the following equation:

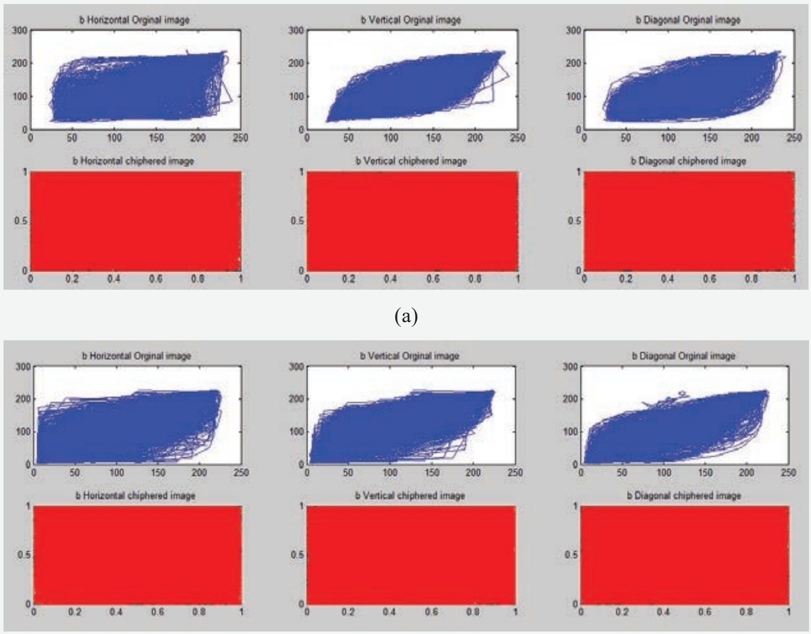
$$p_{xy} = \frac{\sum_{i=1}^{N}(xi - xx)(yi - yy)}{\sqrt{(\sum_{i=1}^{N}(xi - xx)^2)(\sum_{i=1}^{N}(yi - yy)^2)}} \tag{28}$$

Where $xx = \frac{1}{N}\sum_{1}^{N} x, = \frac{1}{N}\sum_{1}^{N} y$, the total number of pixels is N. The encrypted image's ideal correlation value is 1, close to zero. The encryption strongness increases as the correlation value is near to zero. In Table 5. The correlation was found near to zero. Table 6 was compared the encryption algorithm with other algorithms.

8.6 Information Entropy Analysis

A test that checks for unpredictability and randomness. In image encryption, the encrypted image with a high entropy value is better than that with a low one. Information Entropy can be calculated from the following equation:

$$H(m) = \sum_{i=0}^{2^n-1} p(mi)log_2\frac{1}{p(mi)} \tag{29}$$



(a)

(b)

Figure 3 shows the correlation of two plain and encrypted images, (a) Lena and (b) cameraman.

Table 7 Entropy for both cipher and original image

	Lena Image	Cameraman Image	House Image	Peppers Image	Aircraft Image
original images	7.4318	7.0442	6.4961	7.5770	6.7294
encrypted images	7.9948	7.9940	7.9939	7.9937	7.9942

Where image information is m, mi is the probability of p (mi). The entropy values were calculated in Table 7. shows the entropy value was near to 8. Through the result, it was found that the encrypted images have a high randomness.

8.7 Security Analysis

8.7.1 The occlusion attack

Occlusion attack occurs during the image transmission; some pixels are exposed to different intensities in different parts of the images. This method

Table 8 Show the PSNR values when SPN and SN noise are added to the decrypted image

			0.00001	0.00003	0.00005	0.00007
SPN	PSNR	Lena image	34.9015	35.0364	34.7838	34.8739
		Cameraman image	34.6264	34.8478	34.0778	34.8567
			0.000001	0.000002	0.000003	0.000004
SN	PSNR	Lena image	28.7281	28.2467	28.0572	28.3483
		Cameraman image	28.8167	28.4849	28.2496	27.8469

Table 9 NPCR and UACI data for this Algorithm

Images	NPCR	UACI
Lena	94.4397	19.5593
Cameraman	99.4873	37.9183
Pepper	99.2188	36.4080
Aircraft	99.2981	34.5548
House	99.7009	40.5569

can decrypt the encrypted image despite exposure to occlusion attack and retrieve the original image well. Figure 4 shows how to retrieve images exposed to noise, and the recovery of the encrypted image is weak with the increase in the loss within the image.

8.7.2 The noise attack

The intensity of 0.00001, 0.00003, 0.00005, and 0.00007 of Salt and Pepper Noise (SPN) are added to the encrypted images, and the intensity of 0.000001, 0.000002, 0.000003, and 0.000004, of Speckle Noise (SN) are added to the encrypted image too. Table 8 shows the PSNR values for decrypted images. Through this test, the value of PSNR is greater than 30 dB when exposed to SPN from 0.00001 to 0.00007. It can withstand SPN.

8.8 The Resistance Against Differential Attack

This algorithm demonstrates strong cryptographic properties as evidenced by NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changing Intensity) tests in Table 9. The algorithm's sensitivity to plaintext modifications and resistance to differential attacks are attributed to its use of random initial conditions. This randomness ensures that even identical plaintexts produce unique encrypted outputs. Further comparisons with other algorithms can be found in Table 10.

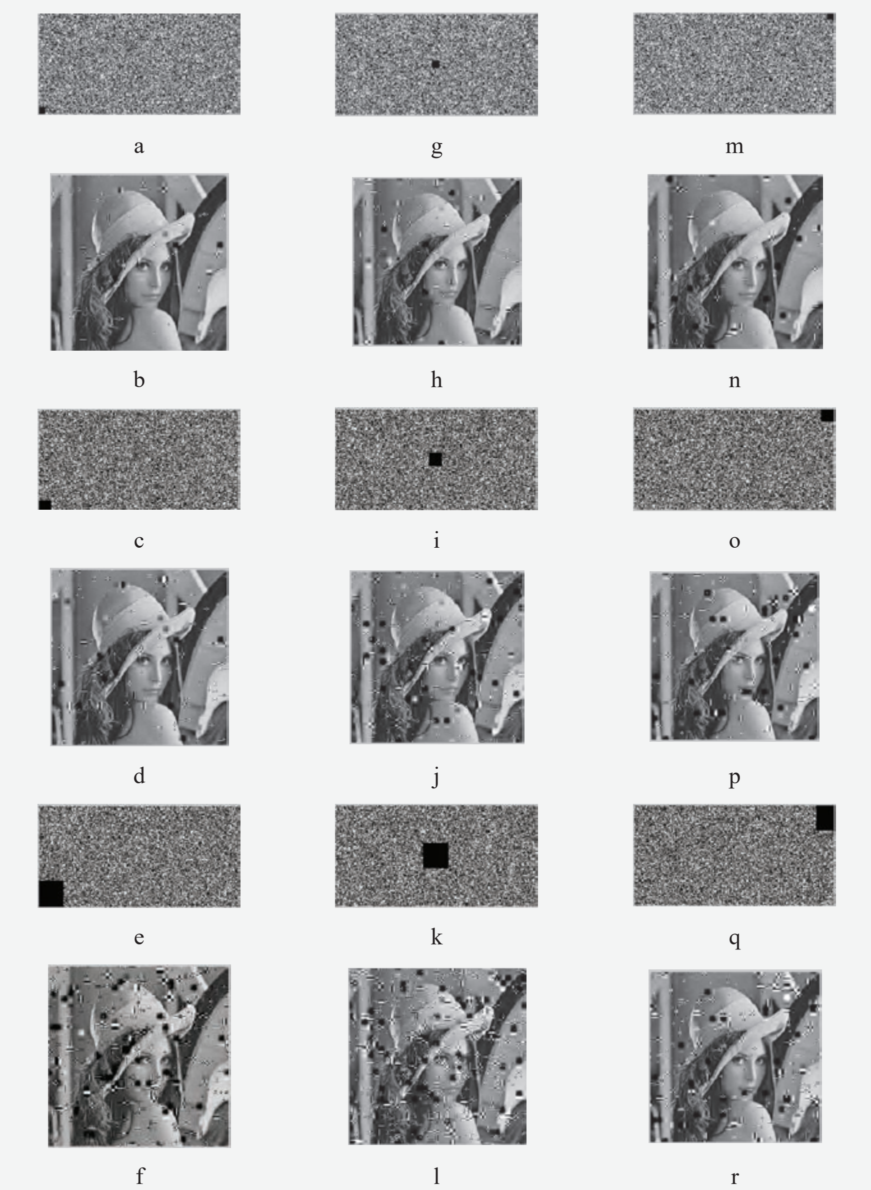


Figure 4 The result of the decrypted images that have an occlusion attack; the encrypted images have lost data with blocks ($8^{\times}8$), ($16^{\times}16$), and ($32^{\times}32$) from lower left, middle, and upper right parts of the image.

Table 10 This analysis compares the NPCR and UACI values of this algorithm with other algorithms to assess its resistance to differential attacks

Image	Ref	NPCR	UACI
Camera-man	Ref [52]	99.6185	33.3882
	Ref [54]	99.6122	33.4513
	Proposed	99.4873	37.9183
Lena	Ref [52]	99.5804	33.4533
	Ref [54]	99.6098	33.4536
	Ref [53]	99.228	30.147
	Proposed	94.4397	19.5593
Peppers	Ref [53]	99.167	30.667
	Ref [54]	99.6108	33.5173
	Proposed	99.2188	36.4080

8.9 Evaluation of Algorithm Execution Time

This method breaks down into four stages: confusion (DWT domain), compressing (compressive sensing), diffusion (spatial domain) and scrambling (optimization). To assess how long it takes to run (execution time or ET), Lena's image was used. The initial steps, including generating secret keys and performing confusion and scrambling, are relatively quick. The majority of the time is spent on the scrambling stage using the optimization algorithm in the DWT domain. In total, the entire encryption process takes 6.599242 seconds.

9 Conclusion

A new image encryption method was designed based on an effective compressive block. Using such an encryption system for data protection resulted in the reduction of the size of redundant data. The CS was applied to each image block where each block was of a size 64×64 pixels. Testing such encryption system have shown that it was faster and had a better quality in encryption and decryption processes. In addition, the scrambling by the COOT optimization algorithm removed the correlation between pixels and improved image reconstruction. The diffusion by random numbers used here that a logistic map has generated resulted in uniform pixel values, and the system could resist the statistical attacks. Using the original image to generate the initial parameters resulted in different initial values for each image, giving different initial values that enhanced the resistance against chosen-plaintext attack and known-plaintext attack. This method possessed a high sensitivity and a large key space compared to other traditional works.

References

[1] X. Gao, 'Image encryption algorithm based on 2D hyperchaotic map', Opt Laser Technol, vol. 142, p. 107252, 2021.

[2] M. Li, D. Lu, Y. Xiang, Y. Zhang, and H. Ren, 'Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion', Nonlinear Dyn, vol. 96, pp. 31–47, 2019.

[3] Q. K. Abed and W. A. M. Al-Jawher, 'A Robust Image Encryption Scheme Based on Block Compressive Sensing and Wavelet Transform', International Journal of Innovative Computing, vol. 13, no. 1–2, pp. 7–13, 2022.

[4] J. Chen, L. Chen, and Y. Zhou, 'Cryptanalysis of a DNA-based image encryption scheme', Inf Sci (N Y), vol. 520, pp. 130–141, 2020.

[5] J. Song and Y. H. Lee, 'Optical image encryption using different twiddle factors in the butterfly algorithm of fast Fourier transform', Opt Commun, vol. 485, p. 126707, 2021.

[6] C. Chen, K. Sun, and S. He, 'An improved image encryption algorithm with finite computing precision', Signal Processing, vol. 168, p. 107340, 2020.

[7] W. A. Mahmoud and I. K. Ibraheem, 'Image denoising using stationary wavelet transform', Advances in Modelling and Analysis-B-, vol. 46, no. 3/4, pp. 1b–18b, 2003.

[8] A. H. M. Al-Heladi, W. A. Mahmmoud, H. A. Hali, and A. F. Fadhel, 'Multispectral Image Fusion using Walidlet Transform', Advances in Modelling and Analysis B, vol. 52, no. 1–2, pp. 1–20, 2009.

[9] W. A. Mahmoud and A. L. M. Rasheed, '3D Image Denoising by Using 3D Multiwavelet', AL-Mustansiriya J. Sci, vol. 21, no. 7, pp. 108–136, 2010.

[10] W. A. Mahmoud and M. R. Shaker, '3D Ear Print Authentication using 3D Radon Transform', in 2006 2nd International Conference on Information & Communication Technologies, IEEE, 2006, pp. 1052–1056.

[11] W. A. Mahmoud, M. E. Alneby, and W. H. Zayer, '2D-multiwavelet transform 2D-two activation function wavelet network based face recognition', J. Appl. Sci. Res, vol. 6, no. 8, pp. 1019–1028, 2010.

[12] D. L. Donoho, 'Compressed sensing', IEEE Trans Inf Theory, vol. 52, no. 4, pp. 1289–1306, 2006.

[13] A. H. Kattoush, W. A. Mahmoud, A. Shaheen, and A. Ghodayyah, 'The performance of proposed one dimensional serial Radon based OFDM system under different channel conditions', The International Journal of Computers, Systems and Signals, vol. 9, no. 2, pp. 3–16, 2008.

[14] W. A. Al-Jawher, 'New fast method for computing multiwavelet coefficients from 1D up to 3D', in Proc. 1st Int. Conference on Digital Comm. & Comp. App., Jordan, 2007, pp. 412–422.

[15] A. H. Kattoush, W. A. M. Al-Jawher, and O. Q. Al-Thahab, 'A radon-multiwavelet based OFDM system design and simulation under different channel conditions', Wirel Pers Commun, vol. 71, pp. 857–871, 2013.

[16] W. A. Mahmoud, 'A Smart Single Matrix Realization of Fast Walidlet Transform', International Journal of Research and Reviews in Computer Science, vol. 2, no. 1, p. 144, 2011.

[17] W. A. Mahmoud, M. S. Abdulwahab, and H. N. Al-Taai, 'The Determination of 3D Multiwavelet Transform', IJCCCE, vol. 2, no. 4, 2005.

[18] M. H. M. Hasan, W. A. A. Jouhar, and M. A. Alwan, '3-d face recognition using improved 3d mixed transform', Int J Biom Bioinformatics, vol. 6, no. 1, p. 278, 2012.

[19] W. Al-Jouhar and T. Abbas, 'Feature combination and mapping using multiwavelet transform', Iraq Academic Scientific Journals, vol. 3, no. 19, pp. 13–34, 2006.

[20] Y. Rachlin and D. Baron, 'The secrecy of compressed sensing measurements', in 2008 46th Annual Allerton conference on communication, control, and computing, IEEE, 2008, pp. 813–817.

[21] L. Y. Zhang, K.-W. Wong, Y. Zhang, and J. Zhou, 'Bi-level protected compressive sampling', IEEE Trans Multimedia, vol. 18, no. 9, pp. 1720–1732, 2016.

[22] L. Gong, K. Qiu, C. Deng, and N. Zhou, 'An image compression and encryption algorithm based on chaotic system and compressive sensing', Opt Laser Technol, vol. 115, pp. 257–267, 2019.

[23] W. Cao, Y. Mao, and Y. Zhou, 'Designing a 2D infinite collapse map for image encryption', Signal Processing, vol. 171, p. 107457, 2020.

[24] Z. Hua and Y. Zhou, 'Exponential chaotic model for generating robust chaos', IEEE Trans Syst Man Cybern Syst, vol. 51, no. 6, pp. 3713–3724, 2019.

[25] P. Ping, F. Xu, Y. Mao, and Z. Wang, 'Designing permutation–substitution image encryption networks with Henon map', Neurocomputing, vol. 283, pp. 53–63, 2018.

[26] X. Wang and N. Guan, 'A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation', Opt Laser Technol, vol. 131, p. 106366, 2020.

[27] W. Wen, K. Wei, Y. Zhang, Y. Fang, and M. Li, 'Colour light field image encryption based on DNA sequences and chaotic systems', Nonlinear Dyn, vol. 99, pp. 1587–1600, 2020.

[28] P. K. Naskar, S. Bhattacharyya, D. Nandy, and A. Chaudhuri, 'A robust image encryption scheme using chaotic tent map and cellular automata', Nonlinear Dyn, vol. 100, pp. 2877–2898, 2020.

[29] B. Mondal, S. Singh, and P. Kumar, 'A secure image encryption scheme based on cellular automata and chaotic skew tent map', Journal of information security and applications, vol. 45, pp. 117–130, 2019.

[30] X.-Y. Wang and Z.-M. Li, 'A color image encryption algorithm based on Hopfield chaotic neural network', Opt Lasers Eng, vol. 115, pp. 107–118, 2019.

[31] F. Yang, J. Mou, Y. Cao, and R. Chu, 'An image encryption algorithm based on BP neural network and hyperchaotic system', China Communications, vol. 17, no. 5, pp. 21–28, 2020.

[32] R. Huang, K. H. Rhee, and S. Uchida, 'A parallel image encryption method based on compressive sensing', Multimed Tools Appl, vol. 72, pp. 71–93, 2014.

[33] L. Zhu, H. Song, X. Zhang, M. Yan, L. Zhang, and T. Yan, 'A novel image encryption scheme based on nonuniform sampling in block compressive sensing', IEEE Access, vol. 7, pp. 22161–22174, 2019.

[34] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, 'Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing', Opt Laser Technol, vol. 82, pp. 121–133, 2016.

[35] A. Souyah and K. M. Faraoun, 'Fast and efficient randomized encryption scheme for digital images based on quadtree decomposition and reversible memory cellular automata', Nonlinear Dyn, vol. 84, no. 2, pp. 715–732, 2016.

[36] H. Zhao, H. Ye, and R. Wang, 'The construction of measurement matrices based on block weighing matrix in compressed sensing', Signal Processing, vol. 123, pp. 64–74, 2016.

[37] G. Hu, D. Xiao, Y. Wang, and T. Xiang, 'An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications', J Vis Commun Image Represent, vol. 44, pp. 116–127, 2017.

[38] G. Hu, D. Xiao, Y. Wang, T. Xiang, and Q. Zhou, 'Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes', Opt Lasers Eng, vol. 98, pp. 123–133, 2017.

[39] R. Ponuma and R. Amutha, 'Compressive sensing based image compression-encryption using novel 1D-chaotic map', Multimed Tools Appl, vol. 77, pp. 19209–19234, 2018.

[40] Z. Gan, X. Chai, J. Zhang, Y. Zhang, and Y. Chen, 'An effective image compression–encryption scheme based on compressive sensing (CS) and game of life (GOL)', Neural Comput Appl, vol. 32, pp. 14113–14141, 2020.

[41] L. Bao and Y. Zhou, 'Image encryption: Generating visually meaningful encrypted images', Inf Sci (N Y), vol. 324, pp. 197–207, 2015.

[42] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, 'A visually secure image encryption scheme based on compressive sensing', Signal Processing, vol. 134, pp. 35–51, 2017.

[43] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, 'An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding', Opt Lasers Eng, vol. 124, p. 105837, 2020.

[44] J. S. Khan et al., 'DNA and plaintext dependent chaotic visual selective image encryption', IEEE Access, vol. 8, pp. 159732–159744, 2020.

[45] G. Ye, C. Pan, Y. Dong, K. Jiao, and X. Huang, 'A novel multi-image visually meaningful encryption algorithm based on compressive sensing and Schur decomposition', Transactions on Emerging Telecommunications Technologies, vol. 32, no. 2, p. e4071, 2021.

[46] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, 'Image encryption and hiding algorithm based on compressive sensing and random numbers insertion', Signal Processing, vol. 172, p. 107563, 2020.

[47] L. Zhu et al., 'A robust meaningful image encryption scheme based on block compressive sensing and SVD embedding', Signal Processing, vol. 175, p. 107629, 2020.

[48] I. Naruei and F. Keynia, 'A new optimization method based on COOT bird natural life model', Expert Syst Appl, vol. 183, p. 115352, 2021.

[49] Y. Luo et al., 'A robust image encryption algorithm based on Chua's circuit and compressive sensing', Signal Processing, vol. 161, pp. 227–247, 2019.

[50] J. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, ‘Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression’, Opt Laser Technol, vol. 99, pp. 238–248, 2018.

[51] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, ‘An image encryption algorithm based on chaotic system and compressive sensing’, Signal Processing, vol. 148, pp. 124–144, 2018.

[52] Z. Bashir, N. Iqbal, and M. Hanif, “A novel gray scale image encryption scheme based on pixels’ swapping operations,” Multimedia Tools and Applications, vol. 80, no. 1, pp. 1029–1054, Sep. 2020, doi: 10.1007/s11042-020-09695-8.

[53] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, and F. Ahmad, “An image encryption approach using particle swarm optimization and chaotic map,” International Journal of Information Technology, vol. 10, no. 3, pp. 247–255, Jan. 2018, doi: 10.1007/s41870-018-0099-y.

[54] X. Wang and M. Zhang, “An image encryption algorithm based on new chaos and diffusion values of a truth table,” Information Sciences, vol. 579, pp. 128–149, Nov. 2021, doi: 10.1016/j.ins.2021.07.096.

Biographies

Qutaiba Kadhim Abed earned a Bachelor from Diyala University in Diyala, Iraq, in 2014 and a Master of Science in Computer Science from Diyala University in Diyala, Iraq, in 2019. Currently, he is a Ph.D. candidate at the Iraqi Commission for Computers and Informatics, Information Institute for Postgraduate Studies in Baghdad, Iraq. His research interests are image encryption, chaos, compressive sensing, and optimization algorithms.

Waleed Ameen Mahmoud Al-Jawher President Assistance for Scientific Affairs, University of Uruk, Iraq. He received a School of Research in Digital Signal Processing (2005). He received his Ph.D. in Digital Signal Processing from the University of Wales, United Kingdom (1986). He has a teaching experience in Computer Science and Communication engineering for 44 years. A total of (15) National Awards. He published over (290) papers and supervised more than (210) MSc and PhD Students. He was the First Professor Award at the University of Baghdad, Iraq. His present areas of research interest are the field of Digital Signal Processing and its applications.