IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 39, No. 3, June, 2022, pp. 853-862
Journal homepage: http://iieta.org/journals/ts

Circulate Matrix and Compression Sensing Based Multi-Level Image Encryption

Ranjeet Kumar Singh[1*], Ganesh Gupta[2], Tej Singh[3], Kalka Dubey[1], Anjula Mehto[1]

[1] Department of Computer Science & Engineering, Madhav Institute of Technology and Science, Gwalior 474005, India
[2] Department of Computer Science & Engineering, Chandigarh University Mohali, Punjab 140413, India
[3] Department of Information Technology, Madhav Institute of Technology & Science, Gwalior 474005, India

Corresponding Author Email: ranjeets@mitsgwalior.in

https://doi.org/10.18280/ts.390310

Received: 26 February 2022
Accepted: 16 May 2022

Keywords:
cryptography, sensing matrix, compressive sensing, random matrix, Arnold cat map

ABSTRACT

Digital data security is a broad research area in the field of science and technology. A lot of research was focused on information security-based mechanism for secure communication. This paper presents a novel image encryption as well as compression based on measurement matrix, pixel exchange and logistic cat map, which includes the permutation, compression, and diffusion processes. Initially the image is divided into four equal sizes of blocks and then each block is transformed into horizontal and vertical low and high frequency band. Then a random matrix multiplication function is applied to achieve an encrypted and scrambling frequency component and apply inverse DWT procedure to get first level of scrambled blocks, and further we apply the second level of security mechanism. Here each adjacent block pixel is exchanged by using the random matrices. For providing the high level of compression we design measurement matrices in compressive sensing by utilizing the circulate matrices and controlling the original column vectors of the circulate matrices with Arnold cat map. With the help of measurement matrix again the blocks are encrypted. Experimental results and performance analyses validate the good compression performance and high security of the given algorithm.

1. INTRODUCTION

With the significant developments of internet, digital communication media, and digital data communication exchange over internet network, security is the very important issue. To overcome this issue Symmetric cryptography algorithms (Data Encryption Standard and Advanced Encryption Standard (AES)) are widely used but it is used for only text data not for image. For the purpose of security of image-based data, some new image encryption algorithms are intended, like the chaos [1-4], deoxyribo nucleic acid (DNA) coding [5-7], and S-box [8, 9].

Now a days, Chaotic system is mostly used in image security purpose due to its initial value sensitivity, randomness and unpredictability. Normally, chaotic maps are decomposed into one-dimensional and high-dimensional map. One dimensional chaotic map may be simply and easily predicted [10] because of its simple trajectory and few initial conditions. But in the high dimensional case their computational cost will be increased, so to reduce this problem sensing matrix-based encryption is one of the choices.

Sensing matrix is a new updated research field in the area of computer science. The sensing matrix provides the updated security mechanism to the digital data. The best feature of this approach is recovery of signal is easier. This approach provides compression as well as encryption, so it is comparative good to other conventional technique. Designing of the sensing matrix is easier and less computational therefor it is rapidly used in image processing, signal processing etc.

The newly proposed approach of compressive sampling (CS) or compressed sensing, shown by Candés et al. [11-13], is a new updated image processing approach. Here It permits the signal to be sampled at too much lower a rate than the Nyquist-Shannon rate and makes the signal to be sampled and compressed in a single-step mechanism. Similarly, a chaotic sequence-based approach is shown by Rong Huang and Sakurai [14]. It explained a tool where the original image is projected in a low-dimensional space. This paper used a logistic map for the purpose of generating chaotic sequences. Arnold scrambling is used to measure matrix scrambling. The main drawback of this approach is computational cost, and it takes a more significant number of variables to design the measurement matrix. Now optimization is one of the ways to reduce the computational cost.

Hence Endra et al. presented a research work based on the optimization of the sensing matrix by the MC-ETF method. The optimized matrix is more robust compared to the random sensing matrix. The quality of reconstruction of a signal is comparatively good compared to the random sensing matrix [15]. A more secure approach was proposed by Xu et al. [16] It deeply explained a digital image scrambling procedure based on CS. Here a novel 2D-SLIM hyper chaotic map is designed for the purpose of generating random sequences. The SHA-512 hash values of the digital image and the primary conditions of the proposed hyperchaotic map are used to create the secret key of the algorithm. Then two different directions, CS is used and then re-encrypted using the row and column encryption procedure.

Shruthi et al. [17] proposed a chaotic function-based image encryption mechanism. In this research authors design a linear feedback shift register for the way of controlling the randomness of sequences. The main advantage of this

approach is the key sequences are stored offline in advance. Gong et al. [18] proposed a compression and encryption based mechanism by applying discrete fractional random transform and hyper-chaotic system. Here DCT is used to convert an image into spectrum and spectrum cutting is applied to compressed the data. Chaotic sequence which is originated from the hyper-chaotic system is used to controlling the random matrix, then discrete fractional random transform is apply to encrypt the compressed spectrum. The computational cost of this algorithm is not moderate and this algorithm is going under plain text attack.

To overcome this weakness a new compressive sensing based simulates compression and encryption mechanism is again proposed by Gong et al. [19], for a linear image. Here authors used Arnold transform to permutate the original image and the bitwise XOR operation is used to measures the change in pixel value.

Ponuma et al. [20] present a research work on hyper-chaos based simultaneous compression-encryption mechanism. Here authors simultaneously compress and encrypt 2D image by using two measurement matrices. Hyper chaos is used for the purpose of improve the security mechanism of digital data. Zhang et al. [21] focus a secrete orthogonal transform-based encryption mechanism. Encrypted image is compressed by using a linear operation. In this article, compressive sensing approach is applied to recover the signal. Recon structed image quality is depending on the rate of compression.

Chai et al. [22] represent an image based data encryption mechanism with the help of compressive sensing, memristive chaotic system and elementary cellular automata. Initially author transform the image into frequency component by discrete wavelet transform, and a zigzag scrambling approach is applied to obtained sparse matrix. Here measurement matrix produced by the memristive chaotic system which is used to compress the data. To improve the recovery of the signal, Chen et al. [23], explain a simultaneous image compression as well as encryption mechanism. This algorithm explains the combined approach of random matrix and compression sensing based permutation-diffusion type image scrambling approach. Here Three-dimensional cat map is used for key stream creation. But this work also not able to reduce the computational cost.

A new image encryption mechanism is proposed by Chen et al. [24], Here authors multi-image encryption mechanism is explained which is based on compressed sensing and optical wavelet transform. In this paper low and high frequency component of four images are merged into a low and high frequency fusion image respectively. After this high frequency fusion image is decomposed into two matrices by CS. Afterward, the two matrices and the low frequency fusion image are scrambled and encrypted to a single ciphertext by phase truncation and phase reservation in the Fresnel domain. A Hybrid concept of cryptography and watermarking concept are also shown in the studies [25-27].

Based upon the above survey, the current image encryption algorithms have the following shortcomings:

1) The compression and encryption of plain images can be handled efficiently through some CS-based image encryption algorithms. Further, the pixel values can be modified through the linear measurement of CS, and the adjacent pixel coefficients can be eliminated by fusing the scrambling operation. The cipher images thus obtained will be devoid of high randomness, thereby making it susceptible to image crypto system attacks.
2) Both the security performance and compression are equally crucial for a real-time image transmission. These are crucial particularly in the areas of battlefield medical online transmission due to bandwidth considerations. But at the same time, these cryptographic techniques do not serve well to encrypt compressed images and their ciphertext. This is due to the removal of redundancy in the encryption procedure.
3) To enhance the encryption security, encryption methods that clubbed fusion with nonlinear operations was proposed. But such techniques inherited issues related to low decrypted image quality and resolution caused by poor high-quality information.

To reduce this problem, here we show the lossless compression and multi-level security mechanism, where computational cost is also moderate's mathematical model of this algorithm is shown in next section. Here, the main goal of author to reduce or compressed the data and also provide the security. Measurement Matrix, pixel exchange and Arnold cat map are used to achieved the research goal.

2. PROPOSED METHOD

In this section of the research work, proposed an image encryption and decryption approach. This section also shows the detail working of measurement matrix-based image encryption and decryption in the section 3.5 and section 3.6.

Now, here we also shown the detail working structure of pixel exchange, designing procedure of measurement matrix, Logistic Map and frequency component scrambling are in section 3.1, section 3.2, section 3.3 and section 3.4:

3. PIXEL EXCHANGE PROCEDURE

Initially, two random matrixes A_1 and A_2 are created whose elements are varied to 0 to 1. Random matrix A_1 is used for pixel change between block B_1 and B_2, and similarly, A_2 is used for pixel exchanged between block B_3 and block B_4. Here the size of the random matrix is the same as the size of the image blocks. Assume the size of the block is $m \times n$ therefore; the size of the random matrix is also $m \times n$. But in this experiment, the size of the random matrix is represented by $M \times N$. The output of the pixel exchange procedure is represented by B_{1p}, B_{2p}, B_{3p}, and B_{4p}. Here, B_{1p} represent the block B_1 after getting the result of pixel exchange with the help of random matrixes A_1, similarly B_{2p}, B_{3p}, and B_{4p}. represents the result of pixel exchange of *block* B_2, block B_3 and block B_4.

For the purpose of successful exchange, the pixel, the most important thing is calculation of modified pixel position. New position (m', n') is created with round function, the detail mathematical expression is given below.

$$m' = f_1(m, n) = 1 + round\{(M-1)\, R\, (m, n)]\}$$

$$n' = f_2(m, n) = 1 + round\,[(N-1)\, R\, (m, n)],$$

$$1 \le m \le M,\ 1 \le n \le N$$

In Eqns. (1) and (2), the $f_1(m,n)$ function is used to calculate the modified value of m and similarly, $f_2(m,n)$ is used to calculate the modified value on n, which is represented by m' and n'. After deciding the new location of pixel we developed a algorithm for exchange procedure based on mean value of

random matrixes A_1 and A_2. Now, calculate the mean value of random matrix to change the pixel values between appropriate positions of blocks of host image. The mathematical function for calculating the mean value is given below:

$$A_1^c = \frac{1}{M \times N} \sum_{\forall m,n} A_1(m,n)$$
$$A_2^c = \frac{1}{M \times N} \sum_{\forall m,n} A_2(m,n)$$

After getting the A_1^c and A_2^c values of random matrix A_1 and A_2, we exchange the pixel of blocks. The detail procedure of pixel exchange is given in below algorithm and the detail working structure is also shown in Figure 1. In the Figure 1, B_1 and B_2 represents the *Block* B_1 and *Block* B_2 and A_1 is the first random matrix.

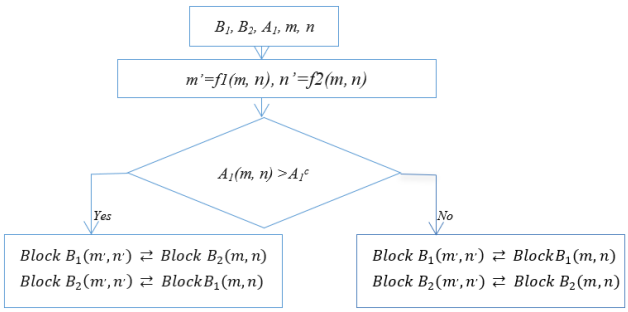


Figure 1. Pixel exchange procedure

Algorithm for Pixel Exchange:

Step 1: Select the pair of $Block\ B_1$ and $Block\ B_2$ for pixel exchange.

Step 2: Generate a random matrix A_1.

Step 3: Find the new location or position of pixel i.e. (m', n').

Step 4: Find the mean value of random matrix A_1.

Step 5: {

$$if\ A1(m,n) > A1^C$$
$$\{$$
$$Block\ B_1(m',n') \rightleftarrows Block\ B_2(m,n)$$
$$Block\ B_2(m',n') \rightleftarrows BlockB_1(m,n)$$
$$\}$$
$$else$$
$$\{$$
$$Block\ B_1(m',n') \rightleftarrows BlockB_1(m,n)$$
$$Block\ B_2(m',n') \rightleftarrows Block\ B_2(m,n)$$
$$\}$$

Step 6: We get the B_{1P}, B_{2P}, B_{3P}, and B_{4P}.

For the recovery of the original frequency sub-bands inverse pixel exchange procedure is applied. If $A_1(m,n) > A_1^c$, the pixel at the position (m,n) and (m',n') are exchanged to each other for two modified $blocks\ B_{1p}$ and B_{2P} and, if $A_1(m,n) < A_1^c$, the pixel exchanged is made in the inner pixel of modified blocks B_{1P} and B_{2P}. Similarly, if $A_1(m, n) > A_1^c$, exchange the pixel present at the position, (m, n) and (m', n') to each other for two modified $blocks\ B_{3P}$ and B_{4P}. If $A_1(m,n) < A_1^c$ exchange the inner pixels of B_{3P} and B_{4P} blocks.

3.1 Measurement matrix

In this section we are going to design a measurement matrix with the help of logistic map. Here, author create two measurement matrix which is represented by MM_1 and MM_2, these matrices are useful to provide second level of data scrambling and data encryption. Initially we generate N number of sequences by using logistic map. Let us consider $y = [y_1, y_2, y_3, y_4 \ldots . y_n]$. Sequences are generated by using logistic map. These sequences are used to fill the column vector of the measurement matrix. The measurement matrix MM_1 and MM_2 is calculated with the help of original column vector $y = [y_1, y_2, y_3, y_4 \ldots . y_n]$. The first element of the measurement matrix $MM_1(1, j)$ is calculated by multiplying $MM_1(N, j-1)$ by λ, where $2 < j < N$ and $\lambda < 1$. The mathematical function for designing a measurement matrix MM_1 and MM_2 is given below:

For measurement matrix $M\,M1$:

$$M_1(1, j) = \lambda . M\ M_1(N, j-1)$$
$$MM_1(2 : N, j) = M\ M_1(1 : N-1, j-1)$$

For measurement matrix $M\,M2$:

$$MM_2(1, j) = \lambda . M\ M_2(N, j-1)$$
$$MM_2(2 : N, j) = M\ M_2(1 : N-1, j-1)$$

3.2 Logistic map

Logistic map is a non-linear mathematical quadratic expression defines as:

$$Xn + 1 = r . Xn\ (1 - Xn)$$

where, $Xn \in (0,1)\ and\ 0 \le r \le 4$.

Here Xn and r represents the system variables and n represents the number of iterations. Basically, it is a recursive function which is used to generate a number of sequences. The value of Xn+1 is dependent on value of Xn and $(1 - Xn)$ where Xn contain only 0 and 1 and r lies between 0 to 4. The mathematical function which is used to create the Column vector of the measurement matrix by using the logistic cat map is given below:

$$M\ M_1(i) = r * M\ M_1(i-1) * (1 - M\ M_1(i-1));$$
$$M\ M_1(1, i) = M\ M_1(i);$$
$$M\ M_2(i) = r * M\ M_2(i-1) * (1 - M\ M_2(i-1));$$
$$M\ M_2(1, i) = MM_2(i);$$

The above mathematical expression used the initial condition $M\,M_1(0) = 0.11, M\,M_2(0) = 0.23\ and\ r = 3.99$.

3.3 Frequency component scambling

In this section, frequency scrambling is explained in detail. Initially, host image is decomposed into four frequency sub-bands by using discrete wavelet transformation. Here, four random matrices R_1, R_2, R_3 and R_4 are generated whose size is equal to the size of all frequency sub bands. In this experiment random matrix R1 is selected for scrambling the frequency sub-band LL, similarly random matrix R_2, R_3 and R_4 is selected for scrambling the frequency sub-band LH, HH and HL. The mathematical function is given below.

$$
\begin{aligned}
&\{\\
&function\ f\ =\ encrypt\ (matrix, sub\ -\ band)\\
&find\ row\ and\ column\ of\ matrix\ and\ sub\ -\ band.\\
&create\ a\ matrix\ X\ =\ zerows(no\ of\ rows\\
&\quad =\ no\ of\ rows\ of\ matrix,\\
&no\ of\ coloum\ =\ no\ of\ coloum\ of\ sub\ -\ band\ matrix)\\
&for\ i\ =\ 1:\ no\ of\ rows\ of\ matrix\\
&for\ j\ =\ 1:\ no\ of\ coloum\ of\ sub\ -\ band\ matrix\\
&for\ k\ =\ 1{:}\ no\ of\ coloum\ of\ sub\ -\ band\ matrix\\
&Y\ (i,j)\ =\ Y\ (i,j)\ +\ sub\ -\ band\ (i,k)\ *\ matrix\ (k,j);\\
&\}
\end{aligned}
$$

The mathematical function of inverse procedure of frequency scrambling is given below:

$$
\begin{aligned}
&\{\\
&Function\ f\ =\ encrypt\ (matrix, encrypted\ sub\\
&\quad -\ band)\\
&find\ row\ and\ coloum\ of\ matrix\ and\ encrypted\ sub\\
&\quad -\ band.\\
&create\ a\ matrix\ M\ =\ zeroes\ (no\ of\ rows\\
&=\ no\ of\ rows\ of\ matrix, no\ of\ column\\
&=\ no\ of\ column\ of\ encrypted\ sub\ -\ band\ matrix)\\
&\quad for\ i\ =\ 1:\ no\ of\ rows\ of\ matrix\\
&\quad for\ j\\
&\quad =\ 1{:}\ no\ of\ coloum\ of\ encrypted\ sub\\
&\quad -\ band\ matrix\ f\ or\ k\\
&\quad =\ 1{:}\ no\ of\ Coolum\ of\ encrypted\ sub\\
&\quad -\ band\ matrix\\
&Y\ (i,j)\ +\ encrypted\ sub\ -\ band\ (i,k)\ *\ matrix\ (k,j)\\
&\quad =\ Y\ (i,j)
\end{aligned}
$$

Now, inverse discrete wavelet transformation is applied to each unscrambled frequency component of blocks and get the blocks of original image. Finally, reassembled the all blocks of original image and get the decrypted original image.

3.4 Encryption algorithm

For the purpose of compression-based encryption, initially two measurement matrixes MM_1 and MM_2 is designed. Measurement matrix is treated as a circulate matrix. The column vector is filled by logistic chaos map and row vector is fixed. Algorithm for design measurement matrix is also explained in the previous section 3.2.

At first original image is selected then divided into four equal parts based on row and column vector. After finding four equal sizes of blocks, again each block is divided into horizontal and vertical low and high frequency band by using discrete wavelet transformations. After finding the four-frequency band i.e., LL, LH, HH and HL, we design a four random matrix. Here; the random matrix is used for scrambling the all frequency sub-bands. The mathematical function of scrambling the frequency sub-band is explained in section 3.4.

In this experiment the original image is divided into four equal sizes of blocks and again each block is decomposed into their four frequency sub-bands. All frequency sub-bands are scrambled with random matrix. After the completions of first phase of scrambling, inverse discrete transformation is applied to reassemble the all appropriate frequency sub-bands.

Now, for the purpose of the enhanced the security mechanism random pixel exchange procedure is applied. The detail explanation of random pixel exchange procedure is shown in section 3.1. Initially A_1 and A_2 two random matrix is generated and their size is equal to the size of image blocks. Random matrix A_1 is used to exchange the pixel between block B_1 and B_2, similarly Random matrix A_2 is used to exchange the pixel between *block* B_3 and B_4. After the completion of the random pixel exchange procedure to get the scramble blocks B_{1P}, B_{2P}, B_{3P} and B_{4P}.

Finally, measurement matrix-based encryption is applied to all scrambled blocks of image. The main advantage of measurement matrix is, it provides compression-based encryption.

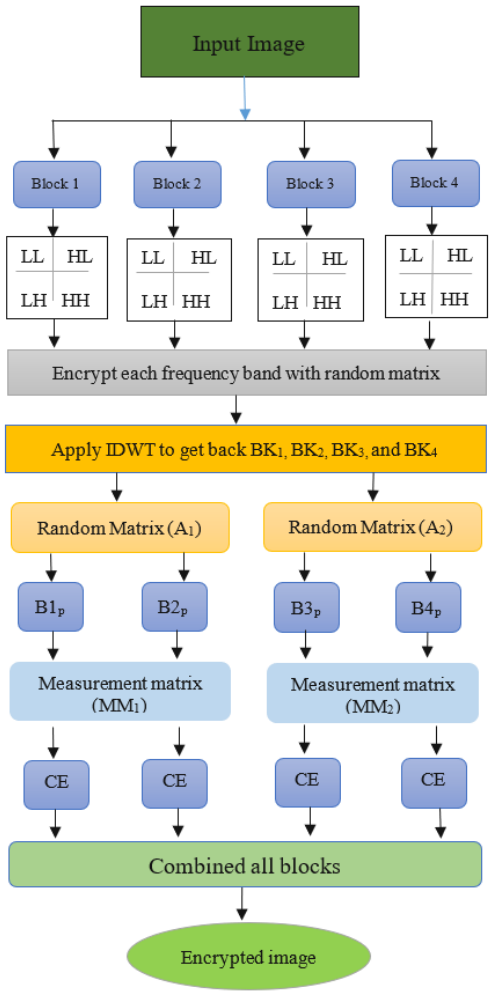


Figure 2. Working structure of encryption mechanism

In this experiment two measurement matrix $MM1$ and MM_2 are designed to encrypt the blocks. The measurement matrix MM_1 is used to compressed and encrypt for blocks B_1 and B_2. Similarly, the measurement matrix MM_2 is used to compressed and encrypt the *blocks* B_3 and B_4. Now, finally combined all blocks to get the encrypted image.

The detail of the working mechanism of the proposed image encryption algorithm is given in Algorithm 1. The detail of the encryption procedure is also given in Figure 2.

Algorithm 1: The basic algorithm step for Image encryption based on measurement matrix:

1: Select an image (original image)

2: At first, divided original image into four equal size blocks i.e. B_1, B_2, B_3 and B_4 and design a measurement matrix. Size of measurement matrix is depending upon size of block size of image. Let us consider $B_1 \in R^{M\times N}$, where $R^{M\times N}$ is original

image signal and B_1 is a one of the blocks of input image. The measurement matrix MM_1, $MM_2 \in R^{M\times N}, M \times N$ is the length of measurement matrix.

3: Now, logistic chaos map is used to create a sequence with initial condition initial condition $MM\ 1\ (0) = 0.11$, $MM2\ (0) = 0.23$ and $r = 3.99$. These sequences are used to fill the column vector of the circulant matrix.

4: Find the frequency based component of each block by discrete wavelet trans-formation. Basically, DWT convert horizontally and vertically low and high frequency component of the blocks, i. e. $[LL, LH, HH, HL] = DWT\ (Block1)$.

5: Create R_1, R_2, R_3, and R_4 four matrices which size is equal to the size of LL, LH, HH and HL sub-band of the blocks of image. Now scrambled all the sub-bands of the blocks by a mathematical function. Here, R_1 matrix is used for LL sub-band, R_2 is LH, R_3 is HH and R_4 is HL sub-band. The mathematical function is given below:

{

$Function\ f = encrypt(matrix, sub - band)$

$find\ row\ and\ coloum\ of\ matrix\ and\ sub - band.$

Create a matrix $X = zerows(no\ of\ rows = no\ of\ rows\ of\ matrix,$ no of coloum = no of coloum of sub − band matrix)

$for\ i = 1 : no\ of\ rows\ of\ matrix$

$for\ j = 1 : no\ of\ coloum\ of\ sub - band\ matrix\ f\ or\ k = 1 : no\ of\ coloum\ of\ sub - band\ matrix$

Y (i, j) = Y (i, j) + sub − band(i, k) ∗ matrix(k, j);

}

6: After finding the scrambled LL, LH, HH and HL sub-band, Now apply inverse discrete wavelet transformation we get scrambled blocks B_1, B_2, B_3, and B_4.

7: Random matrix A_1 and A_2 is used to pixel exchange between the blocks.

8: Now, multiply measurement matrix MM_1 to scrambled $block_1$ and $block_2$ to get the compressed and encrypted data CEB_1 and CEB_2, similarly multiply measurement matrix MM_2 to scrambled block3 and block3 to get CE_{B3} and CE_{B4}. The mathematical function is given below:

$$E_{block1} \times MM_1 = CE_{B1},$$
$$E_{block2} \times MM_1 = CE_{B2}$$
$$E_{block3} \times MM_2 = CE_{B3} \text{ and}$$
$$E_{block4} \times MM_2 = CE_{B4}$$

9: Finally, combined the all compressed and encrypted block to get the encrypted original image.

Algorithm 2: The basic algorithm step to Decryption of image.

1: Select the encrypted image, and divide into four equal size blocks. For creating equal size of blocks at first find row, column of the image and then divide row and Column into two parts.

2: Multiplying inverse of measurement matrix to scrambled block to get B_{1P}, B_{2P}, B_{3P} and B_{4P}.

$$B_{1P} = MM_1^{-1}.\ CEB_1,$$
$$B_{2P} = MM_1^{-1}.\ CE_{B2}$$
$$B_{3P} = MM_2^{-1}.\ CEB_3 \text{ and}$$
$$B_{4P} = MM_2^{-1}.\ CEB_4$$

3: Now, Inverse random pixel exchange procedure is applied and get un-scrambled blocks.

4: DWT is applied to all un-scrambled blocks to get the frequency sub-bands of un-scrambled blocks.

5: Inverse function of the frequency scrambling is applied to get decrypted LL, LH, HH and HL sub-band of the blocks of image. The procedure of inverse pixel exchange is given below.

{

Function f = encrypt (matrix, encrypted sub − band)

find row and column of matrix and encrypted sub − band.

create a matrix M = zerows(no of rows = no of rows of matrix, no of coloum = no of coloum of encrypted sub − band matrix)

f or i = 1: no of rows of matrix

f or j = 1: no of coloum of encrypted sub − band matrix f or k = 1: no of coloum of encrypted sub − band matrix

Y (i, j) + encrypted sub − band(i, k) ∗ matrix(k, j) = Y (i, j)

}

6: After finding the un-scrambled LL, LH, HH and HL sub-band of the blocks of image. Inverse discrete wavelet transformation is applied to get all decrypted blocks i.e. Block1, Block 2, Block 3, and Block 4 of the original image.

7: Finally, combined all blocks to get the decrypted original image.

4. RESULT ANALYSIS

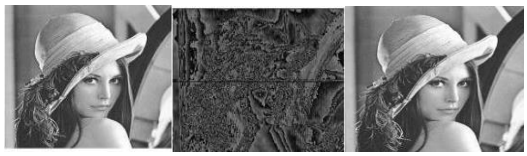
In this experiment test the result on different images i.e. Lena, Pepper, Mandrill and Cameraman image. Histogram of Lena image, encrypted Lena image and decrypted Lena image is show in Figure 4. Similarly histogram of Pepper, Mandrill and Cameraman and their encrypted and decrypted image is also shown in Figure 4. Here all the simulations are done by Matlab on a 64-bit computer and Microsoft Windows 10 operating system. This experiment used 256 × 256 pixel of Lena image, pepper image, mandrill and cameraman image. The tested image is shown in Figure 3.

Figure 3. Lena, pepper, mandrill and cameraman image

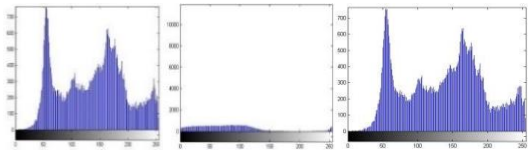
The initial condition of Logistic map is $MM_1\ (0) = 0.11, MM_2\ (0) = 0.23\ and\ r = 3.99$. The simulation results are illustrated in Figure 4 to Figure 6.

This work proposed the enhanced N. Zhou model based on frequency-based compression- encryption procedure. Here, discrete wavelet transformation is used to decomposed the blocks of image into their low and high frequency sub-bands.

In this experiment all the frequency sub-bands are scrambled by random matrix and again blocks are scrambled by random matrix. This frame work provides the dual scrambling procedure to enhanced the data security level. After scrambling measurement matrix is used to compress and encrypt the appropriate blocks. This experiment provides the better result compare to results of N. Zhou approach.

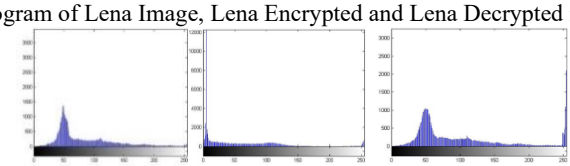


Lena Image, Lena Encrypted and Lena Decrypted.



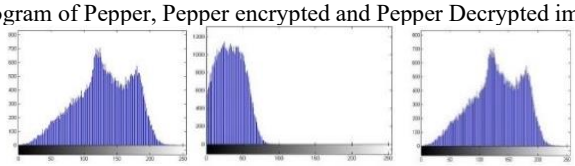
Histogram of Lena Image, Lena Encrypted and Lena Decrypted image

Pepper, Pepper encrypted and Pepper Decrypted image



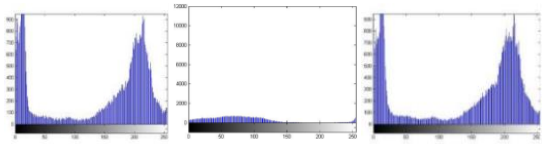
Histogram of Pepper, Pepper encrypted and Pepper Decrypted image

Mandrill, Mandrill Encrypted and Mandrill Decrypted Image.



Histogram of Mandrill, Mandrill Encrypted and Mandrill Decrypted Image.

Cameraman, Cameraman Encrypted and Decrypted Image.

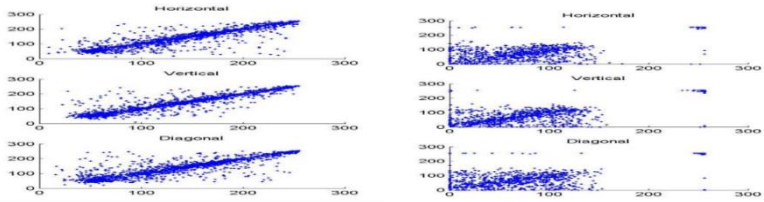


Histogram Cameraman, Cameraman Encrypted and Decrypted Image.

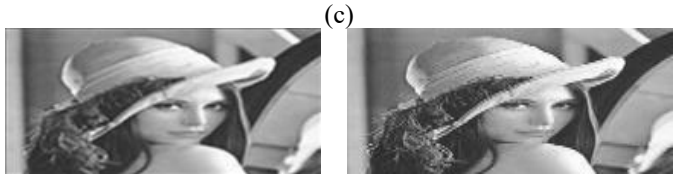
Figure 4. The Lena, pepper, mandrill and cameraman image encryption decryption and their histogram

(a)

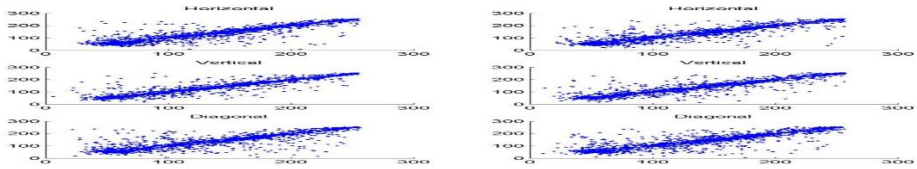
(b)



(c)



(d) (e)



(f)

Figure 5. (a) Lena Image, (b) Encrypted Lena Image, (c) Correlation distribution between original Lena and encrypted Lena (e)Decrypted Lena (f) Correlation distribution between original Lena and decrypted Lena

(a)

(b)

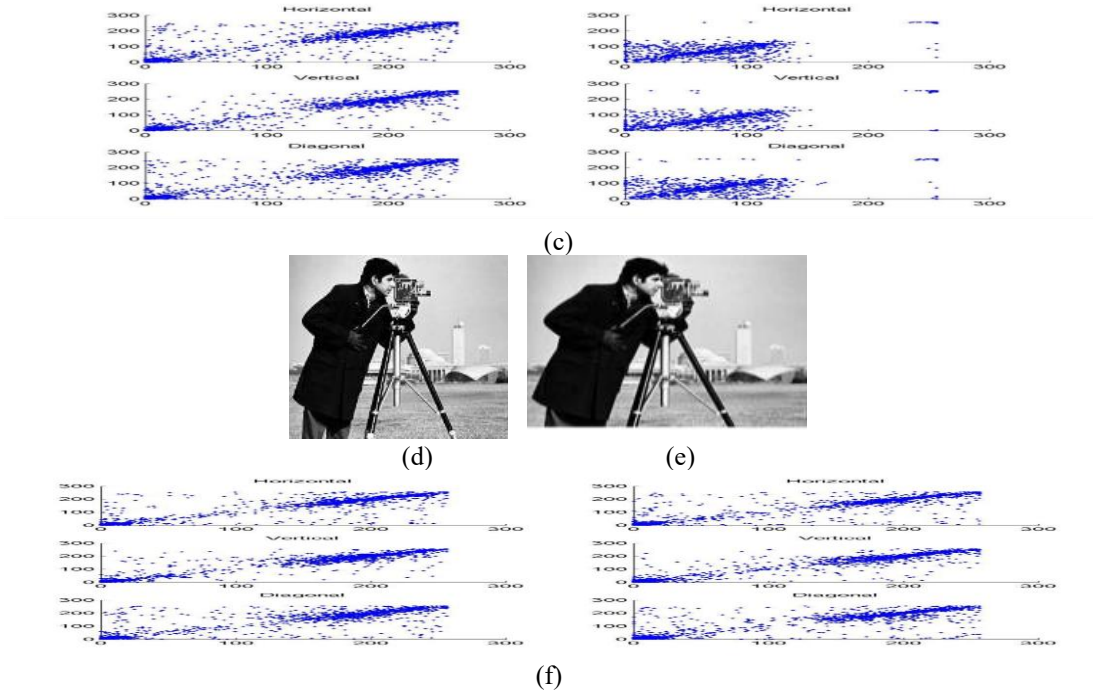


Figure 6. (a) Cameraman image, (b) Encrypted cameraman image, (c) Correlation distribution between original cameraman and encrypted cameraman (e) Decrypted mandrill (f) Correlation distribution between original cameraman and decrypted cameraman

4.1 Histogram

Histogram of the image depicts the distribution of intensities in a digital image. Histogram is the one of the measurements of the quality of images. Here, histogram is used only for performance measurement of encryption algorithm. The histogram of the original image and decrypted image is similar to each other that means the decryption algorithm is robust and efficient. Figure 4 shows the histogram of original image, and their encrypted and decrypted image.

4.2 Correlation of two adjacent pixels

Correlation is a one of the other quality measurement approach of the image. In a meaningful image correlation should be 1 or we can say if correlation between two images is 1, that means both images is same. Here, the correlations between two image pixels are measured in vertical, horizontal and diagonal direction. Figures 5 and 6 show the correlation distribution of original image and encrypted image, original image and decrypted image. The mathematical expression of correlation coefficient is given below:

$$CC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j) * w'(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n} w^2(i,j)}$$

4.3 Entropy

Entropy of image represent the amount of disorder or randomness of the image. Entropy is used to verify the randomness of the decrypted image. The mathematical function of the entropy is given below.

$$H(Y) = -\sum_{i=1}^{n} \Pr(y_i) \log_2 \Pr(y_i)$$

where, $Pr\ (y_i)$ represent the probability of y_i and n represents no of bit in each pixel. The entropy of the plain image, decrypted image and encrypted image for different image is given in Table 1.

In Table 1, we see the entropy value of different image i.e. Lena, encrypted Lena, decrypted Lena image are 7.7364, 4.3909 and 7. 6533.Similarly, the entropy value of Peppers, encrypted Peppers and Decrypted Peppers are 5.4816, 5.7539 and 3. 837.The entropy value of cameraman, encrypted and decrypted cameraman are 7.2678, 4.3319 and 7.2547.

In Table 2, represents the correlation coefficient of adjacent pixels along horizontal, vertical and diagonal axis of Lean, encrypted Lena, Cameraman, encrypted Cameraman and Pepper and encrypted pepper image are shown. This table also provides the comparative results to N. Zhou approach.

Table 1. Entropy table

Image	Entropy	Image	Entropy
Lena	7.7364	Cameraman	7.2678
Lena encrypted	4.3903	Cameraman encrypted	4.3319
Lena decrypted	7.6533	Cameraman decrypted	7.2547
peppers	5.4816	Mandril	7.7748
Peppers encrypted	5.7539	Mandril encrypted	4.3684
Peppers decrypted	3.837	Mandril decrypted	7.4112

4.4 Peak signal to noise ratio (PSNR)

It is a one of the well-known quality measurement tests between the two images i.e. host and encrypted or host and decrypted image. In Table 3, its show the PSNR between host and decrypted host image. The mathematical expression for calculation PSNR between two images is given below [28].

$$PSNR = 10\log \frac{255 \times 255}{(1/\mathrm{M}^*\mathrm{N})\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j))2}$$

Table 2. Comparison of robustness

Image (256×256)	Algorithm	Horizontal	Vertical	Diagonal
Lena	Plain Image	0.9724	0.9449	0.9206
	our	0.0072	0.0004	0.0031
	[29]	0.0064	0.0003	0.0026
	[30]	0.0104	0.0299	0.0062
	[31]	0.0042	−0.0043	0.0163
	[32]	0.0069	−0.0028	−0.0047
Peppers	Plain Image	0.9714	0.9644	0.9388
	Our	-0.1121	0.0041	-0.0029
	[29]	−0.0117	0.0039	−0.0012
	[30]	0.0385	0.0296	0.0069
	[31]	−0.0005	−0.0062	0.0036
	[32]	0.0074	0.0035	0.0041
Cameraman	Plain Image	0.9592	0.9337	0.9079
	Our	0.0048	0.0011	-0.0074
	[29]	0.0040	−0.0027	−0.0084
	[30]	---	---	---
	[31]	---	---	---
	[32]	−0.0044	−0.0054	0.0025
Lake	Plain Image	0.9572	0.9586	0.9289
	Our	-0.0161	-0.0071	-0.0061
	[29]	−0.0159	−0.0074	−0.0005
	[30]	---	---	---
	[31]	0.0231	0.0140	0.0097
	[32]	−0.0084	−0.0028	0.0033
Man	Plain Image	0.9538	0.9403	0.9097
	Our	0.0032	0.0076	-0.0069
	[29]	0.0022	0.0089	−0.0066
	[30]	0.0272	0.0301	0.0089
	[31]	---	---	---
	[32]	---	---	---

Table 3. PSNRs (db) of different image

Plain Image	PSNR (db)
Lena	33.94
Cameraman	32.01
Pepper	33.53
Mandrill	33.21
Man	33.72

Table 4. PSNRs (db) of different methods

Algorithm	PSNR (db)
Ref. [33]	26.52
Ref. [31]	17.42
Ref. [34]	22.62
Ref. [21]	26.06
Ref. [28]	33.92
Our algorithm Mandrill,	33.94

Here, $x\,(i,j)$ represents the host image pixel value, similarly y (i, j) represents the decrypted host image pixel value. Size of the image is here represented by M, N. Normally we know that higher PSNR value show lower distortion. Table 3, show the PSNR value of different host image and decrypted host image. Similarly, in Table 4, we show the PSNR value of different algorithms and images.

4.5 Structural similarity index measurement (SSIM)

Mainly SSIM check the quality between two images in the aspects of brightness, structure and contrast. The measurement value of SSIM lies between 0 to 1. Here, 1 represents the both images are approximate similar and 0 represent the both images are totally different. The mathematical expression of SSIM calculation is given below [28].

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

Here,

$$C_1 = (\mathrm{k}_1 \times L)^2, \mathrm{C}_2 = (\mathrm{k}_2 \times L)^2, \mathrm{k}_1 = 0.01, \mathrm{k}_2 = 0.02, L = 255$$

and $\mu_x, \mu_y, \sigma_x, \sigma_y$, σ_{xy} show the mean value, variance and covariances value of the host and decrypted host image. Table 5 and Table 6 show the SSIM of different images and SSIM values of different algorithm. In Table 5, we observed the values of SSIM of all images are near by 1, that means the decrypted image is very similar to host image. Hence, the proposed mechanism has good performance in SSIM and good quality of recover and reconstructed host image.

Table 5. SSIM values of different image

Plain Image	SSIM
Lena	0.9437
Pepper	0.9186
Mandrill,	0.9289
Man	0.9187
Cameraman	0.9184

Table 6. SSIM Values of different algorithm image

Image	Ref. [33]	Ref. [28]	our
Lena	0.6211	0.9373	0.9437
Man	0.5553	0.9101	0.9187

4.6 Time of encryption mechanism

Time analysis is the one of the most difficult and interesting work for development of algorithm in different field. Table 7 and Table 8 shows the time taken to encrypt the different host image, similarly time taken to encrypt the image based on different algorithms.

Table 7. Encryption time with different images

Plain Image	Time
Lena	0.019621
Cameraman	0.019787
Pepper	0.206430
Mandrill	0.036545
Man	0.046548

Table 8. Encryption time of different algorithm and image

Image	Ref. [33]	Ref. [28]	our
Lena	0.03178	0.0198	0.0196
Man	0.10380	0.0545	0.0465

5. CONCLUSIONS

This work mainly focuses on the security mechanism of host image information. To secure the information, this paper produced a new compression based image encryption mechanism based on pixel scrambling, random pixel exchange and measurement matrix. Here dual security mechanism is already achieved for multi-level encryption are applied. Initially, host image is decomposed into their frequency component and then scrambled. Each block of host image is scrambled based on pixel exchange procedure. Finally, second level of security mechanism is applied i.e. measurement matrix is used to dual security mechanism to encrypt the host image. The results shown is various table and graphs, it also compares to the existing approach.

REFERENCES

[1] Zhu, S., Zhu, C., Wang, W. (2018). A new image encryption algorithm based on chaos and secure hash SHA-256. Entropy, 20(9): 716. https://doi.org/10.3390/e20090716

[2] Cao, C., Sun, K., Liu, W. (2018). A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map. Signal Processing, 143: 122-133. https://doi.org/10.1016/j.sigpro.2017.08.020

[3] Wang, H., Xiao, D., Chen, X., Huang, H. (2018). Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. Signal Processing, 144: 444-452. https://doi.org/10.1016/j.sigpro.2017.11.005

[4] Yang, F., Mou, J., Ma, C., Cao, Y. (2020). Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. Optics and Lasers in Engineering, 129: 106031. https://doi.org/10.1016/j.optlaseng.2020.106031

[5] Chai, X., Fu, X., Gan, Z., Lu, Y., Chen, Y. (2019). A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Processing, 155: 44-62. https://doi.org/10.1016/j.sigpro.2018.09.029

[6] Zhang, Y., Xiao, D., Wen, W., Wong, K.W. (2014). On the security of symmetric ciphers based on DNA coding. Information Sciences, 289: 254-261. https://doi.org/10.1016/j.ins.2014.08.005

[7] Zhang, L.M., Sun, K.H., Liu, W.H., He, S.B. (2017). A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations. Chinese Physics B, 26(10): 100504. https://doi.org/10.1088/1674-1056/26/10/100504

[8] Zhu, C., Wang, G., Sun, K. (2018). Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box. Symmetry, 10(9): 399. https://doi.org/10.3390/sym10090399

[9] Zhu, S., Wang, G., Zhu, C. (2019). A secure and fast image encryption scheme based on double chaotic S-boxes. Entropy, 21(8): 790. https://doi.org/10.3390/e21080790

[10] Liu, X., Cao, Y., Lu, P., Lu, X., Li, Y. (2013). Optical image encryption technique based on compressed sensing and Arnold transformation. Optik, 124(24): 6590-6593. https://doi.org/10.1016/j.ijleo.2013.05.092

[11] Candès, E.J., Romberg, J., Tao, T. (2006). Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. IEEE Transactions on Information Theory, 52(2): 489-509. https://doi.org/10.1109/TIT.2005.862083

[12] Candès, E.J. (2006). Compressive sampling. In Proceedings of the International Congress of Mathematicians, 3: 1433-1452.

[13] Donoho, D.L. (2006). Compressed sensing. IEEE Transactions on Information Theory, 52(4): 1289-1306. https://doi.org/10.1109/TIT.2006.871582

[14] Huang, R., Sakurai, K. (2011). A robust and compression-combined digital image encryption method based on compressive sensing. In 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 105-108. https://doi.org/10.1109/IIHMSP.2011.53

[15] Endra, R.S. (2013). Compressive sensing-based image encryption with optimized sensing matrix. In 2013 IEEE International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM), pp. 122-125. https://doi.org/10.1109/CyberneticsCom.2013.6865794

[16] Xu, Q., Sun, K., Cao, C., Zhu, C. (2019). A fast image encryption algorithm based on compressive sensing and hyperchaotic map. Optics and Lasers in Engineering, 121: 203-214. https://doi.org/10.1016/j.optlaseng.2019.04.011

[17] Shruthi, K.M., Sheela, S., Sathyanarayana, S.V. (2014). Image encryption scheme with key sequences based on chaotic functions. In 2014 International Conference on Contemporary Computing and Informatics (IC3I), pp. 823-827. https://doi.org/10.1109/IC3I.2014.7019667

[18] Gong, L., Deng, C., Pan, S., Zhou, N. (2018). Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform. Optics & Laser Technology, 103: 48-58. https://doi.org/10.1016/j.optlastec.2018.01.007

[19] Gong, L., Qiu, K., Deng, C., Zhou, N. (2019). An image compression and encryption algorithm based on chaotic system and compressive sensing. Optics & Laser Technology, 115: 257-267. https://doi.org/10.1016/j.optlastec.2019.01.039

[20] Ponuma, R., Amutha, R., Haritha, B. (2018).

Compressive sensing and hyper-chaos based image compression-encryption. In 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), pp. 1-5. https://doi.org/10.1109/AEEICB.2018.8480989

[21] Zhang, X., Ren, Y., Feng, G., Qian, Z. (2011). Compressing encrypted image using compressive sensing. In 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 222-225. https://doi.org/10.1109/IIHMSP.2011.12

[22] Chai, X., Zheng, X., Gan, Z., Han, D., Chen, Y. (2018). An image encryption algorithm based on chaotic system and compressive sensing. Signal Processing, 148: 124-144. https://doi.org/10.1016/j.sigpro.2018.02.007

[23] Chen, J., Zhang, Y., Qi, L., Fu, C., Xu, L. (2018). Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression. Optics & Laser Technology, 99: 238-248. https://doi.org/10.1016/j.optlastec.2017.09.008

[24] Chen, X.D., Liu, Q., Wang, J., Wang, Q.H. (2018). Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction. Optics & Laser Technology, 107: 302-312. https://doi.org/10.1016/j.optlastec.2018.06.016

[25] Tiwari, D., Dixit, M., Gupta, K. (2021). Deep multi-view breast cancer detection: A multi-view concatenated infrared thermal images based breast cancer detection system using deep transfer learning. Traitement du Signal, 38(6): 1699-1711. https://doi.org/10.18280/ts.380613

[26] Jayaswal, R., Dixit, M. (2021). Detection of hidden facial surface masking in stored and real time captured images: A deep learning perspective in COVID time. Traitement du Signal, 38(6): 1875-1885. https://doi.org/10.18280/ts.380632

[27] Singh, R.K., Shaw, D.K. (2018). A hybrid concept of cryptography and dual watermarking (LSB_DCT) for data security. International Journal of Information Security and Privacy (IJISP), 12(1): 1-12. https://doi.org/10.4018/IJISP.2018010101

[28] Brahim, A.H., Pacha, A.A., Said, N.H. (2020). Image encryption based on compressive sensing and chaos systems. Optics & Laser Technology, 132: 106489. https://doi.org/10.1016/j.optlastec.2020.106489

[29] Xu, Q., Sun, K., He, S., Zhu, C. (2020). An effective image encryption algorithm based on compressive sensing and 2D-SLIM. Optics and Lasers in Engineering, 134: 106178. https://doi.org/10.1016/j.optlaseng.2020.106178

[30] Zhou, N., Li, H., Wang, D., Pan, S., Zhou, Z. (2015). Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform. Optics Communications, 343: 10-21. https://doi.org/10.1016/j.optcom.2014.12.084

[31] Zhou, N., Pan, S., Cheng, S., Zhou, Z. (2016). Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing. Optics & Laser Technology, 82: 121-133. https://doi.org/10.1016/j.optlastec.2016.02.018

[32] Luo, Y., Lin, J., Liu, J., Wei, D., Cao, L., Zhou, R., Ding, X. (2019). A robust image encryption algorithm based on Chua's circuit and compressive sensing. Signal Processing, 161: 227-247. https://doi.org/10.1016/j.sigpro.2019.03.022

[33] Xu, Q., Sun, K., Cao, C., Zhu, C. (2019). A fast image encryption algorithm based on compressive sensing and hyperchaotic map. Optics and Lasers in Engineering, 121: 203-214. https://doi.org/10.1016/j.optlaseng.2019.04.011

[34] Zhou, N., Zhang, A., Wu, J., Pei, D., Yang, Y. (2014). Novel hybrid image compression–encryption algorithm based on compressive sensing. Optik, 125(18): 5075-5080. https://doi.org/10.1016/j.ijleo.2014.06.054