A Chaos Based Joint Image Compression and Encryption Scheme

Subhashini k[1*], *Nandhini k*[2*]

[1]Sri Sairam Engineering College, ECE Department, Chennai, India
[2] Sri Sairam Engineering College, ECE Department, Chennai, India

Abstract. Cryptography is a technique used for secure communications or information in the presence of third parties. This work proposes an Image encryption algorithm using the chaotic map. First, this method is produced to generate the secret key using a logistic map. Encryption includes two processes confusion and diffusion and compression is performed using the DWT method. It has compressed the size of the image.The output verified this method has better security performance.

1 INTRODUCTION

Security is a common issue in multimedia applications like text, image, audio, video, etc.… Cryptography in the modern age was effectively encryption. The sender can send the input image converted to an unreadable format which can only be read by the receiver. The security of image receiving, the LSSE chaotic sequence used for image encryption algorithm is presented [1]. The various indicators can be tested by using chaotic maps and verifying the security performance. This paperuses a chaos method. It was measured for not in time series. This tested result is nearly close to 1. LSSE is based on scrambling Arnold pixels and using XORvalue operations. This process is based on LSSE. Theseexperiments conduct various patterns of key length andthe size of the image is different. This method proposeda chaotic cellular neural network [2]. It is used in various matrix and pcs technology, reducing unnecessary keytransmission. The chaotic cellular neural network toconstruct encryption key streams. Compressive sensingusing discrete signals based on the sampling rate condition. In this proposed logistic mapping is used to combine after permutation [3]. Logistic map based on discrete convolution techniques for the processing of discrete signals. This discrete convolution is represented using the matrix method. In cellular automata, the security level is increased to produce random and chaotic map behavior. They designed the encryption algorithm [4].

*Corresponding author: secp21cs02@sairamtap.edu.in

It compresses image features using convolutional neural networks and also high level. Classification and regression are a variety of tasks to complete these features It performs scrambling control operations for the encryption process. This learning derived the parameters and weights from the image [5].This proposed method is a power-generating key based on image processing techniques. The logistic map and henon maps are the two chaotic maps used in this method. The measurement matrix and scrambling are generated by using a 3D cat map [6]. It is using the LSBmethod to generate an unreadable format image with better quality. The input image is embedded, and compressed and this image size is less. These algebraicstructures are defined in a finite field [8]. Thecompressed image measurement for confusion and diffusion process is based on a chaotic map. The chaotic map is a complete disorder and confusion and analyzes some Indicators like histogram, correlation, Entropy, etc...

2 BLOCK DIAGRAM

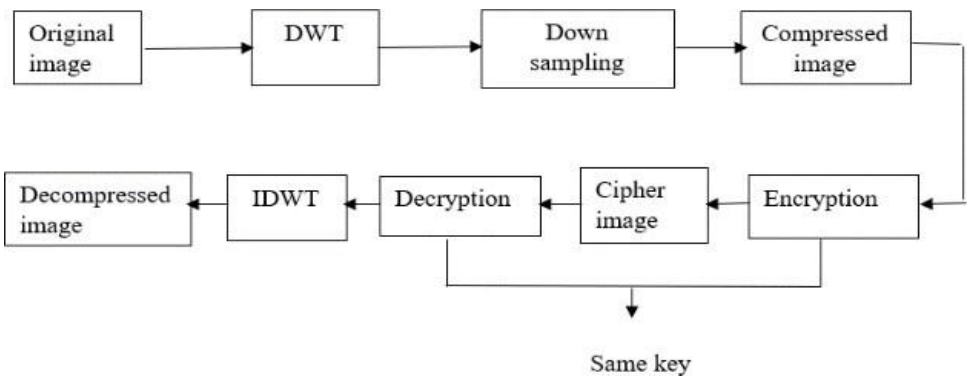

Fig 1. The proposed system of Image encryption and compression

3 PROPOSED METHOD

3.1 ENCRYPTION SCHEME

The proposed method of cryptography uses an encryption process using a chaotic map and a compression process using the DWT method. The input-tested image is taken from the USC-SIPI data set. Two gray input plain images are used as test images.

Step 1**:** Get two grayscale input images to be tested.
Step 2: Get the image size.
Step 3: Assign the number of rows in m and the numberOf columns in n.
Step 4: Generating chaotic map sequences based on thelogistic map. They are selected randomly for initial Values using this method.
Step 5: Confusion and diffusion process is applied in rows.
For k=1:m
sequence value h=h+3
Row 1 is flipped based on sequence value sq1(1)Row 1 is flipped based on sequence value

sq1(2)Row 1 is flipped based on sequence value sq1(3) The flipped rows are processed by XOR operation andget new rows and this process is repeated for all rows. ImR accumulates all new rows.

3.2 COMPRESSION SCHEME

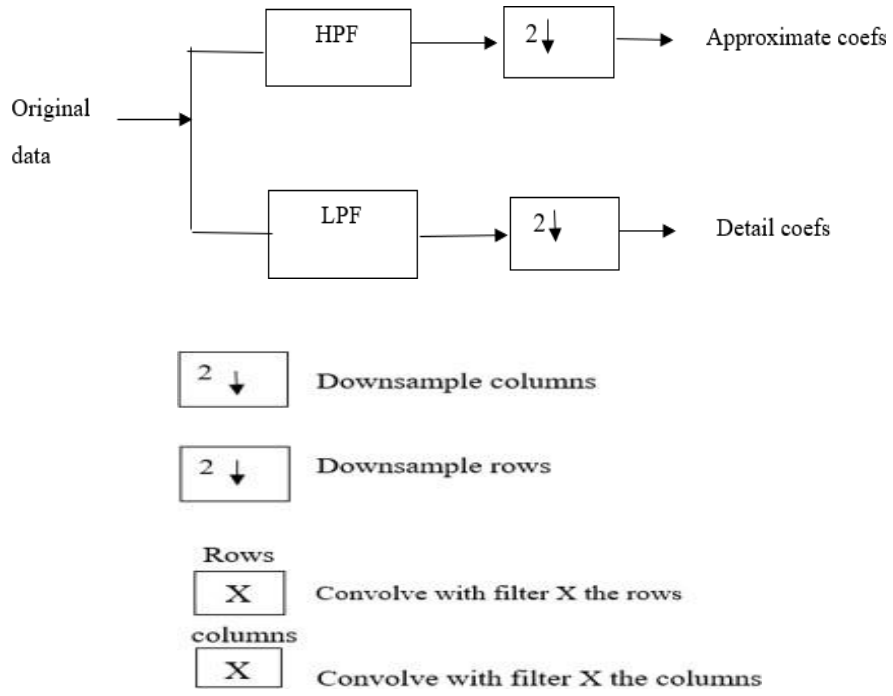

Fig 2. Flow chart of DWT

In this proposed method the input image is compressed using the DWT method. This compression has helped toreduce image pixels and also the size of the file. Two gray input plain images are used as test images. These test images are used for image compression based on theDWT method and the lossy compression technique,which reduces the size of the pixel 128x128.

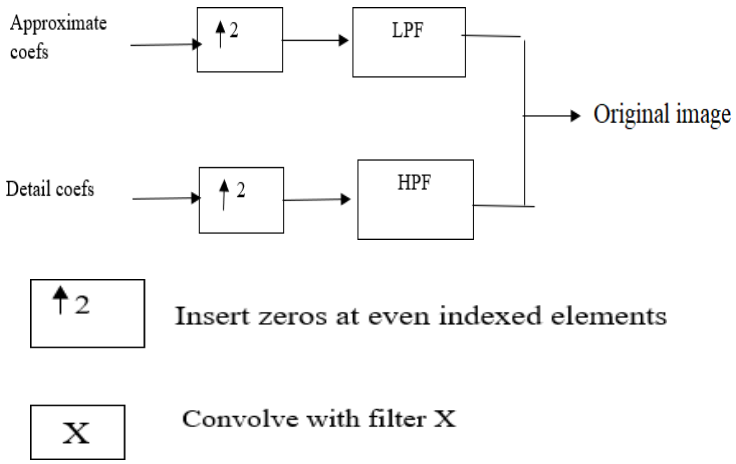

Fig 3. Flow chart of IDWT

4 Experimental Output

The proposed method is tested in the MATLAB 2020a platform. The tested input images mandril, a boat sizeis 512x512.

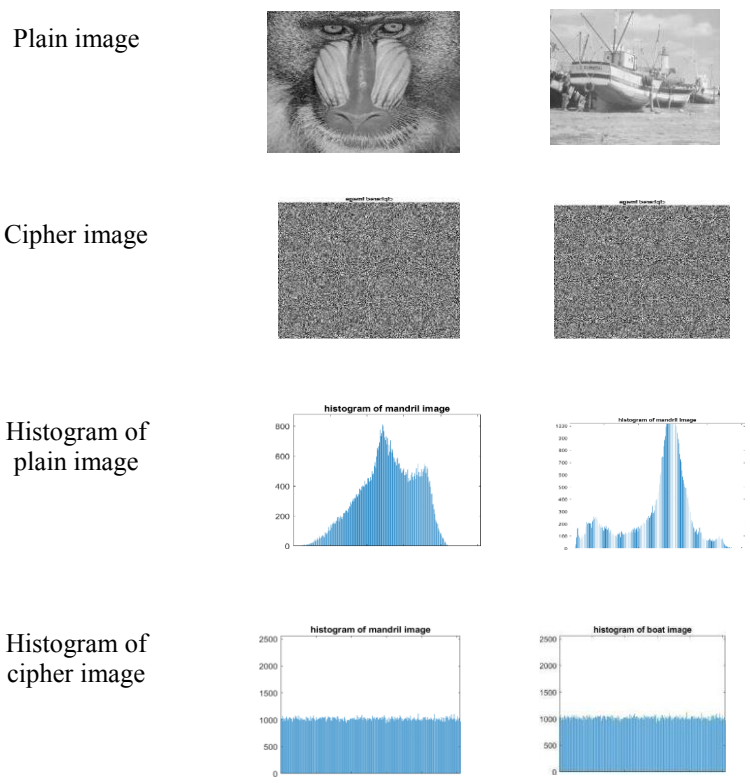

Fig 4. Input Image and Ciphered Image Output

The proposed map is an encrypted input and this process produces an unreadable format image and the histogram is analyzed for both the input image and encrypted image.

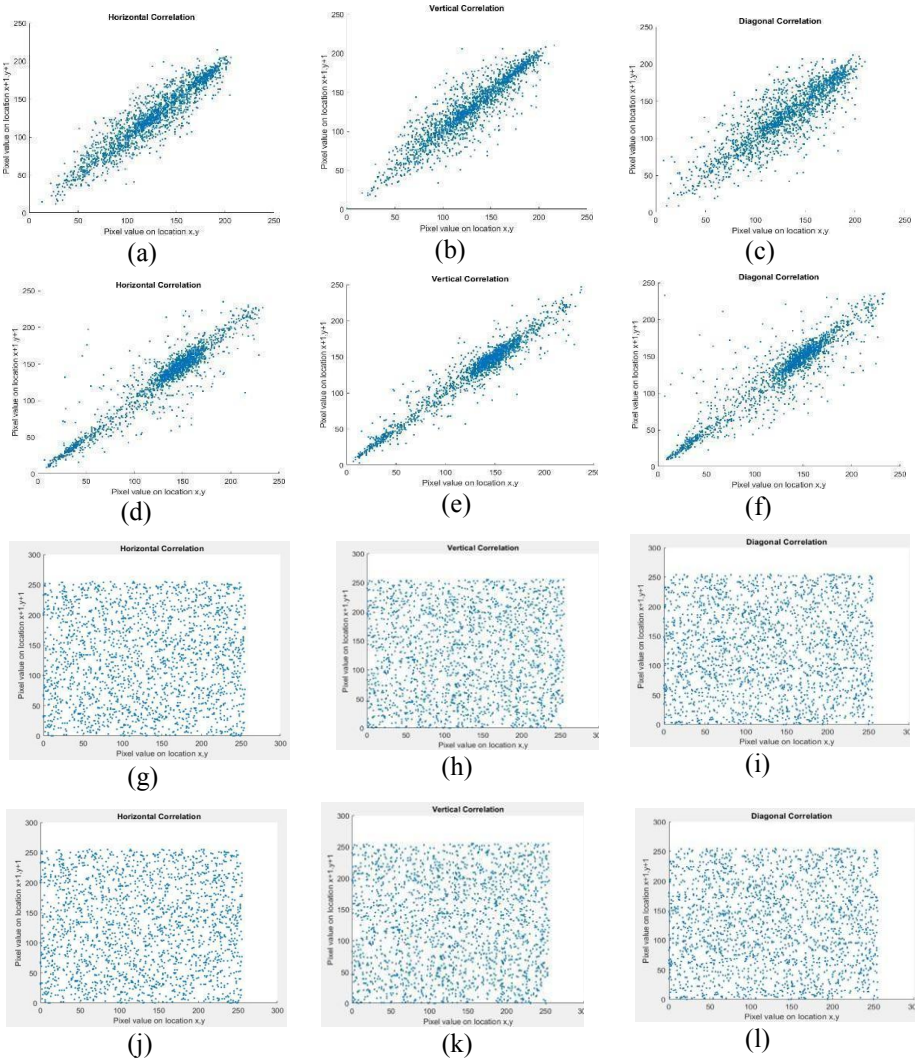

Fig 5. Correlation analysis for input images and cipher images.Input image correlation (a)(d) Horizontal, (b)(e) Vertical, (c)(f) Diagonal. Cipher image correlation horizontal (g)(j), Vertical (h)(k), Diagonal (i)(l)

The input image has a high correlation, the coefficient isalmost 1, the ciphered image has no correlation, and thecoefficient is almost 0.

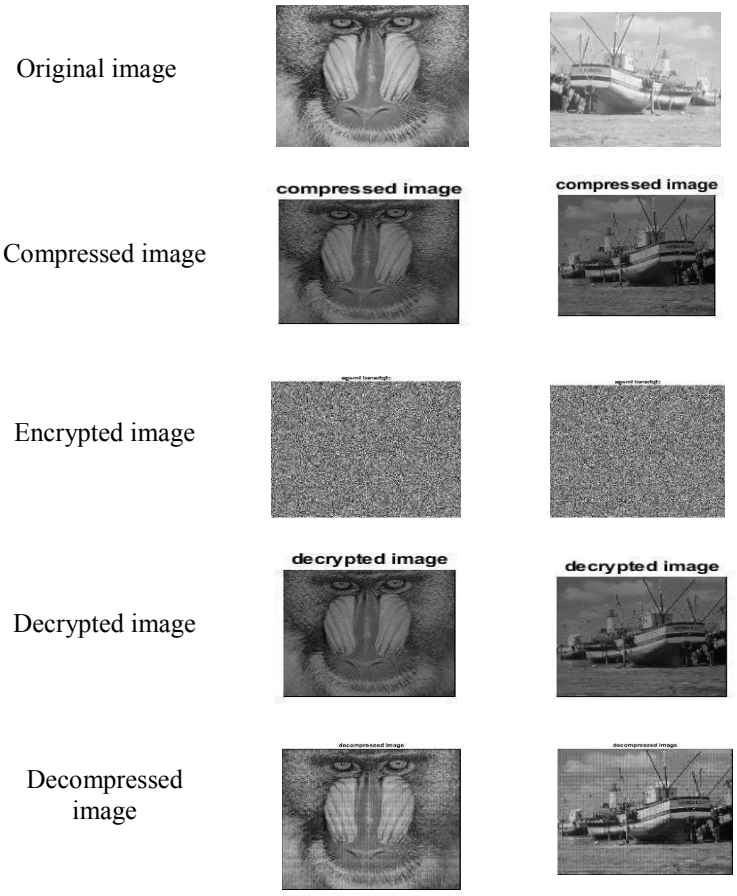

Fig 6. Compressed Image Output

The two gray input images are taken and the DWT method is used to compress the input image. Discrete Wavelet Transform for lossy compression technique isapplied. This lossy compression technique is to reduce the size of the pixel. This compression is used for enormous storage capacity and further downsampling to reduce the image size. The compressed image is applied for the chaotic map technique and the image is encrypted. Chaotic maps have two processes: Diffusionand Confusion. The process for shuffling the value of pixels. It helps that the compressed image is encrypted.The encryption is produced as the cipher image. Both the encrypt and decrypt processes are used as the asymmetric key to process it.

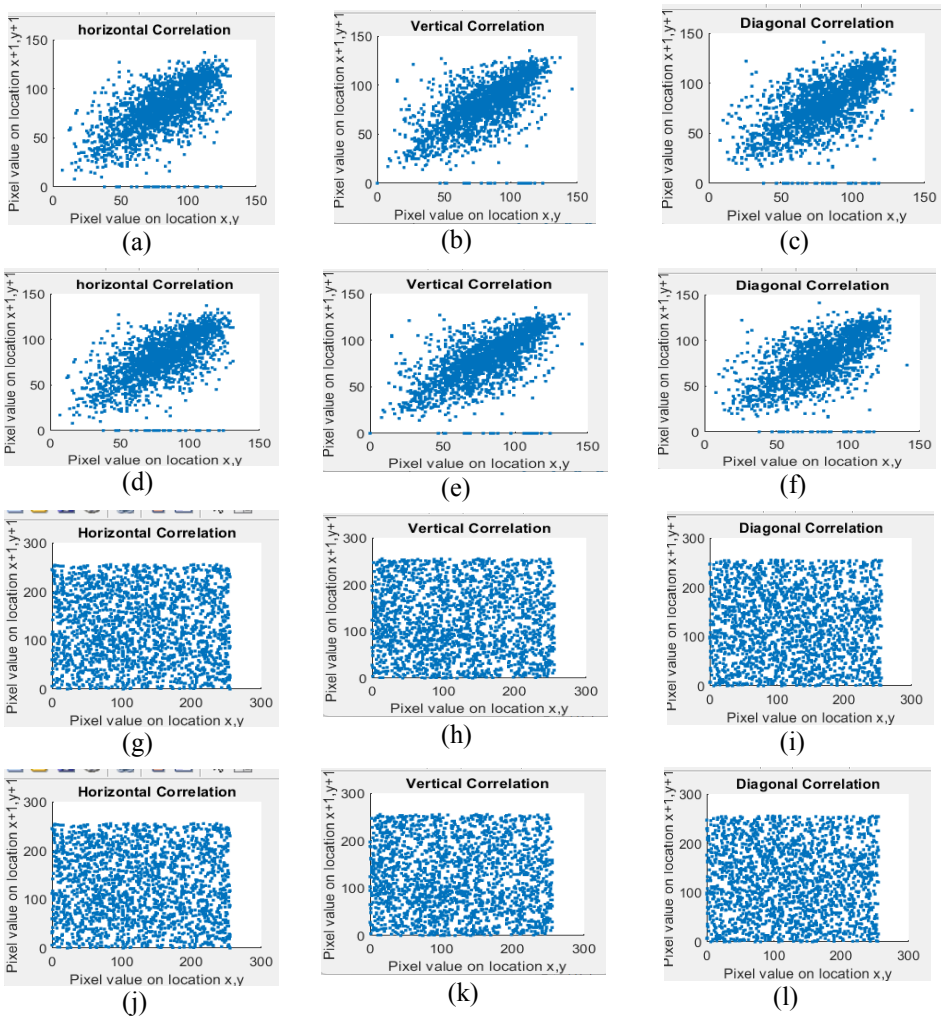

Fig 7. Correlation analysis for compressed input images andcipher images. Compressed input image correlation (a)(d) Horizontal, (b)(e) Vertical, (c)(f) Diagonal. Cipher image correlation horizontal (g)(j), Vertical (h)(k), Diagonal (i)(l)

The image compression is based on the DWT method and the lossy compression technique, which reduces thepixel size 128x128. The proposed map is to encrypt thecompressed input with both encryption, decryption is used as the same key to generate the cipher image. Decryption is a reverse process of encryption, and converting decompressed images using inverse DWT. The decompressed image is similar to the input image.

5 SECURITY ANALYSIS

5.1 HISTOGRAM ANALYSIS

An encryption algorithm is processed for goodperformance of the encrypted image and similar histogram. The grayscale value distribution displays occurrences of frequency for each gray-level value. The ciphered image is produced by the dissimilar fromthe image of input and the encrypted image is produced by the uniform distribution.

5.2 ENTROPY

Entropy is used to produce random number generation and produce security keys to protect the information data.

The information entropy is calculated using

$$H(Z) = -\sum_{i=0}^{255} pr\,(GLi)\log 2\ pr\,(GLi) \qquad \ldots\ldots\ldots (1)$$

Where pr (GLi) probability of gray level GL
For an input, grayscale images to be gray level are random for uniform distribution.

Table 1. Entropy for Plain and Cipher Images

Tested image	Plain Image	Cipher Image
Mandril	7.2925	7.9971
Boat	7.1914	7.9971

This table shows the entropy values of the plain image and cipher image. Hence for noise like encrypted images, the informationentropy has nearly 8.

5.3 CORRELATION ANALYSIS

The analysis changes to values for one variable to predict change to the value of another. It measures the similarity between the adjacent pixel degree for animage. To estimate the encryption quality is analyzed inthis method. The correlation analysis used for the input image has a high correlation and the coefficient isalmost 1 and the ciphered image has no correlation andthe coefficient is almost 0.

$$y = \frac{cov(a,b)}{\sqrt{D(a)}\sqrt{D(b)}} \qquad \text{---------(2)}$$

$$D(a) = \frac{1}{R}\sum_{i=0}^{R}(a-a)^{-2} \qquad \text{---------(3)}$$

$$cov(a,b) = \frac{1}{R}\sum_{i=0}^{R}(a-\bar{a})(b-\bar{b}) \qquad \text{---------(4)}$$

Table 2. Correlation of plain image and cipher image

Correlation	Plain Image	Cipher Image
Horizontal	0.9299	-0.0534
Vertical	0.9062	0.0136
Diagonal	0.8697	-0.0096
Horizontal	0.9384	0.0146
Vertical	0.9720	0.0224
Diagonal	0.9376	0.0384

Table 2. Shows the correlation values of the input plain image and cipher image. The correlation analysis used for the inputimage has a high correlation and the coefficient is almost 1 and the ciphered image has no correlation andthe coefficient is almost 0.

Table 3. Correlation of compressed image and cipher image

Correlation	Plain Image	Cipher Image
Horizontal	0.729	-0.034
Vertical	0.717	0.09
Diagonal	0.643	-0.010
Horizontal	0.643	0.012
Vertical	0.807	0.031
Diagonal	0.704	-0.03

Table 3. shows the correlation values of a compressed plain image and a cipher image. The correlation analysis used for the inputimage has a high correlation and the coefficient is almost 1 and the ciphered image has no correlation andthe coefficient is almost 0.

5.4 PSNR VALUE

PSNR Value measures the quality of the decompressed image of lossy and lossless compression. In this method, the input image and the noise is the error described by compression. The lossy compression reduces an image file size but it also reduces image quality. The PSNR is calculated via the mean squared error.

PSNR is defined as

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{i=0}^{m-1} [I(i-j) - k(i-j)]^2 \quad \text{---------- (5)}$$

$$\text{PSNR} = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad \text{---------- (6)}$$

$$20.\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \quad \text{---------- (7)}$$

Table 4. PSNR Values for tested image

Tested image	MSE Value	PSNR Value
Mandril image	194.99	25.26
Mandril Decompressed image	51.91	31.00
Boat image	193.29	25.29
Boat Decompressed image	62.31	30.20

The lossy compression is used in the tested image and the PSNR value is calculated. The value is above 30 and it is better image quality.

Table 5. Compression Ratio

Image	Compression ratio
Mandril	8:1
Boat	9:1

Two gray input plain images are used as test images. These test images are used for image compression based on the DWT method and the lossy compression technique, which reduces the size of the pixel 128x128.

6 CONCLUSION

This work was proposed by using a logistic map. The confusion and diffusion process produces encrypted images. This process shuffles values of pixels in rows and columns mxn. This parameter, the secret key, is generated by using chaotic maps. This process of encryption is done and analyzes the Histogram,Correlation analysis, and entropy. The input histogramhas uneven distribution and the encrypted image has uniform distribution. Input image Correlation shows a high level, the ciphered image does not correlate, and the correlation coefficient is almost zero. The entropy value is nearly 8. Image compression is proposed usingthe DWT method. This compression technique is used for size reduction of the image pixel. The input image is 512x512 in size and it compresses 128x128 pixels and saves lots of time to receive data. In the future, the algorithms can be used with techniques like machine learning, and convolutional neural networks or combining them with other methods of image compression to produce better image quality.

References

1. Wang, J., Jiang, W., Xu, H., Wu, X., & Kim, J. (2022). Image encryption based on Logistic-Sine self- embedding chaotic sequence. *Optik*, *271*, 170075.
2. Wang, X., Liu, C., & Jiang, D. (2022). A novel visually meaningful image encryption algorithm based on parallel compressive sensing and adaptive embedding. *Expert Systems with Applications*, *209*, 118426.

3. Hanis, S., & Amutha, R. (2018). Double image compression and encryption scheme using logistic mapped convolution and cellular automata. MultimediaTools and Applications, 77(6), 6897-6912.
4. Man, Z., Li, J., Di, X., Sheng, Y., & Liu, Z. (2021). Double image encryption algorithm based on neural network and chaos. Chaos, Solitons & Fractals, 152, 111318.
5. Yang, Y. G., Wang, B. P., Yang, Y. L., Zhou, Y. H., Shi, W. M., & Liao, X. (2022). A visually meaningful image encryption algorithm based on adaptive 2D compressive sensing and chaotic systems. Multimedia Tools and Applications, 1-30.
6. Ponuma, R., & Amutha, R. (2019). Encryption of image data using compressive sensing and chaotic systems. *Multimedia Tools and Applications*, *78*(9), 11857-11881.