VOL. 13, NO. 4, FEBRUARY 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

COMPRESSIVE SENSING BASED IMAGE ENCRYPTION SCHEME

K. Saravanan[1], T. Purusothaman[2] and KVN. Kavitha[1]
[1]School of Electronics Engineering, Vellore Institute of Technology, Vellore, India
[2]Department of Information Technology, Government College of Technology, Coimbatore, India
E-Mail: kasisaravanan@vit.ac.in

ABSTRACT

On the basis of a compressive sensing technique, an encryption scheme is proposed in order to improve security for the image. In the proposed algorithm, Discrete Wavelet Transform is applied to the plain image in order to transform it into many wavelet coefficients and then those coefficients are in turn confused using zigzag confusion. Finally they are converted into a cipher image by applying the proposed compressive sensing technique. Randomly generated 256 bit key is used to calculate the skew tent map, which further forms the basis for creating the measurement matrix used in compressive sensing. Simulation results show good performance for the proposed algorithm over the existing algorithms.

Keywords: compressive sensing, cryptography, steganography.

1. INTRODUCTION

Nowadays we are living in digital world and with the arrival of internet, various technologies and various equipment like electronic gadgets; digitally images are being generated immensely. These images are being stored in various storage platforms such as cloud servers, laptops, hard drive, etc. They are also being transmitted across various platforms such as social networking sites like Facebook, WhatsApp and Emails from one person to another. A large amount of information is present in digital data. For example, from a military base image we can estimate the size of base and various weapons present. So protecting images has many uses in various fields like medical images, military images, and personal information. Security of information is one of the most important factors of Information technology and communications. So in order to protect these images encryption of images [1], [2] comes into play.

2. REVIEW OF RELATED WORK:

A large number of image encryption algorithms have been proposed and are in existence [3], [4], [5]. Of all these algorithms the common feature is that in the process of encryption, the final result is a noisy cipher image. With the help of a secret key an image is encrypted. The generated cipher image [7] is communicated to the receiver and no middle person can decrypt the original image from the cipher image. With the help of decryption key only, anyone can extract the information from cipher image.

Some image compression and encryption algorithms based on Compressive sensing (CS) have already been proposed [6], [7], [8], [9]. CS compresses and samples at the same time. In a communication system the transmitted signal can be exactly reconstructed at the receiver if the transmitted signal is sampled at a particular rate which can be either equal to or greater than that of the Nyquist rate. For some cases of sampling rate which are below Nyquist rate, the CS recovers them completely. A sparse signal is allowed to be recovered by the CS, so DWT to sparsify the image is used. Applying DWT decomposition gives floating values coefficient matrix. The SHA (Secure hash algorithm) is one of the commonly used cryptographic hash function. The hash functions in cryptography act like an authorization (i.e. signature) for a data or text file. SHA-256 algorithm [3] generates a 32-byte (256-bit) hash which is of a fixed size and it is also unique. The Hash function can't be decrypted at all, as it is a one way function. This property of hash functions makes them possible to be used in digital world applications like digital signatures, password validation, anti-tamper and various other authentication schemes.

Many signal samples used in real-world applications are encoded as integers, for example the signal amplitudes encoded by analog-to-digital (A/D) converters and colour intensity value of pixels encoded in digital images [1], [2]. For these integer-encoded signals, a discrete wavelet transform (DWT) can be particularly efficient.

This remaining paper is organized as given below. In section 3 and section 4, the proposed algorithm and its performance analysis are described in detail respectively.

3. PROPOSED WORK

In this proposed algorithm a plain image is taken which has to be transmitted and the coefficient matrix of that image is created using the Discrete Wavelet Transform. This coefficient matrix is in turn confused using zigzag confusion which decreases the correlation among pixel values to increase the image security. A randomly generated key is used to calculate the one-dimensional skew tent map's parameters which in turn are used in generating the measurement matrix. And also the same key is used to generate parameters which are used in zigzag confusion. The matrix of coefficients of image after zigzag is compressed and encrypted into cipher image with the help of measurement matrix and sensing matrix. This entire process is called Encryption and its block diagram is shown in Figure-1. Each block in Figure-1 is explained below. The decryption process is the exact reverse process of encryption process and it is shown in Figure-2.

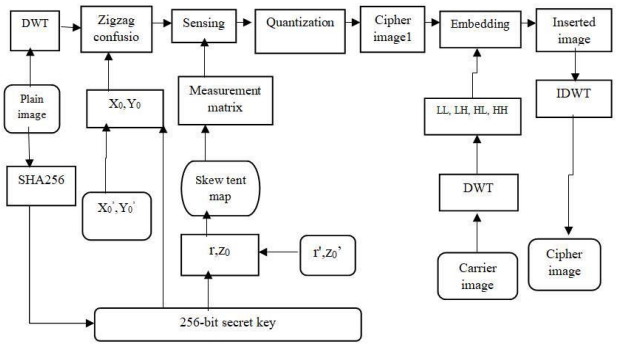

Figure-1. Flowchart of proposed encryption algorithm.

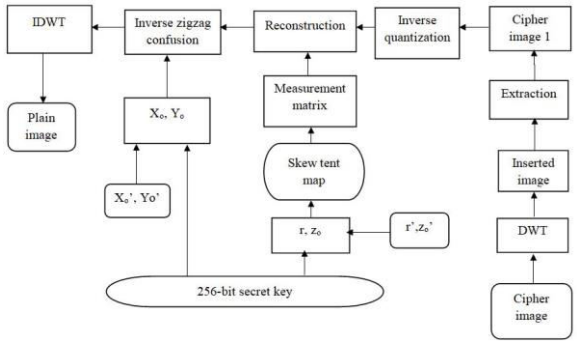

Figure-2. Flowchart of proposed decryption algorithm.

3.1 Parameters generation

Initially, one need to generate a 256 bit random key and then the random key is divided into 32 different blocks with each block of 8 bit length, thus the key can be expressed as follows:

$$P = p_1, p_{2,\ldots}p_{32} \text{ where } p_i = \{ p_{i,0}, p_{i,1}, \ldots\ldots, p_{i,7} \} \quad (1)$$

In $p_{i,j,}$ i and j represents the character and bit number of p_i respectively ;

Next, the four intermediate parameters qi are computed by,

$$q_i=[S_i +((p_{4i-2} +(4i-2)/(p_{3i} +3i)) + (p_{5i-3} +(5i-3)/(p_{4i} +4i)))$$

$$*\sum_{j=1}^{32} pj * 2\text{^}8 * (j-1)/2^{256}] \text{ i=1, 2, 3, 4} \quad (2)$$

Here, $S_i(i$ =1 to 4) are the parameters given and they individually represent parameters such as x_0', y_0', r', z_0', q_3 and q_4 individually denote the parameters r, z_0 and the values of x_0,y_0 are calculated using these key

3.2 The encryption algorithm

In this section, the proposed image encryption algorithm on the basis of compressive sensing is explained in detail. The plain image is modified by using zigzag confusion and it is then compressed and encrypted using Compressive sensing.

Step-1: Generate a 256 bits key randomly. Then the parameters x_0, y_0 are calculated with the help of given parameters x_0', y_0', r', z_0' as mentioned in Section 2.1.

Step-2: Let us assume the plain image be A and its size be m×n, and then apply Discrete Wavelet Transform for the image in order to obtain coefficient matrix A1. The obtained coefficient matrix is of the same size as the image. After applying Discrete Wavelet Transform image is sparsified as shown in Figure-3.

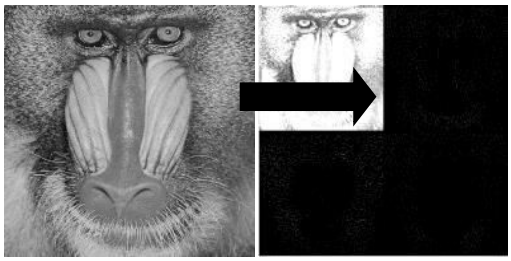

Figure-3. Decomposition of image after applying wavelet transforms.

Step-3: Now apply zigzag confusion on A1 as described below to obtain the confused matrix A2. The zigzag path shown in below Figure-4 alters the position of sparsified coefficients in A1. The correlations among the pixels in the image are reduced by zigzag confusion and thus the security level of the proposed encryption algorithm is increased.

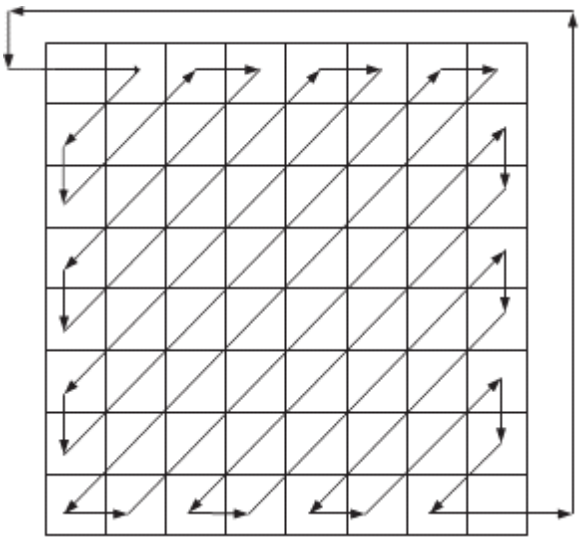

Figure-4. Zigzag confusion process.

Step-4: Now set a threshold limit TS, and make the coefficients of the matrix A2 below the given threshold to zero and the matrix obtained is named as A3.

Step-5: In this step one has to generate the measurement matrix Φ using r, z_0 and then the compressive sensing technique is applied to matrix *A3* which results in the measurement matrix *A*4 i.e. A4 = Φ * A3.

Let the plain image's compression ratio be *CR*, then the Φ's size is *M*N*, where *M=CR*m*, *N=n*. This gives the size of *P*4 as *M*n.*

Measurement matrix:

The measurement matrix acts as an encryption key in this encryption process. The chaotic sequence [7] which is obtained from the logistic map is used to create the measurement matrix. Thus it is proved that its Restricted Isometric Property has a high probability of being guaranteed. In this approach, the 1-Dimensional skew tent map forms the basis in generating the measurement matrix. The probability density function can be represented as given below:

$$g(k+1) = T[g(k);r] = \begin{cases} g(k)/r, & 0 < g(k) < r \\ [1-g(k)]/(1-r), & r \le g(k) \le 1 \end{cases} \quad (3)$$

Here the system parameter r (0, 1) and initial value g_0 (0, 1)

Let $g(d,l,r,g_0)=(g(n+i\times d))_{i=0}^{l} = (g_n , g_{n+d} , g_{n+2d} , \ldots\ldots g_{n+ld})$ be the generated chaotic sequence obtained by sampling the output sequence which is produced by equation (3), where d and g_0 is the sampling distance and skew tent map's initial value respectively.

On applying transformation to chaotic sequence:

$$\emptyset\ (l)\ |^{MN-1}_{l=0} = (1-2g_{n+ld})\ |^{MN-1}_{l=0} \quad (4)$$

Now creating measurement matrix ∅ as:

$$\emptyset=\sqrt{(2/M)}\begin{bmatrix} \emptyset(0) & .. & .. & \emptyset(M(N-1)) \\ \emptyset(1) & .. & .. & \emptyset(M(N-1)+1) \\ .. & .. & .. & .. \\ \emptyset(M-1) & .. & .. & \emptyset(MN-1) \end{bmatrix} \quad (5)$$

Step-6: Now to quantify the elements of matrix A4, and convert the values of elements such that they are in between 0 and 255 as per the given equation (6) given below, and the matrix *A*5 is generated, and it is the A's cipher image in compressed form.

$$a_{5i} = floor\ (255 \times (a4i - \text{Min}) \div (\text{Max} - \text{Min})) \quad (6)$$

where, Min and Max denotes the minimum and maximum value of matrix *A*4 respectively, fl*oor*(*x*) calculates a largest integer which is not more than *x*, *a*4i and *a*5i are the *i*th elements of *A*4 and *A*5 ($1 \le i \le Mn$), respectively.

Step-7: The carrier image which is taken as input undergoes DWT and then, the cipher image is embedded inside it and finally the embedded carrier image is generated which is sure for transmission.

Step-8: 10 different channels with different SNR values varying from 1dB to 10 dB are introduced at this step to check the efficiency of the algorithm at the receiver end.

3.3 The decryption algorithm

The process of decryption is a reverse to that of the encryption process. The flow chart representation of the decryption process is depicted in Figure-2. In this the plain image has to be constructed from the cipher image A5. Before the start of decryption randomly generated 256 bit key, x_0', y_0', r', z_0' and the parameters Min, Max should be transmitted to the receiver. The parameters r, g_0 can be calculated as mentioned in section 2.1

Step-1: The inverse quantification process has to be applied on A5 according to the equation (7) given below. After this operation is performed obtained A4 matrix and it is measurement value matrix.

$$a4i = (a5i * (\text{Max} - \text{Min}))/255 + \text{Min}. \quad (7)$$

Where, a4i and a5i are i th element of A4 and A5 respectively. The values Max and Min are received secretly from the sender.

Step-2: Generate the measurement matrix Φ using the parameters received by the receiver according to equation in section 2.1 Now obtain the matrix A3 from A4 using a suitable reconstruction algorithm.

Step-3: In this step perform the inverse zigzag confusion on matrix A3 to obtain the matrix A1. To obtain the plain image from A1, perform the Inverse Discrete Wavelet Transform (IDWT) on A1 you will get the plain image. Thus the decryption process is completed.

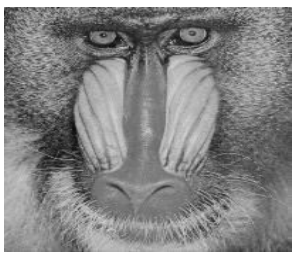

Figure-5. Baboon image.

Figure-6. Cipher image1.

Figure-7. Carrier cipher image.

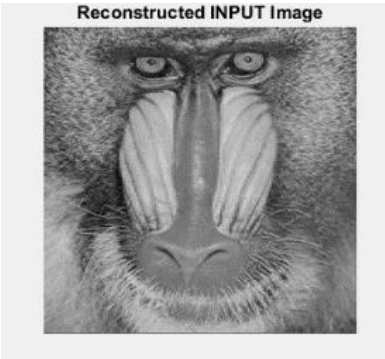

Figure-8. Reconstructed plain input image.

4. RESULTS ANDDISCUSSIONS

The performance of the proposed algorithm is verified and analyzed using Matlab simulation. The parameters we have used in Section 3.1 are $x_0' = 0.2796$, $y_0' = 0.7531$, $r_0' = 0.5678$, $z_0' = 0.8652$ and the sampling distance d = 20. The value used as threshold limit used in step 4 of Section 3.2 is 50. The Compression ratio (CR) determines to what size the plain image has to be compressed. In this simulation we have used CR = 0.25. In mathematical terms we have calculated the Bit Error Rate (BER), peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) for various SNR values of channels to check encryption and decryption processes. Thus the calculated values were plotted. The MSE is calculated by comparing the original image with decrypted image. The values we have obtained are considered for plotting the graphs as given below. We have obtained highest PSNR value 34.8838 in our simulation results for the image plane. tiff (256x256) which shows good simulation results. The values obtained shows we have obtained good PSNR values, thus the proposed algorithm gave good results and it can be used for secured data transmission with less compression loss. In this algorithm the compressed cipher image size is lesser than plain image and it depends on CR. So, there is actually less transmission bandwidth, memory and time required than to transmit the plain image.

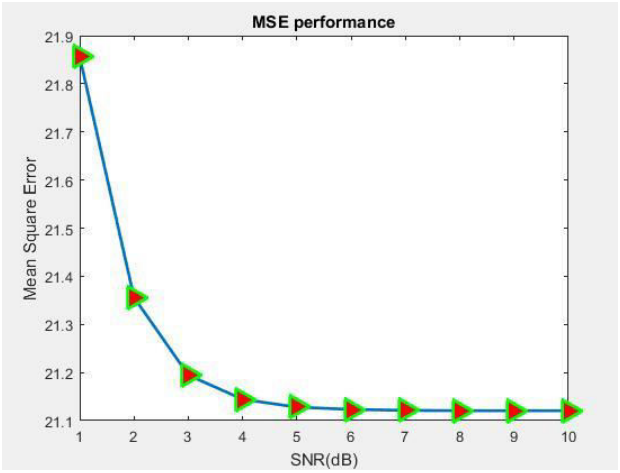

Figure-9. Mean squared error.

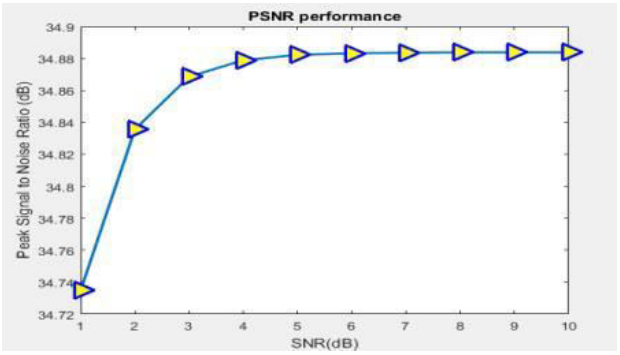

Figure-10. Peak signal to noise ratio.

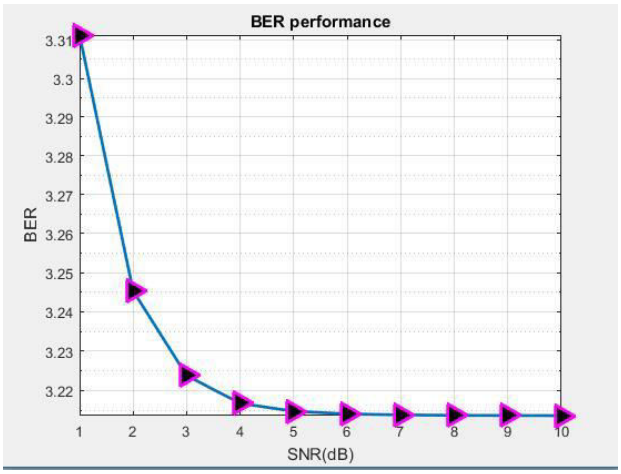

Figure-11. Bit error rate.

5. CONCLUSIONS

The proposed algorithm is an image encryption scheme which is primarily based on compressive sensing technique and it was verified by simulation. The algorithm uses a larger key space which is more immune to brute force attack and also it has high sensitivity to plain images. Thus it can prevent attacks like chosen-plaintext and known-plaintext.

The PSNR analysis was done using the CS approach in order to minimize the data required for extracting reasonable amount of information. It was observed that 20% of the information conveyed by the data is necessary for extracting a PSNR value equal to 25.104 dB. The redundant pixels in the complex encrypted image were discarded and at the same time about 20 % of sporadic encrypted samples were retained. This significantly compressed the encrypted image. The process of decryption is benefited by reconstructing the original image from the encrypted image**.** With obtaining a more correct measurement matrix, more robustness can be achieved. Also this encryption process can be extended by data hiding process in which this cipher image is hidden in other data to obtain visually secure image.

ACKNOWLEDGEMENTS

The authors sincerely acknowledge the efforts of the authorities of VIT University for their constant support

by providing resources which made this research work to be successful.

REFERENCES

[1] Y.C. Zhou, L. Bao, C.L. Philip Chen. 2014. A new 1D chaotic system for image encryption. Signal Processing-Science direct 00: 1-21.

[2] Manish Kumar, Akhlad Iqbal, Pranjal Kumar. 2016. A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography, Signal Processing. 125(C): 187-202.

[3] R. Guesmi, M.A.B. Farah, A. Kachouri, M. Samet. 2016. A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2. Journal. Nonlinear Dynamics. 83(3): 1123-1136.

[4] W. Chen. 2016. Single-shot imaging without reference wave using binary intensity pattern for optically-secured-based correlation. IEEE Photonics J. 8(1): 6900209.

[5] X.Y. Wang, D.H. Xu. A novel image encryption scheme based on Brownian motion and PWLCM chaotic system. Nonlinear Dyn. 75(1-2): 345-353.

[6] Y.S. Zhang, Leo Y. Zhang, J.T. Zhou, L.C. Liu, F. Chen, X. He. 2016. A review of compressive sensing in information security field. IEEE Access. 5: 2507-2519.

[7] Xiuli Chai, Zhihua Gan, Yiran Chen, Yushu Zhang. 2017. A visually secure image encryption scheme based on compressive sensing. ACM Signal Processing. 134 (C): 35-51.

[8] N.R. Zhou, H.L. Li, D. Wang, S.M. Pan, Z.H. Zhou 2015. Image compression and encryption scheme based on 2D compressive sensing and fractional mellin Transform. Journal. Optical Communication. 343: 10-21.

[9] H. Liu, D. Xiao, R. Zhang, Y.S. Zhang, S. Bai. 2016. Robust and hierarchical watermarking of encrypted images based on compressive sensing. Journal. Signal Processing. Image Communication. 45: 41-51.

[10] Narendra K. Pareek, Vinod Patidar, Krishan K. Sud. 2013. Diffusion-substitution based gray image encryption scheme. Digital Signal Processing. 23(3): 894-901.