Received: December 10, 2020. Revised: February 22, 2021. 11

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Novel Approach based on Compressive Sensing and Fractional Wavelet Transform for Secure Image Transmission

Anil Kumar Chatamoni[1]* **Rajendra Naik Bhukya[1]** **Praneet Raj Jeripotula[1]**

[1] *Department of Electronics and Commination Engineering,*
University College of Engineering, Osmania University, Hyderabad, India
* Corresponding author's Email: anilkumarou2016@gmail.com

Abstract: In this paper, a novel scheme for secure image transmission based on compressive sensing (CS) and Fractional Wavelet Transform (FrWT) is proposed. The scheme uses CS and a multi chaotic pseudo random Sine-Tent- Hénon (STH) map based measurement matrix, in the first stage of encryption. Therefore, it provides a simultaneous compression and encryption. Then the security is further enhanced through the novel approach in the second stage of encryption with an iterative procedure, in which a combination of FrWT and random pixel exchange method is applied. The key parameters used in the generation of random matrix, measurement matrix and fractional orders of FrWT are served as keys. This approach has the larger key parameters provided by the STH map and high degree of scrambling and diffusion with FrWT. With the simulation results, the novel proposed scheme has better compression performance as the PSNR value is 35.6631 dB with 0.75 compression ratio and above 25dB with only 4950 coefficients in the reconstruction of image. When the different types of attacks applied, the value of PSNR in the range of 20-30dB shows the good reconstruction robustness of the proposed scheme. Numerical value comparison with other recent CS based encryption schemes, represents the superiority of the proposed scheme in terms of security.

Keywords: Compressive sensing, Chaotic map, Fractional wavelet transform, Random pixel exchange, Image encryption, Image compression, PSNR.

1. Introduction

Content protection is the major issue in today's 5G scenario due to great usage of images in the Internet. When the data is transmitted on the wireless channel, user privacy is more essential because there is a chance of sensitive information leakage. The information security plays a major role in concern of individual privacy and national security.

Many chaotic based encryption algorithms are proposed due to the advantage of its key sensitivity. A large image data can transfer with efficient encryption scheme, it is possible only when considering compression is a part it.

Recently, chaos based image encryption schemes have been proposed [1-3]. Image encryption is a combination of scrambling and diffusion [4].

X. Wang and P. Liu, [1] proposed a new image encryption scheme based on a new one-dimensional sine chaotic system (1DSCS) with large parameter interval. In this algorithm, dynamic Arnold map combines with row-column index scrambling and a remainder selection diffusion method is performed. 1D chaotic maps are in simple structure and easy to implement but they have the drawbacks of vulnerability and finite chaotic ranges.

On the other hand, HD (higher dimensional) chaotic maps have better chaotic behaviour and more complex structures. Due to high computational cost, HD chaotic map systems are replaced with an image encryption scheme based on the hyper-chaotic system [5].

H. Xu and H. Jiang, [2] proposed a new hyper chaotic image encryption algorithm. A combination of new hénon chaotic system, and 2-dimension logistic chaotic system is used. In [3] A. P. Kari et al. proposed an image cryptosystem based on hybrid chaotic maps. In this scheme, Arnold's cat map is

used to perform confusion phase. Four hybrid chaotic systems based on Sine map, Tent map and Logistic map are used to perform diffusion phase. With the analysis and simulations, hybrid chaotic maps have the excellent chaotic ness.

Compressive sensing (CS) [7] is a candidature, provides the compression and encryption at a time. N. Zhou et al., [8] considered the measurement matrix as key. These type of schemes are having the drawback of large storage space and less resistance to chosen plaintext attacks.

Encryption schemes based on chaos and CS are proposed [9-11]. Y. Dou and M. Li, [9] proposed an image encryption algorithm based on CS and M sequence. With the help of an improved 1D chaotic system, in the generation of measurement matrix, the computational complexity and storage space are reduced. J. Chen et al., [10] explained a joint image encryption and compression scheme by using SRM (structurally random matrix) followed by the permutation-diffusion. Next, a new image compression-encryption algorithm proposed by S. Zhu and C. Zhu, [11], where CS performed on scrambled pixels with Chebyshev mapping and then a cyclic-shift function is applied for image diffusion. X. Chai et al., [12] proposed an encryption algorithm based on CS, elementary cellular automata (ECA) and the memristive chaotic system, Firstly, the sparse coefficient matrix is generated by applying DWT on plain image. The combination of ECA (elementary cellular automata) and zigzag method is adopted for the scrambling of sparse coefficient matrix. The measurement matrix is generated by the memristive chaotic system. CS technique applied on the scrambled coefficient matrix and measurement matrix to ensure the encryption. The initial configurations of the ECA, the zigzag process parameters and the initial values of the chaotic system are generated with the SHA 512 hash function.

Q. Xu et al., [13] presented a fast image encryption algorithm based on CS and a two-dimensional Sine improved Logistic iterative chaotic map with infinite collapse (ICMIC) modulation (2D-SLIM) map. SHA- 512 is used to generate the parameters and initial values of the 2D-SLIM map. The chaotic sequences generated by the 2D-SLIM map are used to create the measurement matrix. Hyperchaotic sequences are used to generate the two circular measurement matrices. Then the CS technique applied on the transform coefficients in two directions to ensure the initial encryption and compression. Further, a two times iterative procedure with a combination of row encryption followed by column encryption is used to obtain the second level encryption. Here the diffusion and permutation are simultaneously executed with row and column encryption algorithm.

In addition to these, in the implementation process of the schemes [14, 15], initially image was encrypted by CS, and then the resultant measured coefficients are scrambled with the chaotic map to generate the final encrypted image, but it increases the computational budget.

Q. Xu et al., [16] presented an image encryption scheme based on CS and a hyperchaotic map. SHA-512 is used to generate the parameters and initial values of the 2D-SLIM map. Before CS, row and column permutations are applied on the transform coefficients of the plain image to acquire a good scrambling effect. The chaotic sequences generated by the 2D-SLIM map are used to create the measurement matrix. Next, CS performed on the scrambled data with measurement matrix to ensure the initial encryption. Further, Galois field multiplication based diffusion algorithm is designed to obtain final encryption.

The fractional wavelet transform [FrWT) [17, 18] generates a continuous change in details representation with respect to transform orders. It is a Fractional version of wavelet transform, provides additional keys in the form of fractional orders in the encryption process. Therefore, this gives more flexibility in the security operations. The merger of random pixel exchange and FrWT yields better encryption algorithm.

In this paper, a joint compression and encryption algorithm is developed with the use of compressive sensing, chaotic map, FrWT and random pixel exchange [19]. A hybrid chaotic sine-tent- hénon (STH) [20] map is used to create the random measurement matrix. Then the CS technique is applied to ensure the initial encryption and compression. Further, the iterative procedure with the combination of FrWT and random pixel exchange is developed to obtain the final encryption. With correct key set values, the original image is recovered after performing the decryption process.

The paper organization is as follows: the fundamental concepts required to develop the proposed scheme are introduced in Section 2. Section 3 represents the proposed scheme with detailed description. Section 4 explains the simulation results and numerical analysis of the proposed scheme. In the end, Section 5 represents the concluding remarks.

2. Fundamental theory

In this section, the detailed description of major and fundamental concepts required to build the proposed scheme are explained.

2.1 Compressive sensing

Sparse signal representation is the fundamental concept for compressive sensing (CS) [7] theory. CS performs concurrent signal sampling and compression with sampling rate is lower the Nyquist frequency. In CS theory, the necessary information is conquered with a small number of compressed measurements.

Assume the signal of interest $X \in \Re^{N\times 1}$ is a real valued signal with K sparsity ($\|X\|_0 \leq K$) means it consists a few significant (or non-zero) values.

Let the sensing matrix $\Phi \in \Re^{M\times N}$ ($M \ll N$).The signal acquisition through linear measurements is given as

$$Y = \Phi \mathrm{X} \tag{1}$$

where measurement vector $Y \in \Re^{M\times 1}$ gives the CS measurements. The input N-dimensional signal is directly transformed into an M -dimensional measurements by means of $M \times N$ measurement matrix. This sampling method gives the noticeable compression effect.

The sparse signal X recovered from the measurement vector Y by solving the minimization problem

$$\hat{X} = \arg\min_{X} \|X\|_0 \quad such\ that\ Y = \Phi \mathrm{X} \tag{2}$$

The above NP-hard l_0-norm replaced with l_1-norm which is defined as

$$\hat{X} = \arg\min_{X} \|X\|_1 \quad such\ that\ Y = \Phi \mathrm{X} \tag{3}$$

for sufficient large M ($M \geq cKlog(N)$). Where c is constant. There are many solutions existed in the literature. One of the greedy algorithm, OMP (orthogonal matching pursuit) is efficiently adapted for the recovery. The efficient signal recovery guarantees when the Φ meets the restricted isometric property (RIP).

Definition: Measurement matrix $\Phi \in \Re^{M\times N}$satisfies the RIP of order K if $\gamma \in (0,1)$ so that

$$(1-\gamma)\|X\|_2^2 \leq \|\Phi X\|_2^2 \leq (1+\gamma)\|X\|_2^2 \tag{4}$$

2.2 Sine-tent- hénon (STH) chaotic map

Chaotic map is deeply sensitive to control parameters and initial values. The sensitivity of initial specifications restrict the prediction capability. The initial conditions are used as a key in the encryption algorithm. Some of the one dimension maps like Sine map and Tent map and one dimensional decomposition Hénon map are expressed in Table 1. One dimensional map consists only one variable and less parameters.

Table 1 different chaotic maps

Map	Function $x(n+1)$
Sine Map	$r[\sin(\pi x(n))]$
Tent Map	$r\|1-2x(n)\|$
Hénon Map	$1-ux(n)^2+\beta x(n-1)$

The iterative one dimensional Sine- Tent- Hénon (STH) chaotic map is expressed as

$$x(n+1) = \left|u - 10\sin^2(\pi x(n)) + (\beta r|1-x(n-1)|)\right| \tag{5}$$

Multi chaotic STH map, is a hybrid one dimensional chaotic system with the combination of Sine map, Tent map and Hénon map. Where $x(0)$ and $x(1)$ are initial values and $\beta, u\, r$, is the chaotic system parameter. STH consists more numbers of variable and parameters compared to other single one dimensional map. The advantages of STH map are it generates a uniformly distributed highly chaotic sequence and it has positive value Lyapunov Exponent (LE) for all the values of $u \in (0,4)$.

2.3 Random measurement matrix generation

The random measurement matrix $\Phi \in R^{M\times N}$ ($M < N$) is generated with the help of iterative one dimensional STH map. By defining the control parameters $\beta, u, r \in (0,4)$ and initial values $x(0), x(1) \in (0,1)$, a chaotic sequence $(\varphi_0, \varphi_1, \varphi_2, .., \varphi_{MN-2}, \varphi_{MN-1})$ is generated. Measurement matrix created with chaotic sequence $\{\varphi_i\}_{i=0}^{MN-1}$ in row by row way. The created measurement matrix is as follows:

$$\Phi = \frac{1}{\sqrt{N}}\begin{pmatrix} \varphi_0 & \varphi_1 & \cdots & \varphi_{N-1} \\ \varphi_N & \varphi_{N+1} & \cdots & \varphi_{2N-1} \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_{MN-N} & \varphi_{MN-N+1} & \cdots & \varphi_{MN-1} \end{pmatrix} \tag{6}$$

where $1/\sqrt{N}$ is used for normalization

2.4 Random pixel exchange method

The image pixel is scrambled based on the secured predesigned key value with the random pixel exchange method.

The image A of size $M \times N$ is equally divided into two parts of either horizontal direction (with

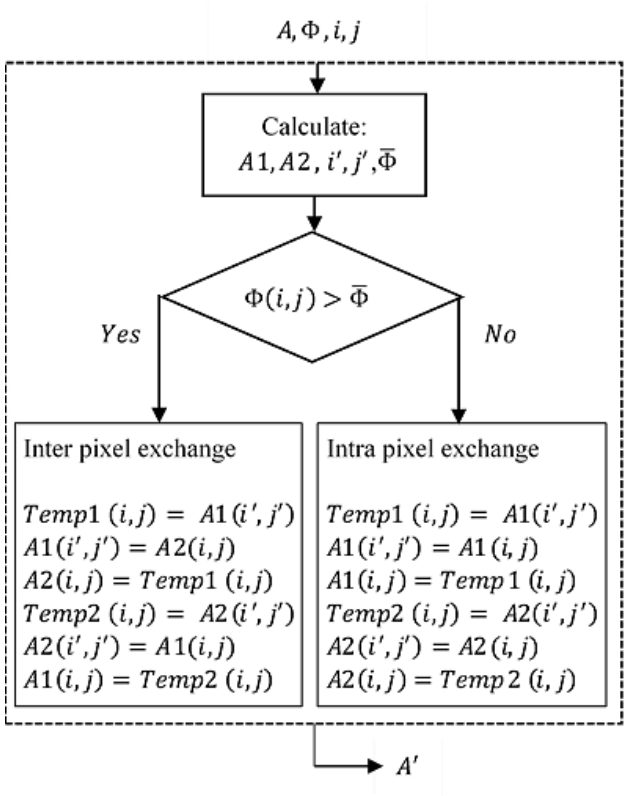


Figure. 1 Random pixel exchange technique

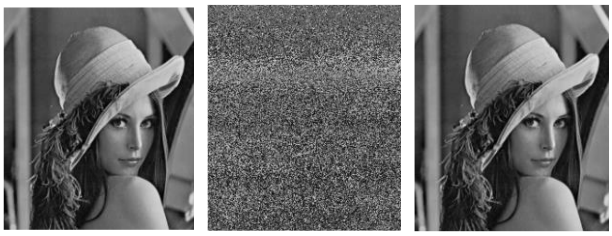
sizes $M/2 \times N$) or vertical direction (with sizes$M \times N/2$). In this procedure, the horizontal direction is considered and top side and bottom side of A are designated as $A1$ and $A2$ respectively. Random pixel exchange method as shown in Fig. 1, is used to scramble the pixels between the two sub images $A1$ and $A2$, which generates a random pattern of the image A.

Consider the primary position of the pixel as (i, j), where variables i and j are the indices of an image. The updated position (i', j') is measured with the following equations.

$$i' = 1 + \text{round}\{(M-1)\sin(\Phi(i,j))\}\ 1 \le i \le M/2 \quad (7)$$

$$j' = 1 + \text{round}\{(\text{N}-1) \times \Phi(i,j)\} \quad 1 \le j \le N \quad (8)$$

Φ is a $M/2 \times N$ size random matrix, generated with STH map and its mean calculated as $\bar{\Phi} = \frac{1}{(M/2)\times N} \sum_{\forall\, i,j} \Phi(i,j)$. *Round* function is used to generate the nearest integer value. Temp1 and Temp2 represents an intermediate variables. Whenever $\Phi(i,j) > \bar{\Phi}$, pixels are exchanged between two sub images (inter pixel exchange) otherwise pixels are exchanged within the same sub images (intra pixel exchange). When all the pixel positions have been dealt with in the operation, a random pattern A' generated as output, which is the encrypted version of the image A.



(a) (b) (c)

Figure. 2: (a) Original image, (b) encrypted image, and (c) decrypted image

The effectiveness of the proposed technique is verified with the following example. A test image of size 256 X 256 and a random matrix of size 128X 256 generated using STH chaotic map are treated as inputs. As the outcome of random pixel exchange, an encrypted image of size 256X 256 is generated. Further, inverse random pixel exchange applied to retrieve the decrypted image with perfect key parameters. Fig. 2 shows the encrypted and decrypted image using random pixel exchange technique.

2.5 Fractional wavelet transform(FrWT)

Fourier Transforms (FT) are most commonly used in the field of engineering. The standard integer order FT makes the domain conversion of a signal from time to frequency, to study the different frequency components presented in the signal. Fourier Transform have the drawback of providing the local time - frequency characteristics of the signal. To overcome this, Fractional Fourier Transform (FrFT), a generalized version of Fourier transform, is used.

The two times repetition of Fourier transform on a signal $f(t)$ is $\mathcal{F}\mathcal{F}\{f(t)\}$ gives $f(-t)$ and four times repetition $\mathcal{F}\mathcal{F}\mathcal{F}\mathcal{F}\{f(t)\}$ gives the original signal $f(t)$. $\mathcal{F}^{\alpha}$ is the general notation of FT where α is the integer number define the number of repetitions. On the other hand, non-integer value of α gives the operation of FrFT. The output of the FrFT is rotated time–frequency representation of the signal. The angle of rotation is defined as $a = \alpha \times 0.5 \times \pi$.

The convention FT of a signal is defined as

$$F(x) = \mathcal{F}\{f(t)\} = \int_{-\infty}^{\infty} f(t)\ e^{-i2\pi tx} dt \quad (9)$$

The α order FrFT is

$$F^{\alpha}(x) = \mathcal{F}^{\alpha}\{f(t)\} = \int_{-\infty}^{\infty} f(t) K_{\alpha}(t,x)\ dt \quad (10)$$

where transform kernel $K_\alpha(t,x)$ is is expressed as

$$K_\alpha(t,x) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2}} \times \\ e^{i(x^2/2)\cot\alpha} e^{i(t^2/2)\cot\alpha - jxt\ cosec\ \alpha} & for\ \alpha \neq 2\pi \\ \delta(t-x) & for\ \alpha = 2n\pi \\ \delta(t+x) & for\ \alpha = (2n-1)\pi \end{cases}$$

The two dimensional FrFT is

$$F^{\alpha_1,\alpha_2}(x,y) = \mathcal{F}^{\alpha_1,\alpha_2}\{f(t_1,t_2)\} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(t) K_{\alpha_1,\alpha_2}(t_1,t_2,x,y)\ dt_1 dt_2 \quad (11)$$

and its inverse transform is

$$f(t_1,t_2) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(t) K_{-\alpha_1,-\alpha_2}(t_1,t_2,x,y)\, F^{\alpha_1,\alpha_2}(x,y)\, dxdy \quad (12)$$

The conventional wavelet transform is defined as

$$W(s,\tau) = \int_{-\infty}^{\infty} f(t)\psi^*(t)\, dt \quad (13)$$

where $\psi^*(t) = \frac{1}{\sqrt{s}}\psi\left(\frac{t-\tau}{s}\right)$ is the mother wavelet, s is the scaling value and τ is the translation value

FrWT is a consolidation of wavelet Transform (WT) and FrFT, used to derive the spectrum of signal. Mendlovic et al. [21], introduced the FrWT and the α order FrWT is defined as

$$W^\alpha(s,\tau) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(t) K_\alpha(t,x)\psi_{s,\tau}(x)\, dtdx \quad (14)$$

The FrWT kernel $k_\alpha(t,x)$ is given by

$$K_\alpha(t,x) = \frac{e^{-\frac{i}{2}\left(\frac{\pi}{2}sgn(\sin\bar{\alpha})-\bar{\alpha}\right)}}{\sqrt{2\pi|(\sin\bar{\alpha})|}} e^{(i/2)\left(t^2+x^2\right)\cot\bar{\alpha}}\ e^{-itx\csc\bar{\alpha}} \quad (15)$$

The inverse FrWT is illustrated as

$$f(t) = \frac{1}{\mathrm{C}}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} W^\alpha(s,\tau) K_{-\alpha}(t,x)\psi_{s,\tau}(x)\frac{dsd\tau dx}{s^2} \quad (16)$$

where $\mathrm{C} = \int_{-\infty}^{\infty}\frac{|\tilde{\psi}(u)|^2}{|u|}du$. FwFT is periodic over the range $\alpha \in (0,4)$.

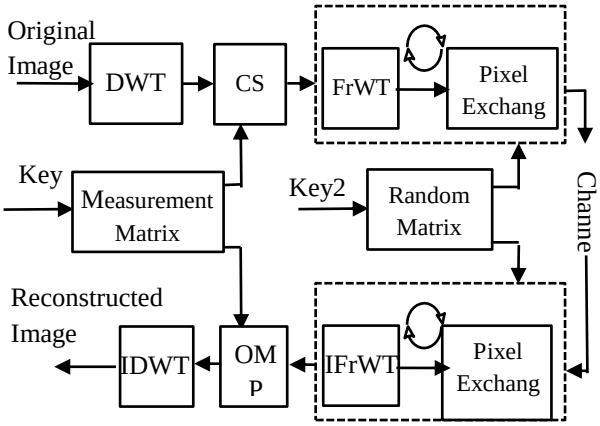


Figure. 3 Proposed scheme

3. The proposed scheme

The novel scheme for simultaneous image compression and encryption is depicted in Fig. 2. In this section, a detailed step wise procedure of encryption process followed by decryption process are explained.

3.1 Encryption process

The original image is transformed into sparse with the help of some transform basis, and performed the CS operation to generate the measured coefficients with a key based measurement matrix. This gives the initial encryption and compression. The subsequent encryption obtained by encrypting the measured coefficients with iterative operation together with FrWT and random pixel exchange. The stepwise procedure is as follows.

Step 1: Sparse representation

The original Image I of size $N \times N$ is transformed into the discrete wavelet transform (DWT) domain. A 2-level decomposition performed to generate the sparse coefficient matrix with most of the elements are close to zero. The sparsity of the resultant matrix considered as K.

$$A = DWT\ [I] \quad (17)$$

Step 2: Measurement matrix generation

A $M \times N$ size measurement matrix Φ_1, is generated using STH map. With control parameters (β_1, u_1, r_1) and initial values $(Z_1^0,\ Z_1^1)$, a $MN-1$ length chaotic sequence generated according to Eq. (5). These set of parameters considered as Key1. The $M \times N$ measurement matrix is constructed matching with Eq. (6). The size of the M should satisfy $M \geq K\log(N)$ and RIP conditions. Here M considered as 192.

Step 3: Measured coefficients

Performed compressive sensing with sparse image A and measurement matrix Φ_1 in accordance with Eq. (1), to generate measured coefficient matrix (Y) of size $M \times N$. The cipher image Y gives the simultaneous compression and encryption.

$$Y = \Phi_1 A \tag{18}$$

Meanwhile, this process is considered as initial encryption and parameter set Key1 served as key.

Step 4: Random matrix generation

Similar to Step 2, a $M/2 \times N$ size random matrix Φ_2, is generated with initial values (Z_2^0, Z_2^1) and control parameters (β_2, u_2, r_2) and these parameter set is considered as Key2.

Step 5: Encryption of measured coefficients

The measured coefficient matrix Y is equally divided into two parts Y_1 and Y_2 in horizontal direction and each part having size of $M/2 \times N$.

Composed a new complex number Y_c by considering Y_1 as real part and Y_2 as imaginary part

$$Y_c = Y_1 + i\, Y_2 \tag{19}$$

Applied two dimensional FrWT on Y_c with fractional orders α^1 in x and α^2 in y results,

$$Y_c' = \text{FrWT}(Y_c) \tag{20}$$

and extracted real part and imaginary part are as follows

$$Y_1' = real(Y_c') \tag{21}$$

$$Y_2' = imag(Y_c') \tag{22}$$

Performed the random pixel exchange method between Y_1' and Y_2' as explained in Section 2.4. The resultant real and imaginary parts are used to compose the new complex number in the next iteration.

After p iterations, the ciphertext Y' generated, which is the final encrypted image. The set of fractional orders in the iteration procedure is considered as Key3. In the proposed scheme $p = 2$.

3.2 Decryption process

The stepwise procedure of decompression and decryption is as follows

Step 1: Decryption of measured coefficients

The decryption is same and opposite of encryption. Performed an iterative procedure with random pixel exchange and inverse FrWT (IFrWT) with correct key sets Key2 and Key3 to get the decrypted measurement coefficients.

Step 2: Restoration of measurement coefficients

Obtain the measurement matrix using STH map with key set Key1. The OMP algorithm is applied on the decrypted measurement coefficients, to restore the measurement coefficients

Step 3: Reconstruction of original image

To recover the original image, applied inverse DWT (IDWT) on the restored measurement coefficients.

4. Simulation results and analysis

Desktop used is Intel(R)Core(TM) i7-6700CPU @ 3.40 GHz, 64 bit windows 10 with 8 GB RAM. Simulations are carried out to implement the proposed algorithm in MATLAB R2019a. In this section, simulation results, different security analysis methods followed by comparison with other CS based encryption schemes are discussed.

4.1 Simulation results

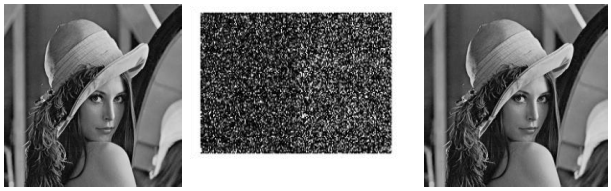
A 256-scale gray image with 256×256 pixels, as shown in Fig. 5 (a), is considered as original image. The size of the chaotic measurement matrix is 192×256 and chaotic random matrix size is 81×256. In Table 2, the key specifications are indexed.

The cipher image after compression and encryption of size 192×256 is shown Fig. 4 (b). The cipher image is totally changed into confusion and no correct information leakage of corresponding original image.

The original image is recovered with correct key set after decryption and decompression as shown in Fig. 4 (c). The encrypted image size is less compared to the size of original and recovered image, thus the proposed algorithm implemented the simultaneous compression and encryption.

Table 2. Key specifications for the simulation

Description	Value
For Measurement matrix	
Initial values $(Z_1^0\ Z_1^1)$	(0.35,0.69)
Control parameters (β_1, u_1, r_1)	(0.6387,0.4862,0.9256)
For Random matrix	
Initial values $(Z_2^0\ , Z_2^1)$	(0.01,0.95)
Control parameters (β_2, u_2, r_2)	(0.8929,0.2365,0.9876)
FrWT orders (α_1^1, α_1^2)	(0.67,0.91)
FrWT orders (α_2^1, α_2^2)	(0.59,0.16)



(a) (b) (c)

Figure. 4 Test results on image "Lena": (a) original image, (b) encrypted image, and (c) recovered image

4.2 Compression performance

The PSNR (peak -signal to -noise -ratio) metric is considered to evaluate the performance of image recovery and it is defined as

$$PSNR = 20\log_{10}\left(f_{max}/\sqrt{MSE}\right) \quad (23)$$

where $f_{max} = 255$, which is the maximum value presented in the image and mean squared error (MSE) estimated as

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left\|f(i,j) - \hat{f}(i,j)\right\|^2 \quad (24)$$

The resultant PSNR value in this case is 35.6631 dB, an adequate performance value in image recovery. The PSNR curves with different number of measured coefficients used in the image recovery at the receiver side on Lena image, Cameraman image and Boat image is shown in Fig 5.

From Fig. 5, it is observed that, with 4950 coefficients in reconstruction, PSNR of the image recovery is above 25dB, which implies good performance is possible with fewer measurements with the proposed scheme.

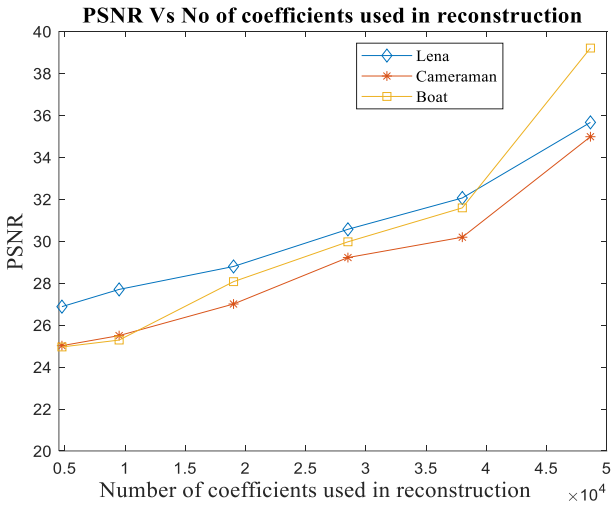
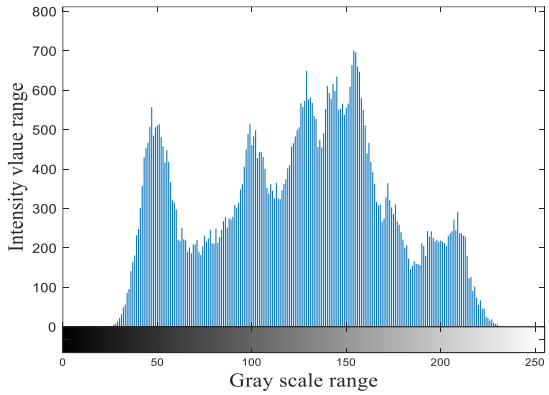
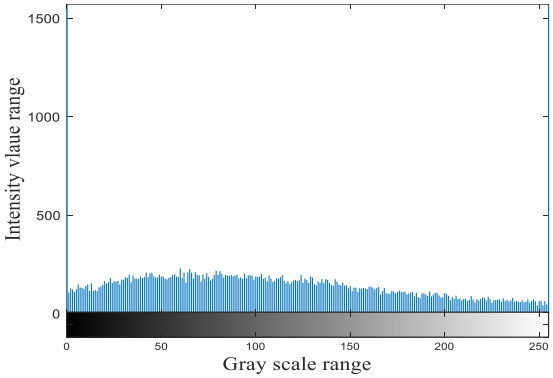


Figure. 5 PSNR graphs with different number of measurements

(a) (b)



(c)



(d)

Figure. 6 Histogram analysis with "Lena" image

4.3 Security analysis

The security analysis is evaluated in terms of histogram, correlation coefficient and information entropy.

4.3.1. Histogram

An image histogram defines the pictorial description of pixel intensities. The quality of the encryption is determined based on the pixel distribution in histogram representation. The original image histogram as shown in Fig. 6(c) has unique pattern, which ease the attackers to understand the image data with statistical analysis.

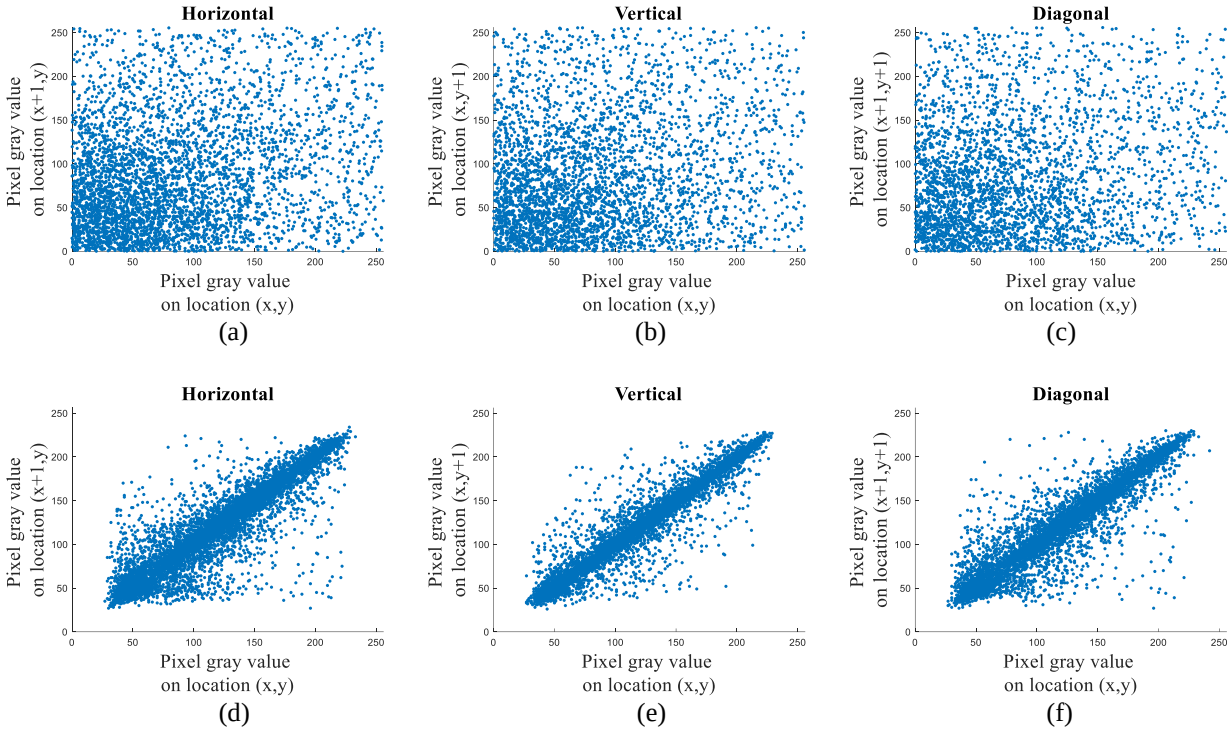


Figure. 7: Correlation of adjacent pixel in "Lena" image

On the other hand, the encrypted image histogram as shown in Fig. 6 (d) has uniformly distributed which defence against the statistical attacks.

4.3.2. Correlation coefficient

The adjacent pixels correlation is to be low for effective encryption scheme. That means, correlation value is to be high in the original plain image and low in the encrypted image. In this analysis, considered the sample data as 4000 randomly selected pixels in horizontal, vertical and diagonal directions from both original image and encrypted images. Figs. 7 (a)-(c) shows the correlation plots of original Lena image and Figs. 7 (d)-(e) shows the correlation plots of encrypted Lena image in horizontal, vertical and diagonal directions respectively. In Fig. 7, the pixel distribution of original image in horizontal, vertical and diagonal directions has a unique pattern which leads to unsecure. Whereas the pixel distribution of encrypted image in horizontal, vertical and diagonal directions has a uniform pattern which ensures the image security.

Consider the adjacent pixel pairs (x_i, y_i) with $i = 1,2,..,T$. where T is the randomly selected pixel value. The correlation coefficient (CC) between $x = \{x_i\}$ and $y = \{y_i\}$ is defined as

$$CC = \frac{\frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))(y_i - E(y))}{\sqrt{\frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2}\sqrt{\frac{1}{T}\sum_{i=1}^{T}(y_i - E(y))^2}} \quad (25)$$

where $E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i$, $E(y) = \frac{1}{T}\sum_{i=1}^{T} y_i$.

The correlation coefficient values of both the original and encrypted image are listed in Table 3.

Table 3. The correlation coefficient values

Image	Direction	Original image	Encrypted image
Lena	Horizontal	0.96890	0.00014
	Vertical	0.96627	0.00017
	Diagonal	0.95547	-0.01710
Cameraman	Horizontal	0.93571	0.00013
	Vertical	0.95561	0.00054
	Diagonal	0.93143	0.00065
Boat	Horizontal	0.95596	0.01710
	Vertical	0.91827	0.00065
	Diagonal	0.94218	-0.00410

We can notice that, the CC value of the original image near to 1, which indicates the strong correlation between adjacent pixels. After encryption pixels are scattered with good scrambling effect and CC value near to 0, which means pixels are uncorrelated leads to a good correlation performance. Therefore, the proposed scheme can strongly defence against statistical attacks.

4.3.3. Information entropy

The strength of pixel randomness is evaluated with the help of information entropy. Theoretically, for a true random 256 grey scale image, the maximum entropy value is 8. The entropy values before and

Table 4. Entropy values

Image	Cameraman	Boat	Lena
Original image	7.0911	7.1905	7.4429
Encrypted image	7.8735	7.9156	7.9985

Table 5. PSNR of encrypted Lena image with modified key parameters

Method	Actual key Value	Modified key Value	PSNR (dB)
For Key1			
Initial value Z_1^0	Z_1^0	Z_1^0 +0.1	0.0125
Initial value Z_1^1	Z_1^1	Z_1^1 +0.01	0.0065
Control parameter β_1	β_1	β_1 +0.1	0.0115
Control parameter u_1	u_1	$u_1 + 0.01$	0.0568
Control parameter r_1	r_1	β_1+0.01	0.0365
For Key2			
Initial value Z_2^0	Z_2^0	Z_2^0 +0.1	0.0990
Initial value Z_2^1	Z_2^1	Z_2^1 +0.05	0.0578
Control parameter β_2	β_2	β_2 +0.005	0.0706
Control parameter u_2	u_2	$u_2 + 0.1$	0.0005
Control parameter r_2	r_2	r_2+0.01	0.0569
For Key3			
FrWT order α_1^1	α_1^1	α_1^1 +0.06	0.0005
FrWT order α_1^2	α_1^2	α_1^2 +0.5	0.0063
FrWT order α_2^1	α_2^1	α_2^1 +0.001	0.0002
FrWT order α_2^2	α_2^2	α_2^2 +0.02	0.0018

after encryption are listed in Table 4. The values in table represents the proposed scheme provides performance guarantee against brute force attack.

4.4 Key sensitivity analysis

Small changes in key value effects the image recovery, this is analysed through key sensitive analysis. In this proposed scheme, with correct key set, the original Lena image recovered with 35.6631 dB. Table 5 shows the PSNR values with tiny variation in initial key values. It is observed that, the proposed scheme is more sensitive to the initial key parameters.

4.5 Noise attack analysis

The effect of noise on encrypted image exist during the transmission over noisy channel. The efficiency of the encryption algorithm depends on reconstruction robustness.

The proposed scheme tested with different noise attacks on encrypted Lena image and corresponding PSNR values are shown in Table 6. The PSNR values are in acceptable range even though the noise intensities are increases. With this, the proposed scheme is strongly oppose the noise attacks.

Table 6. Different attacks on encrypted lena image

Attack	PSNR(dB)
No attack	35.6631
Gaussian Noise ($\sigma = 5$)	26.6188
Gaussian Noise ($\sigma = 10$)	24.5379
Salt & pepper noise with 20% density	25.6188
Salt & pepper noise with 50% density	23.0163
Speckle noise with 0.02 variance	26.6188
Speckle noise with 0.04 variance	26.4289

4.6 Comparison

Compared the proposed scheme with latest CS based encryption schemes [12-13, 16] in terms of PSNR, correlation coefficients and information entropy. All the algorithms have the same simulation environment as follows. A 256-scale gray image with 256×256 pixels is considered as the original image. After successful compression and encryption, the cipher image size is 192×256.

In [12], the measurement matrix is generated by the memristive chaotic system and the combination of elementary cellular automata (ECA) and zigzag method is applied for the scrambling of sparse coefficient matrix. The cipher image generated with totally permuted sparse matrix applied on CS. This method provides the single level encryption. In the method proposed in [13], the initial encryption obtained with CS and 2D SLIM map. Further the security improved with the row encryption and column encryption in the second level. The 2D-SLIM map is used to generate sequences in the complete scheme. This method has two level encryption without any permutations in sparse matrix. As shown in Fig. 8, the extended version is proposed in [16], has three steps to generate the cipher image. First, the sparse coefficient matrix is permuted and second, applied the CS on permuted matrix to ensure the initial encryption. Finally, diffuse the compressed matrix with GF multiplication to get the cipher image.

information entropy comparison. The proposed scheme has good correlation in encrypted image. The proposed scheme has better information entropy value compare to others schemes and near to the reference value 8. With these results, the proposed

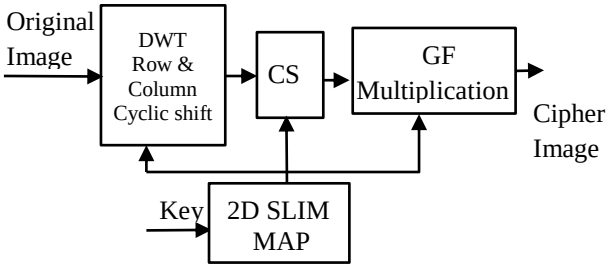


Figure. 8: Comparison model [16]

Table 7. PSNR comparison with different encryption schemes

Scheme	PSNR (dB)
[12]	32.9821
[13]	29.2184
[16]	32.3500
Proposed	**35.6631**

Table 8. Correlation coefficients of encrypted image

Scheme	Correlation coefficients		
	Horizontal	Vertical	Diagonal
[12]	0.0001	-0.0011	-0.0014
[13]	-0.0015	0.0041	0.0069
[16]	0.0064	0.0003	0.0026
Proposed	**0.00014**	**0.00017**	**-0.01710**

Table 9. Information entropy comparison

Scheme	Information Entropy
[12]	7.9968
[13]	7.9935
[16]	7.9960
Proposed	**7.9985**

scheme has better compression and encryption.

5. Conclusion

In this work, a novel image encryption scheme based on compressive sensing and FrWT is proposed. The proposed scheme is a prominent candidate for image encryption with advantage of simultaneous encryption and compression. To increase the system security, a hybrid STH chaotic map is used to generate the CS measurement matrix. Executed the initial encryption with CS and chaotic map, but it has leakage of original image information. An iterative procedure with a combination of FrWT and random pixel exchange applied to get the final encryption. This double encryption achieves good randomness and more robust against attacks. The key parameters used in the generation of measurement matrix, random matrix and fractional orders, are increases the scheme security. The observed concrete results are as follows:

We have conducted several experiments for key sensitivity analysis and noise attack analysis in terms of PSNR. From key sensitive analysis it is observed that, a small change in the key value results the PSNR value near to 0dB. The PSNR value in the range of 20-30dB when the different types of attacks applied in the noise attack analysis. This implies that the proposed scheme has high robustness. With the simulation results, the proposed scheme outperforms the existing approaches in terms of PSNR, correlation coefficients and information entropy.

From the comparison analysis, PSNR value of the proposed scheme has high PSNR values as 35.6631dB when compared with existing methods. In the perspective of correlation coefficients, the proposed scheme has achieved good correlation value (near to the ideal value 0) in three directions when compared with existing methods. Finally, the improved information entropy of proposed scheme is noticed as 7.9985 when compared with existing methods and it is closed to the ideal value 8.

With the test results, the proposed scheme has better compression performance and high security. In addition, due to the proposed scheme advantages, the future work can be further extended to multimedia like video and audio with performance improvement.

Conflicts of Interest

The authors declare that they do not have any conflict of interest.

Author Contributions

A. K. Chatamoni: Conceptualization, software simulation, methodology, investigation, resources, and original draft preparation, Writing - review and editing R.N. Bhukya: Validation, formal analysis, project administration supervision, and funding acquisition. P. R. Jeripotula: Data curation, visualization, Writing - review and editing.

Acknowledgments

“This work is supported by Visvesvaraya PhD Scheme, MeitY, Govt. of India. <MEITY-PHD-1589>”.

References

[1] X. Wang and P. Liu, “A New Image Encryption Scheme Based on a Novel One-Dimensional Chaotic System”, *IEEE Access*, Vol. 8, pp. 174463-174479, 2020.

[2] H. Xu and H. Jiang, “An Image Encryption Schema Based on Hybrid Optimized Chaotic System”, In: *Proc. of International Conf. on Electronic Information Technology and Computer Engineering (EITCE)*, Xiamen, China, pp. 1160-1164, 2019.

[3] A. P. Kari, A. H. Navin, A. M. Bidgoli, and M. Mirnia, “A new image encryption scheme based on hybrid chaotic maps”, *Multimedia Tools and Applications*, Vol. 80, pp.2753–2772, 2021.

[4] X. Wang, L. Feng, and H. Zhao, “Fast image encryption algorithm based on parallel computing system”, *Information Sciences*, Vol. 486, pp. 340-358, 2019.

[5] C. Chen, K. Sun, and S. He, "An improved image encryption algorithm with finite computing precision", *Signal Processing*, Vol. 168, 2020.

[6] S. S. Yu, N. R. Gong, L. H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system", *Optics and Lasers in Engineering*, Vol. 124, 2020.

[7] D. L. Donoho, "Compressed sensing", *IEEE Trans. on Information Theory*, Vol. 52, No. 4, pp. 1289–1306, 2006.

[8] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression – encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing", *Optical Laser Technology*, Vol. 62, pp. 152–160, 2014.

[9] Y. Dou and M. Li, "An Image Encryption Algorithm Based on Compressive Sensing and M Sequence", *IEEE Access*, Vol. 8, pp. 220646-220657, 2020.

[10] J. Chen, Y. Zhang, L. Qi, C. Fu, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression", *Optics & Laser Technology*, Vol. 99, pp. 238-248, 2018.

[11] S. Zhu and C. Zhu, "A new image compression-encryption scheme based on compressive sensing and cyclic shift", *Multimedia Tools and Applications*, Vol. 78, No. 15, pp. 20855–20875, 2019.

[12] 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.

[13] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map", *Optics and Lasers in Engineering*, Vol. 121, pp. 203-214, 2019.

[14] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing", *Optics & Laser Technology*, Vol. 115, pp. 257-267, 2019.

[15] F. Musanna, S. Kumar, "A novel image encryption algorithm using chaotic compressive sensing and nonlinear exponential function", *Journal of Information Security and Applications*, Vol. 54, pp. 1-17, 2020.

[16] Q. Xu, K. Sun, S. He, and C. Zhu, "An effective image encryption algorithm based on compressive sensing and 2D-SLIM", *Optics and Lasers in Engineering*, Vol. 134, pp. 1-12, 2020.

[17] J. Shi, X. Liu, W. Xiang, M. Han, and Q. Zhang, "Novel Fractional Wavelet Packet Transform: Theory, Implementation, and Applications", *IEEE Transactions on Signal Processing*, Vol. 68, pp. 4041-4054, 2020.

[18] J. Wang, Y. Ding, S. Ren, and W. Wang, "Sampling and Reconstruction of Multiband Signals in Multiresolution Subspaces Associated with the Fractional Wavelet Transform", *IEEE Signal Processing Letters*, Vol. 26, No. 1, pp. 174-178, 2019.

[19] C. A. Kumar and B. R. Naik, "A new encrypted image watermarking based on DTCWT and random pixel exchange", In: *Proc. of International Conf. on Advanced Computing & Communication Systems (ICACCS)*, Coimbatore, India, pp. 567-570, 2019.

[20] R. I. Abdelfatah, "Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography", *IEEE Access*, Vol. 8, pp. 3875-3890, 2020.

[21] D. Mendlovic, Z. Zalevsky, D. Mas, J. García and C. Ferreira, "Fractional wavelet transform", *Applied Optics*, Vol. 36 No. 20, pp. 4801-4806, 1997.