Volume 64, Issue 1, 2020
Journal of Scientific Research
Institute of Science,
Banaras Hindu University, Varanasi, India.

A systematic survey on Image Encryption using Compressive Sensing

Saumya Patel*[1] and Ankita Vaish[2]

*[1]Department of computer science, BHU, saumyapatel5@gmail.com
[2]Department of computer science, BHU, av21lko@gmail.com

***Abstract*—In today's world of developing technology, Multimedia transmission through public network is increasing drastically, so there is a need of fast transmission with data security. Compressive Sensing (CS), is a new approach which can acquire the signal in a compressed form. It dimensionally reduces the signal with the help of measurement matrix. Reduction of dimension is totally dependent on the Sparsity. CS has a feature to reconstruct the signal in lesser than the Nyquist sampling rate if the signal is sparse. In the case of transmission, signal security is also a serious concern. CS has an embedded feature of cryptography. It works as a cryptosystem when measurement matrix is shared as a key between the sender and receiver. CS has a vital scope in medical imaging, video acquisition etc. Many researchers have tried to encrypt the signal with the help of different chaos based measurement matrix. This paper gives a detailed survey and critical analysis on the image encryption techniques using CS which can help the naive researchers to excel the field.**

***Index Terms*—Compressive Sensing, Sparsity, Measurement matrix, Image encryption, Reconstruction**

I. Introduction

With the rapid development of multimedia transmission through the public network, security is a serious concern in the transformation and storage of the signal. For the fast and secure transmission of signal, the signal must be in a compressed and encrypted form. Encryption converts the signal into another form which is difficult to understand. Encryption is required because it will keep the information confidential between sender and receiver. Compression is required for fast transmission and efficient storage of the information.

In 1949, Shannon-Nyquist has proposed an algorithm, which states that the sampling rate should be more than twice of the maximum frequency for perfect reconstruction of the signal. D. L. Donoho (2006) has introduced a new concept called Compressive Sensing (CS) for signal acquisition. Candes et al. (2008) has given a detailed theoretical knowledge about CS. Foucart et al. (2017) has given a mathematical overview on CS. It is quite different from the Nyquist sampling shown in the figure 1. CS has some inherent features through which compression as well as encryption is possible. CS compresses the signal in less than the twice of the maximum frequency of the signal. CS has two important requirements measurement matrix and reconstruction algorithm. CS states that if the signal is sparse then it can be compressed. Sparsity means signal has some non-zero values which contain most of the information of the signal. Measurement matrix is responsible for the compression. If measurement matrix is shared between the sender and receiver as a key then CS works as a cryptosystem. Although there are good research papers on image encryption, which covers systematic review. But in our knowledge there is a lack of a survey which covers CS based encryption. This paper provides a survey on image encryption using CS. The organization of paper is as follows: The basic background of cryptography, sparsity and CS is discussed in section 2. Preliminaries of encryption is discussed in section 3. A detailed review is discussed in section 4. Finally, the conclusions are drawn in section 5.

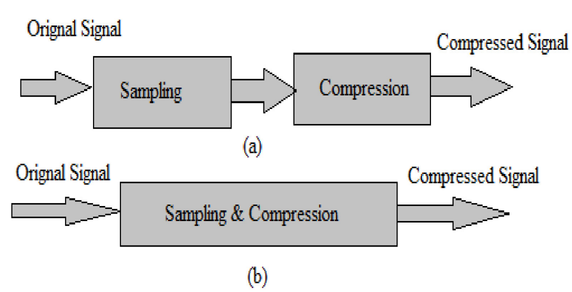

Fig. 1. Difference between traditional and new sampling

*DOI:*http://dx.doi.org/10.37398/JSR.2020.640154

II. Basic Background

A. Encryption

Encryption is a technique in which plain image is converted into cipher image using keys. In cryptography, encryption is used to send confidential signal through public network. To encrypt the signal there are two basic needs: an algorithm to encrypt the signal and a key. Encryption is done at the sender side.

B. Decryption

Decryption is reverse process of encryption. It converts cypher image into plain image. Decryption takes place at the receiver side to obtain readable message from cipher text. Generally same key is used for encryption and decryption as shown in the figure 2.

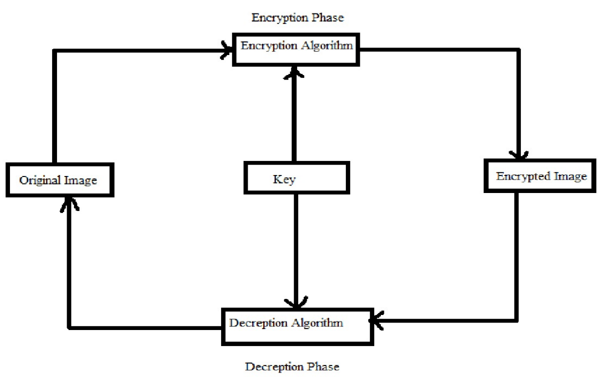

Fig. 2. Encryption-Decryption technique

C. Key

Key can be a numeric, alpha numeric or special symbol. Key is used on both side sender side as well as receiver side. At sender side key is used to encrypt the signal and other side it is used to decrypt the signal. Selection of key is a very important part of the cryptography because security of encrypted signal totally depend on key.

D. Cryptography

Cryptography is a mathematical function which is used to encrypt or decrypt the signal. Cryptography with all protocols and algorithm is known as cryptosystem. Cryptography is capable to provide authentication and better security. There are two main type of cryptography:
(i) Symmetric Key Cryptography
(ii) Asymmetric Key Cryptography

In Symmetric key cryptography, sender and receiver both knows about the secret key. Both uses the same key to encrypt and decrypt the signal. It is also known as secret key cryptography.

In Asymmetric key cryptography, sender and receiver uses a pair of secret key to encrypt and decrypt the signal.

Cryptography is a technique which is used when signal is transmit over the network. Some algorithms are also needed by cryptosystem to encrypt and decrypt the signal.

E. Sparsity

Sparsity states that the signal has less number of non-zero values which contain most of the information. If the signal $A \in R^{N \times N}$ has K non-zero values and rest of values are zero then K is the sparsity of the signal. A signal S shows sparsity in certain orthogonal basis such as Discrete cosine transform (DCT), Discrete wavelet transform (DWT) etc.

$$S(n) = \sum_{i=1}^{N} X_i \varphi_i \tag{1}$$

l_0-norm specifies the sparsity of the signal. It counts the non-zero values in the signal which is the sparsity of the signal. The sparsest solution can be obtained by solving the above equation with l_0-norm. Thus the equation will be:

$$\hat{\varphi} = arg\ min\ ||\varphi||_0 \qquad subject\ to\ \ S = X\varphi \tag{2}$$

If there are only K non-zero elements which are utilized to represent the signal then the optimization problem will be equivalent to:

$$S = X\varphi \quad s.t. \quad ||\varphi||_0 \leq k \tag{3}$$

above is called K-sparse approximation problem.
l_0-norm is a fundamental operation which can obtain sparse φ over the basis X but l_0-norm is still a NP-hard problem. Recent literature has assured that the representation obtained by l_1-norm also follows the condition of sparsity. The solution obtained by l_1-norm is equivalent to the result of l_0-norm. l_1-norm can be solved in a polynomial time and defined as:

$$||a||_1 = |a_1| + |a_2| + |a_3| + ... + |a_n| \tag{4}$$

$$\hat{\varphi} = arg\ min\ ||\varphi||_1 \qquad subject\ to\ \ S = X\varphi \tag{5}$$

l_p-norm is a general method to solve a linear representation. Some researchers are trying to represent sparse matrix using $l_p - norm$ $(0 < p < 1)$, defined as:

$$||a||_p = (\sum_{i=1}^{n} |a|^p)^{1/p} \tag{6}$$

F. Compressive Sensing (CS)

CS is a technique in the case of sampling and reconstruction. It reduces the sampling rate at complex reconstruction. CS can reconstruct the signal in less then traditional Nyquist sampling rate if the signal is sparse or compressible. Compressible indicates magnitude of signal's frequency decay which follow the power law. Signal can be derived sparse from DCT, DWT etc.

Let a signal $S \in R^{N \times 1}$ of length N can be represented in sparse domain as:

$$X = \phi\alpha \tag{7}$$

where $\phi \in R^{N \times K}$ is an orthogonal basis (DCT, DWT etc) or dictionary. $X \in R^{N \times K}$ is the sparse representation of signal S with sparsity L i.e. X has only L non-zero values. CS can acquire the signal in compressed form. Acquisition model of CS can be defined as:

$$Y = A\varphi = A\phi s = \theta s \tag{8}$$

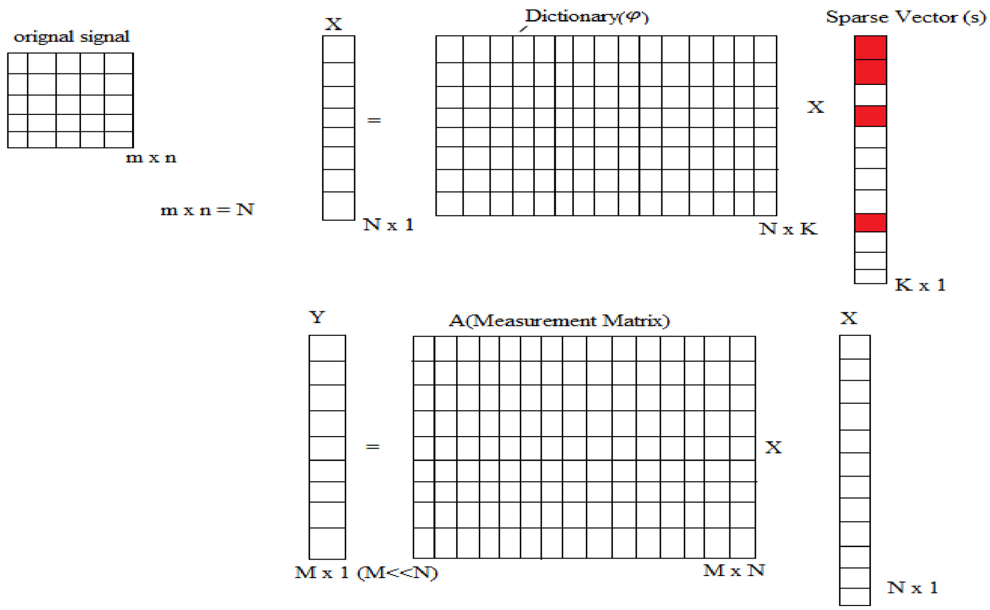

Fig. 3. Pictorial representation of Compressive Sensing

where $A \in R^{M \times N}$ is the measurement matrix of size $M \times N$. $Y \in R^{M \times 1}$ is the measurement data of length $M << N$. θ is the sensor matrix which is the product of A and ϕ. Pictorial representation of CS is shown in figure 3. The uneven size of measurement matrix results problem in the phase of reconstruction. It will give many solution. To overcome this problem, Restricted isometric property (RIP), a sufficient and necessary condition has been proposed which is defined as:

$$(1-\delta)||X||_2 \leq ||\psi X||_2 \leq (1+\delta)||X||_2 \tag{9}$$

where $X \in R^{N \times 1}$ is a sparse signal which has L non-zero values. RIP for a measurement matrix is an NP-hard problem and alternative solution of RIP is incoherence. Incoherence measure the dissimilarity of the signal. Measurement matrix and basis should be incoherent with each other. Incoherence should be minimum for better reconstruction. The coherence between two matrix can be defined as:

$$\mu(A, \varphi) = \sqrt{n} \max_{1 \leq i,j \leq n} |(A, \varphi)| \tag{10}$$

Coherence should lie between 1 and $\sqrt{(n)}$.

III. Preliminaries

In this section, some necessary preliminaries are introduced, including logistic map, arnold scrambling, zig-zag scrambling etc.

A. Chaotic map

Measurement matrix generally uses larger space for direct storage. So the measurement matrix is stored using initial state value and control parameters. Some chaotic maps are discussed below:

B. Logistic Map

Logistic map is 1D-chaotic map usually contain one variable and a few parameters. 1D- logistic map has simple structure. It is vulnerable to many cryptographic attacks. It is widely used in image encryption. It has a single control parameter μ

$$x_{n+1} = \mu x_n(1-x_n), x \in (0,1) \tag{11}$$

Logistic map gives good chaotic characters when $\mu \in$ (3.94,4).

C. Skew tent map

The skew-tent map can be defined as:

$$X_{i+1} = \begin{cases} X_i/p, & X_i \in [0,p] \\ (1 - X_i/(1-p)), & X_i \in [p,1] \end{cases}$$

where $X_i \in$ [0,1] and parameter p $\in$ (0,1). This equation involves in the chaotic state. The initial value of X_i and p can be used as a key.

D. Arnold Scrambling

Arnold Scrambling is used to scramble the pixel values of the signal. It shifts the pixel values using the relation given below:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod N$$

where N is the size of the matrix, x', y' is the position of pixel after scrambling and (x, y) is the position of pixel before scrambling. The strength of encryption is increased by repeating the above scrambling process. The number of iteration of scrambling can be used as a key.

E. Zig-Zag scrambling

Zig-zag scrambling is used to disturb the location of the entries in the matrix. It is performed by selecting the start pixel and then traverse the matrix from starting pixel. The matrix after zig-zag scrambling is totally different from the plain matrix. For example, a 4 $\times$ 4 matrix, if the starting position is (2,2) then the matrix is traversed from (2,2) is shown in the figure 4.

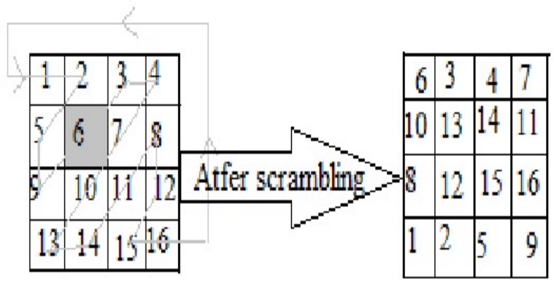

Fig. 4. Zig-Zag scrabling

IV. Literature Review

The fast transmission of image through public network can be obtained by compression, but for secure transmission of signal encryption is indeed required. CS can perform as a cryptosystem when measurement matrix is shared between sender and receiver as a key. A lot of work has been done by researchers in the field of encryption using CS. In the case of parallel image encryption Huang et al. (2014) has proposed an algorithm, in which, at first image is divided into blocks and each block shares the same size then each block is converted into vector. DCT is used as a basis for sparse representation of the signal. Gaussian measurement matrix is used as a measurement matrix. After that Lloyd quantization is applied to quantize the measurement matrix which is optimal quantizer in the sense of mean square error. The quantized data has reallocated and arnold scrambling is applied to permute the measurement values. S-box substitution is applied on scrambled data to provide confusion. Deepan et al. (2014) has proposed a multiple-image encryption algorithm using CS, in which multiple images are embedded in the host image. Space multiplexing is used to integrate multiple image. In the case of visually secured image Chai et al. (2017) has proposed an algorithm. In which DWT is used as basis for sparse representation of the signal then zig-zag scrambelling is applied to create confusion. At the phase of sampling chao-based measurement matrix is used and the resulted image is a cipher image. Zhang et al. (2013) has proposed an algorithm for color image encryption based on CS in which the image is decomposed into three components red(R), green(G), blue(B). Then all three components are measured by CS where measurement matrix of these components are utilized as a sub-key. After that these components are grouped in gray scale and Arnold transform is applied to obtain cipher image. Sl_0-algorithm is used at the reconstruction phase. Chaotic maps are used to encrypt the signal. George et al. (2014) has proposed an algorithm to encrypt the signal using chaotic map, in which cipher measurement matrix is generated using any two chaotic maps. And selected chaotic maps are X-ORed to generate measurement matrix. George et al. (2014) has proposed another algorithm in which a secured measurement matrix is generated using linear feedback shift register. In the case of parallel image compressive sensing Hu et al. (2017) has proposed an algorithm for image compression where CPA-resistance technique is used for sampling. After that double random phase encryption with gyrator transform is used to encrypt the signal. For secure multimedia transmission Li et al. (2016) has proposed an algorithm for image encryption in which logistic-controlled partial Hadamard is used to generate measurement matrix for sampling then scrambling is applied with the help of logistic-controlled index. After that quantization is applied with the help of sigmoid function. In the case of robust image encryption Luo et al. (2019) has proposed an algorithm in which DWT is applied to decompose the signal in approximate and detailed components. After that the approximation part is scattered by threshold processing of local binary pattern operator based chaotic sequence. It is generated with the combination of chua's circuit and logistic map. Chaos-combined asymptotic deterministic random measurement matrices (CADRMM) is used as a measurement matrix. Detailed part is mapped with the help of X-OR operation. At last the combination of approximation and detailed part is shuffled by the logistic map. Ma et al. (2018) has proposed an algorithm based on the combination of CS and computer generated holography (CGH), in which the image is first encrypted by CGH. After that when encrypted hologram is obtained it is compressed with the help of CS. The frequency spectrum of the hologram is obtained by Fourier transformation and an appropriate measurement matrix is used to obtain measurement of the signal. For optical image encryption Liu et al. (2014) has proposed an algorithm, in which the original signal is dimensionally reduced with the help of CS and chaotic based double random phase encoding is used to encrypt the signal in fractional fourier transform domain. Measurement matrix and random phase mask used to encrypt the signal is formed with the help of chaotic map. Another optical image encryption technique is proposed by Liu et al. (2013) in which CS is used for dimension reduction and random projection. Random measurement matrix is used to reduced the dimension of the signal. After that scrambling is applied on the measurement with the help of Arnold transformation. The encrypted image is re-encrypted with the help of double random phase encoding optical encryption technique. Sequence of irrational number is used to generate the two random phase mask. At the end, the encrypted signal is embedded in the host image. For the case of visual image encryption, Ponuma et al. (2019) has proposed an algorithm, in which, CS is used for dimension reduction and measurement matrix is controlled by chaos which is used to obtain measurement. DWT is utilized as a basis to represent the sparse signal. Scrambling is applied on the sparse signal. Measurement matrix is controlled by chaotic map. Then the encrypted data is quantize and embedded in the cover image. Another algorithm for image encryption is proposed by Ponuma et al. (2019) in which, DWT is used as a basis for sparse representation. Then scrambling is applied on the sparse data with the help of logistic map. After that CS is applied to obtain measurement. Measurement matrix is controlled by chaotic sequence. Ponuma et al. (2019) has proposed an algorithm for image encryption using sparse coding. Sparse coding is used for sparse representation of the signal from an over complete learned dictionary. K-SVD is used to obtain over complete learned dictionary. After that CS is used to obtain compressed samples. Gaussian measurement matrix is used to get the measurements. The cipher image is obtained by chaos based permutation and substitution operation. Zhang et al. (2016) has proposed an algorithm for bi-level protected CS to encrypt the signal, in which measurement matrix is obtained by product of key-dependent sensing matrix and key-dependent original basis. In the case of parallel CS, an image encryption algorithm has proposed by Wang et al. (2019) in which DWT is applied on the plain image to get the sparse representation of the signal. Scrambling is applied on the sparse signal. After that CS is applied to measure the compressed sample where measurement matrix is controlled by skew tent map. Then the secret image is embedded in the host image. For color image encryption using CS, Yao et al. (2019) has proposed an algorithm in which the color image is decomposed into three components RGB. DWT is applied on each component of the signal to obtain sparse representation. Different gaussian measurement matrix is used to obtain the measurement of each component. After that all the components are grouped and then encrypted by using multi-image cross pixel scrambling. Zhang et al. (2016) has proposed an algorithm using block CS, in which, the image is divided into significant and insignificant blocks. Significant block contain more useful information and insignificant block contain less useful information. Significant block is encrypted by chaos-based structurally random matrix and insignificant block is encrypted by chaos-based random convolution. After that both are grouped together and an encrypted image is obtained. An algorithm for two-level image authentication is proposed by Zhang et al. (2018) in which, DWT is applied on the signal to get sparse signal after that arnold scrambling is applied on the sparse signal to obtain the encrypted signal. After the detail discussion of related work, one of the works is discussed below:

Ponuma et al. (2019) has proposed an algorithm for image encryption using CS.

1)An grey level image I_n, where n defines the number of images that can be embedded, of size N $\times$ N. The tri-level DWT is applied on that image to obtain the coefficient matrix I_{1_n}.

2) Scrambling is applied on the coefficient matrix I_{1_n} with the starting position (x_0, y_0) to obtain matrix I_{2_n}.

3)The element of I_{2_n} are sparsified by using threshold (T). The element of I_{2_n} is changed into I_{3_n} with respect to threshold. I_{3_n} can be obtained as:

$$I_{3_n} = \begin{cases} 0, & |I_{2_n}(i,j)| < T \\ I_{2_n}(i,j), & elsewhere \end{cases}$$

4)Measurement matrix of size $M \times N$ is generated with the help of logistic map using μ_x and z_{0x}. CS is applied on I_{3_n} to obtain the compressed measurement I_{4_n}. The number of measurements is defined as:

$$M = round(sr \times N) \tag{12}$$

where sr is the sampling ratio.

5) Normalization is applied on element of I_{4_n} to obtain compressed cipher image I_{5_n}. Normalization can be done as:

$$I_{5_n} = \left\lfloor \frac{I_{4_n} - min_n}{max_n - min_n} \right\rfloor \tag{13}$$

where min_n and max_n is the minimum and maximum value of the I_{4_n}. And I_{5_n} is reshaped in $R_n \in R^{N/2 \times N/2}$ of size N/2 $\times$ N/2.

6) Tri-level DWT is applied on grey level cover image of size N/2 $\times$ N/2 to obtain its approximation (LL) and detailed part (LH, HL, HH). Minimum and maximum value of LL is min_c and max_c respectively. The interval [min_c, max_c] is divided into three equal intervals.

7) The matrix R_n is embedded in the remaining three bands LH, HL, HH as follows:

case(i): if LL(i,j) $\in$ lower interval, then

$$\begin{cases} LH(i,j) = R_1(i,j) & x = 1 \\ LH(i,j) = R_1(i,j), & \\ HL(i,j) = R_2(i,j) & x = 2 \\ LH(i,j) = R_1(i,j), & \\ HL(i,j) = R_2(i,j), & \\ HH(i,j) = R_3(i,j) & x = 3 \end{cases}$$

case(ii) : if LL(i,j) $\in$ middle interval, then

$$\begin{cases} HL(i,j) = R_1(i,j) & x = 1 \\ HL(i,j) = R_1(i,j), & \\ LH(i,j) = R_2(i,j) & x = 2 \\ LH(i,j) = R_1(i,j), & \\ HL(i,j) = R_2(i,j), & \\ HH(i,j) = R_3(i,j) & x = 3 \end{cases}$$

case(iii): if LL(i,j) $\in$ upper interval, then

$$\begin{cases} HH(i,j) = R_1(i,j) & x = 1 \\ LH(i,j) = R_1(i,j), & \\ HH(i,j) = R_2(i,j) & x = 2 \\ LH(i,j) = R_1(i,j), & \\ HL(i,j) = R_2(i,j), & \\ HH(i,j) = R_3(i,j) & x = 3 \end{cases}$$

8) Visually secure cipher image is obtained to combine the modified LL, LH, HL, HH band of cover image with tri-level inverse DWT.

9) Decryption scheme is just inverse of the encryption scheme.

V. Conclusion

This paper delivers a brief knowledge of CS with application image encryption. CS can sample the signal in compressed form which helps in compression. CS works as a cryptosystem when measurement matrix is shared between the sender and receiver. CS can reconstruct the signal along with encryption with the help of measurement matrix. A detailed study on image encryption using CS has been discussed. The mathematical view of CS for naive researchers has also been considered with detail discussion of some methods which can boost this research area.

References

Chai, X., Gan, Z., Chen, Y., & Zhang, Y. (2017). A visually secure image encryption scheme based on compressive sensing. Signal Processing, 134, 35-51.

D. L. Donoho, (2006) Compressed sensing. In: IEEE Transactions on Information Theory, 52(4), 1289-1306.

Deepan, B., Quan, C., Wang, Y., & Tay, C. J. (2014). Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. Applied optics, 53(20), 4539-4547.

E. J. Cand‘es and M. B. Wakin (2008) An introduction to compressive sampling. In: IEEE Signal Processing Magazine, 25(2), 21-30.

Foucart, S., Rauhut, H. (2017) A mathematical introduction to compressive sensing. In: Bull. Am. Math, 54, 151–165.

George, S. N., & Pattathil, D. P. (2014). A novel approach for secure compressive sensing of images using multiple chaotic maps. Journal of Optics, 43(1), 1-17.

George, S. N., & Pattathil, D. P. (2014). A secure LFSR based random measurement matrix for compressive sensing. Sensing and Imaging, 15(1), 85.

Huang, R., Rhee, K. H., & Uchida, S. (2014). A parallel image encryption method based on compressive sensing. Multimedia tools and applications, 72(1), 71-93.

Hu, G., Xiao, D., Wang, Y., Xiang, T., & Zhou, Q. (2017). Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes. Optics and Lasers in Engineering, 98, 123-133.

Li, Y., Song, B., Cao, R., Zhang, Y., & Qin, H. (2016). Image encryption based on compressive sensing and scrambled index for secure multimedia transmission. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 12(4s), 1-22.

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.

Liu, X., Mei, W., & Du, H. (2014). Optical image encryption based on compressive sensing and chaos in the fractional Fourier domain. Journal of Modern Optics, 61(19), 1570-1577.

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.

Ma, L., & Jin, W. (2018). Symmetric and asymmetric hybrid cryptosystem based on compressive sensing and computer generated holography. Optics Communications, 407, 51-56.

Ponuma, R., Amutha, R., Aparna, S., & Gopal, G. (2019). Visually meaningful image encryption using data hiding and chaotic compressive sensing. Multimedia Tools and Applications, 78(18), 25707-25729.

Ponuma, R., & Amutha, R. (2019). Encryption of image data using compressive sensing and chaotic system. Multimedia Tools and Applications, 78(9), 11857-11881.

Ponuma, R., & Amutha, R. (2019). Image encryption using sparse coding and compressive sensing. Multidimensional Systems and Signal Processing, 30(4), 1895-1909.

Wang, H., Xiao, D., Li, M., Xiang, Y., & Li, X. (2019). A visually secure image encryption scheme based on parallel compressive sensing. Signal Processing, 155, 218-232.

Yao, S., Chen, L., & Zhong, Y. (2019). An encryption system for color image based on compressive sensing. Optics & Laser Technology, 120, 105703.

Zhang, A., Zhou, N., & Gong, L. (2013). Color Image Encryption Algorithm Combining Compressive Sensing with Arnold Transform. JCP, 8(11), 2857-2863.

Zhang, L. Y., Wong, K. W., Zhang, Y., & Zhou, J. (2016). Bi-level protected compressive sampling. IEEE Transactions on Multimedia, 18(9), 1720-1732.

Zhang, Y., Zhou, J., Chen, F., Zhang, L. Y., Xiao, D., Chen, B., & Liao, X. (2016). A block compressive sensing based scalable encryption framework for protecting significant image regions. International Journal of Bifurcation and Chaos, 26(11), 1650191.

Zhang, X., Meng, X., Yin, Y., Yang, X., Wang, Y., Li, X., ... & Chen, H. (2018). Two-level image authentication by two-step phase-shifting interferometry and compressive sensing. Optics and Lasers in Engineering, 100, 118-123.

***