 doi:10.20944/preprints201807.0258.v1

HYBRID OPTICAL CRYPTOGRAPHY AND COMPRESSIVE SENSING BASED ON ORTHOGONAL MATCHING PURSUIT

Ertan ATAR[*], *Okan ERSOY*[**]

[*]*Türk Telekom, İstanbul, Turkey, ertan.atar@turktelekom.com.tr*

[**]*School of ECE., Purdue University, Indiana, USA, ersoy@purdue.edu*

ABSTRACT

Compressive sensing (CS) is a technique that allows a signal vector to be reconstructed with a number of linear measurements far fewer than its size. In this study, optical hybrid cryptography with simultaneous compressive sensing based on orthogonal matching pursuit (OMP) is proposed as an alternative solution to the two important problems in communications, namely, effective / efficient / signal processing and secure encryption/decrypton. The whole system is able to both compress and encrypt data with attack immunity.

Keywords — Compressive sensing, orthogonal matching pursuit, hybrid optical cryptography, symmetric cryptography, asymmetric cryptography, Fourier related transforms, double random phase/amplitude optical key encryption, data compression, sensor reduction.

1. INTRODUCTION

Many signals used in practise such as audio, image, radar, and video signals are highly correlated and can be represented as sparse signals [1]. Compressive sensing theory shows how to restore the original signal from the compressed signal [2], [3].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0258.v1

The number of measurements (M) required for signal recovery depends on the signal length (N), and the number of nonzero sparse signal elements (K). The most commonly used relation is given by [4-6]

$$M \geq (K \times log\ (N)) \quad (1)$$

Cryptography involves methods used to encrypt and decrypt information. Studies on mathematical methods dealing with information security such as reliability, data integrity, and authentication are important topics of cryptography [7-8]. Cryptoanalysis involves methods to investigate the strengths and weaknesses of cryptographic systems.

Symmetric encryption algorithms use the same key for encryption and decryption operations. Symmetric encryption is very fast and easy to implement in electronic devices. In asymmetric encryption, one general key is used for encryption, and another special key is used for decryption. Asymmetric encryption algorithms are usually developed with very large prime numbers.

2. LITERATURE SUMMARY

Amir and Ester proposed that EEG signals can be encrypted by using the measurement vector of the EEG signal [9]. Minal and Rajankar proposed to change the rows and columns of the detection matrix for encryption [10]. Rachlin et al. and Dwork et al. proposed using CS for data security and encryption [11], [12]. Özdemir et al. proposed using a random detection matrix as an encryption key [13]. Ramezani et al. also proposed using a detection matrix for encryption and decryption [14]. Zhang et al. proposed an encryption and decryption method by using two different detection matrices [15]. Moreover, Zhang et al. used two different transform methods to generate a detection

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0258.v1

matrix for encryption and decryption [16]. Mo et al. proposed to use the Hadamard matrix as detection matrix for encryption and decryption [17].

3. HYBRID OPTICAL CRYPTOGRAPHY WITH COMPRESSIVE SENSING BASED ON ORTHOGONAL MATCHING PURSUIT

Orthogonal Matching Pursuit (OMP) is an iterative method to recover the non-zero elements of a sparse signal from the measured signal. If the length m of the measurement vector is larger than k, the number of nonzero elements of the sparse signal, the sparse signal can be recovered by OMP with a very large probability [18,19].

In the proposed work, the detection matrix was generated by using a fast transform such as discrete Fourier transform (DFT), discrete cosine transform (DCT), real sinusoidal transform (RST), Haar wavelet transform, Hadamard transform, discrete sine transform (DST) and discrete cosine-III transform (DC3T) [21]. In the experiments discussed in Section 6, the ranking of transforms in terms of accuracy of results were DC3T, DCT, DFT, RST, DST, Hadamard and Haar. In addition, DC3T has fewer number of multiplications than DCT.

The procedure for the OMP is as follows:

Given:

A = measurement matrix, y = measurement vector

Define:

Λ_l =index set at the *lth* iteration

x_l = sparse signal vector estimate at the *lth* iteration

r_l = residual signal vector at the *lth* iteration

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0258.v1

$|\bullet|_2$ = Euclidian norm

$A\left[\Lambda_{l+1}\right]$ = matrix consisting of columns of A from the set Λ_{l+1}

Initialization:

$\Lambda_0 = \phi, r_0 = y, l = 0$

while not converged, do

$h_l = A^t r_l$

$\Lambda_{l+1} = \Lambda_l \cup \arg\max\left(h_l\right)$

$A'_{l+1} = A\left[\Lambda_{l+1}\right]$

$x_{l+1} = \arg\min_z \left|y - A'_{l+1} z\right|_2$

$l = l + 1$

end while

Output:

$\hat{x} = x_l$

In the proposed method, the RSA algorithm was used for asymmetric encryption of the keys [7,8,20,21]. In this method, two very large prime numbers p and *q* with *N=pq* as well as bit length *n* are selected. *N* does not exceed *n* bits in length. The algorithm generates two keys e, the public key, and d, the private key. *e* being an integer less than and coprime to *Q=(p-1)(q-1)*. d is found by

$$d = e^{-1} \bmod Q \qquad (2)$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0258.v1

where d^{-1} is the multiplicative inverse of $d \ mod \ Q$.

A message M is coded as an integer such that $0 \le M \le N$, and M is prime to N. The message is encrypted as a ciphertext C by

$$C = M^e \bmod N \tag{3}$$

Decryption is achieved by recovering M from C by using

$$C^d = M \bmod N \tag{4}$$

Using asymmetric and symmetric encryptions together is named hybrid cryptography. It increases the advantages and decreases the disadvantages of the asymmetric and symmetric encryptions [7,8,20,21].

The fllow diagram for simultaneous compressive sensing and optical encryption is shown in Figure 1. In the figure, it is assumed that DFT is used for CS OMP compression with its associated fast algorithm FFT. In the actual implementation, the CS measurement matrix generated by multiplying a fast transform matrix with pre and post random permutation matrices is obtained independently of the input signal.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0258.v1

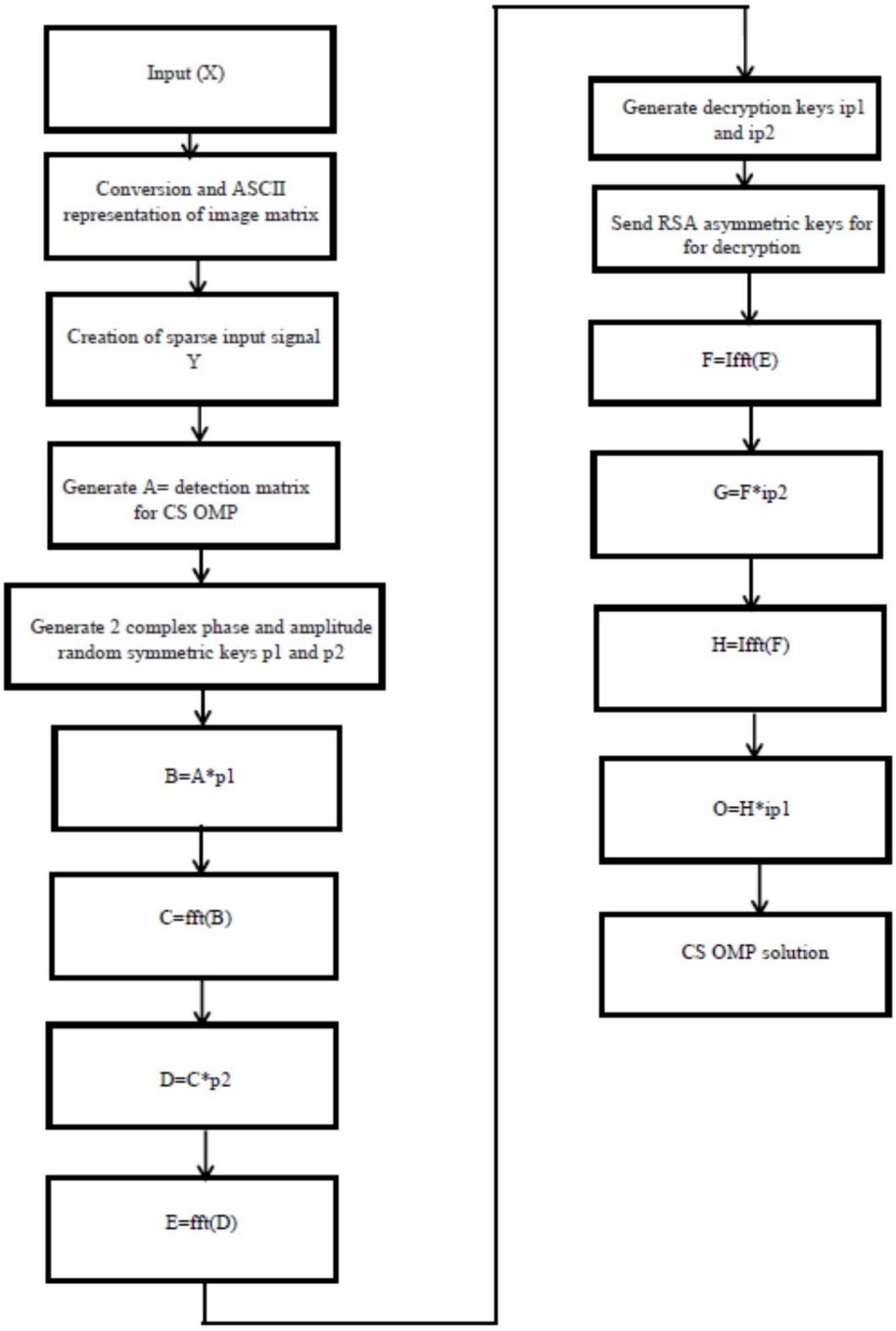

Figure 1. Flow diagram of the proposed method.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0258.v1

In the case of 1-D signals, the signal is processed in small vectors. In the case of images, an image of size *I*I* is first divided in to blocks of size *J*J*. For example, *I*=256, and *J*=16. The elements of each block are ordered lexicographically to generate a 1-D signal of length J^2. In this way, 2-D images are converted to 1-D signals. Sparse signals can be created in practice by using, for example, the DCT as commonly done in JPEG image and audio signal compression. Next the sparse signal per block is generated with length *M* satisfying $M \geq K * log(N)$ by keeping *M* largest elements in magnitude and zeroing the others.

The proposed method is applied per block (vector) as shown in Figure 2. The optical phase/amplitude keys p1 and p2 are generated with random complex numbers. The phase covers 360 degrees. The corresponding 2-f optical encryption system using the Fourier transform is shown in Figure 2 as an optical system. The lens represents the Fourier transformation. This is repeated once more for a 4-f optical encryption system for additional security. The resulting encrypted signal is of smaller size than the original signal.

In order to increase cryptographic security, the optical p1 and p2 phase + amplitude keys are composed of complex random numbers. The use of complex numbers with double random optical phase + amplitude keys and transform processing provides good scattering. In order to apply asymmetric cryptography in our proposed algorithm, the symmetric keys are sent asymmetrically to the receiver by separating the real and imaginary parts of the two optical random phase + amplitude complex keys and the keys are received symmetrically with the RSA. At the receiver, the CS OMP algorithm is used to recover the original signal. We claim that $(A * (e^{j\theta}))$ keys and encryption algorithms including CS OMP makes phase and amplitude recovery virtually impossible.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0258.v1

4. RESULTS

Examples of encryption with 1-D signals are shown in figures 3 and 4. Figure 3 shows the audio (1-D) inputs, outputs and encrypted signals. In Figure 4, p1 and p2 phase and amplitude keys are visualized.

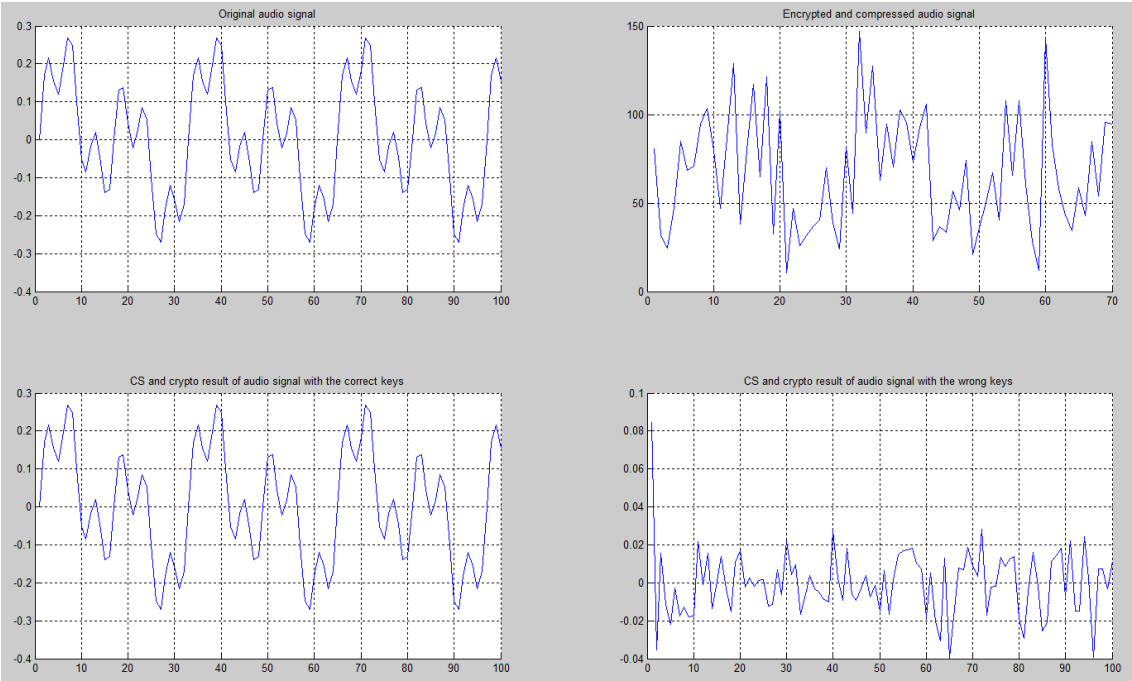

Figure 3. 1-D experiment: audio signal (top left), encrypted signal (top right), correctly decrypted signal with correct keys (bottom left), wrongly decrypted signal with wrong keys (bottom right).

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0258.v1

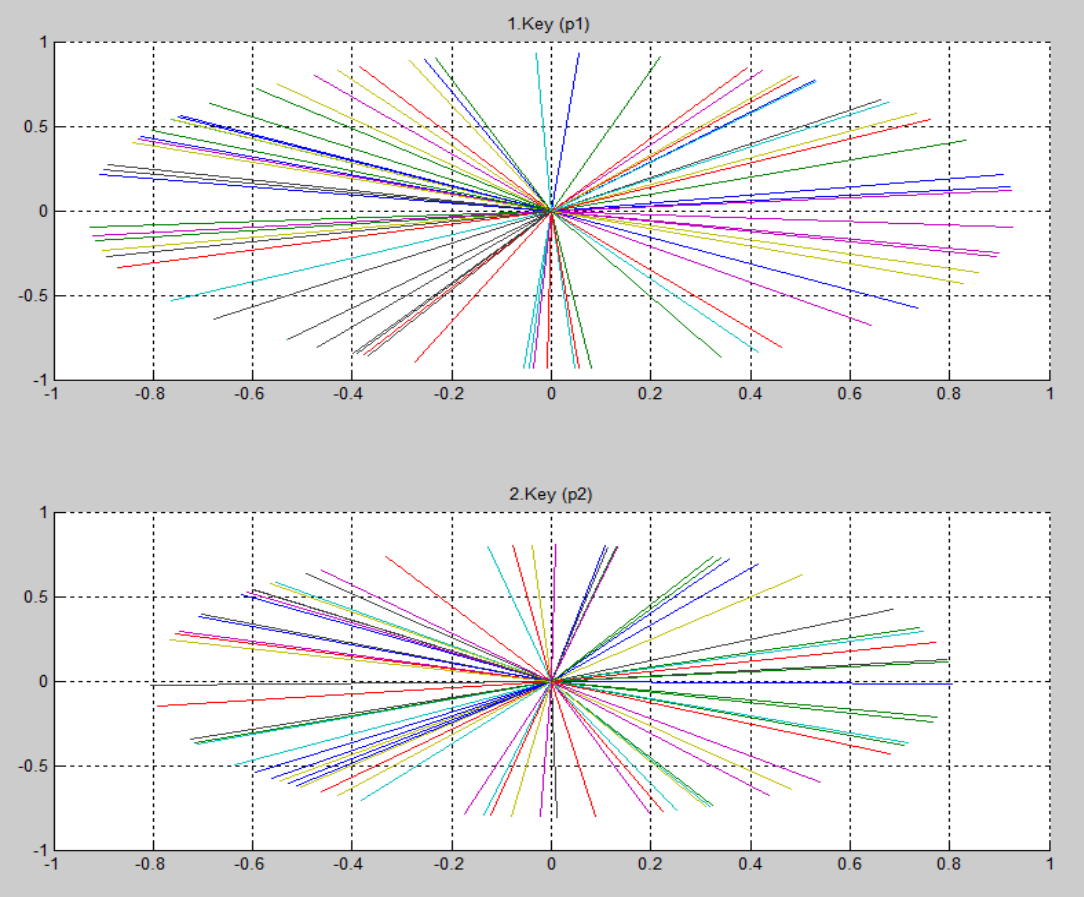

Figure 4. Complex, randomly distributed phase and amplitude keys.

The experimental results in 2-D are shown in Figures 5, 6, 7 and 8. Figure 5 shows the original BABOON image. Figure 6 shows the encrypted image obtained with the SCOSC method and blockwise processing. Figure 7 shows the result obtained after decryption when the correct key was used. The image is essentially the same as the original image. Figure 8 shows the result obtained after decryption when the wrong key was used. The image is totally unrecognizable.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2018 doi:10.20944/preprints201807.0258.v1

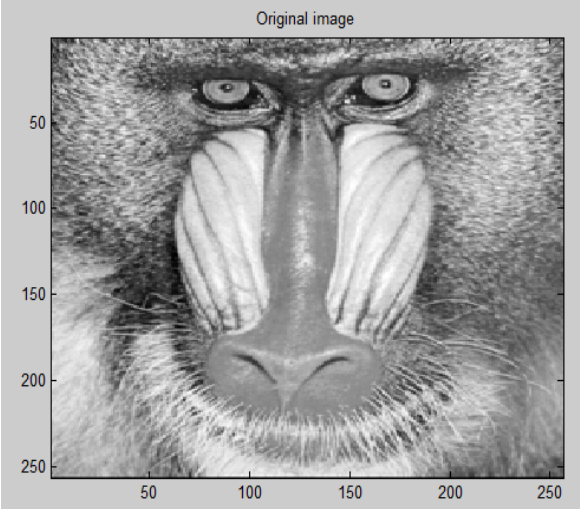

Figure 5. Original BABOON image.

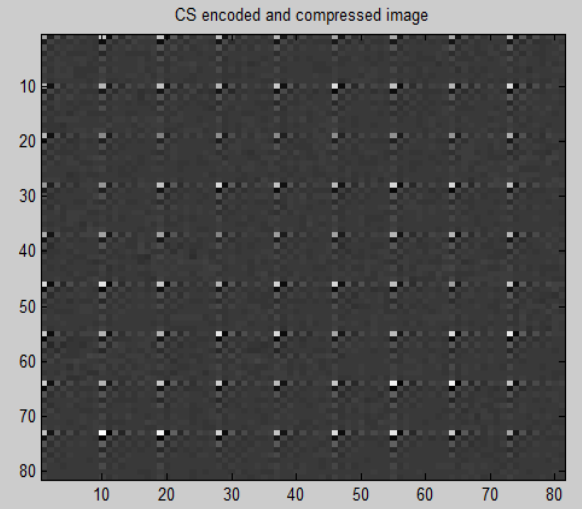

Figure 6. Encrypted image by CSOCS method and blockwise processing.

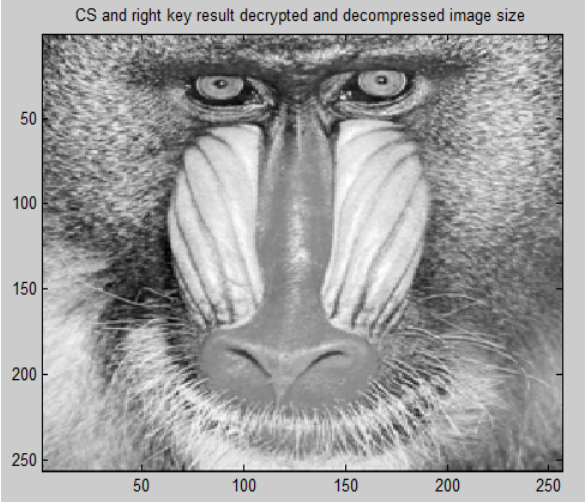

Figure 7. Decrypted image when the correct key was used.

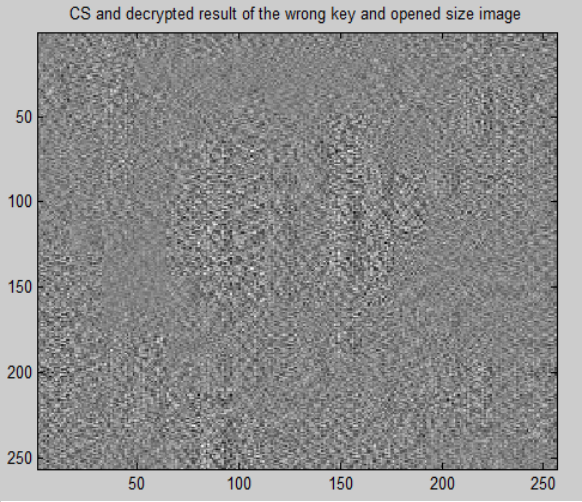

Figure 8. Decrypted image when the wrong key was used.

5. CONCLUSIONS

In this study, a method for simultaneous compressive sensing using OMP and optical cryptography using double random phase/amplitude keys was proposed. The RSA algorithm involving asymmetric cryptography was used to encrypt/decrypt the optical keys.

 doi:10.20944/preprints201807.0258.v1

The phase/amplitude keys were used as in a 4f optical cryptography system. The measurement matrix for the OMP algorithm was constructed using Fourier-related fast transforms such as discrete Fourier transform (DFT), discrete cosine transform (DCT), real sinusoidal Transform (RST), Haar wavelet transform, Hadamard transform, discrete sine transform (DST) and discrete cosine-III transform (DC3T) [22] together with random permutation matrices.

The experimental results with encryption/decryption of 1-D audio signals and 2-D images showed that the method is capable of very safe encryption and decryption with correct keys. It was not possible to achieve correct decryption with 1-D and 2-D input signals when the keys were wrong.

 doi:10.20944/preprints201807.0258.v1

REFERENCES

1. Candès E., Romberg J., Tao T., ‘‘Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information’’, IEEE Trans. On Information Theory, 52 (2), 489-509, 2006.

2. Donoho D., ‘‘Compressed sensing’’, IEEE Trans. On Information Theory, 52 (4), 1289 - 1306, 2006.

3. Donoho D., Chen, S., Saunders, M., ‘‘Atomic decomposition by basis pursuit’’, SIAM Journal on Scientific Computing, 20 (2), 33-61, 1998.

4. Baraniuk, R., ‘‘Compressive sensing’’, *IEEE Signal-Processing Magazine*, 24(4), pp. 118-121, July 2007.

5. Candès, E. and Wakin, M., ‘‘An introduction to compressive sampling’’, *IEEE Signal Processing Mag*., Vol. 25, No. 2, p. 21-30, 2008.

6. Anila Satheesh, B., Deepa, B., Subhadra, B., Anjana Devi S., ‘‘Compressive Sensing for Array Signal Processing’’, *IEEE Transactions on Information Theory*, p.555-561, 2012.

7. Washington, L. C., ‘‘*Elliptic Curves, Number Theory and Cryptography’’,* Chapman&Hall/Crc, 2003.

8. Schneier, B., ‘‘*Applied Cryptography - Protocols, Algorithms, and Source code in C’’*, John Wiley & Sons, Inc., 2nd edition, 1996.

9. Amir M. A. and Esther R., ‘‘Compressive Sensing: From Compressing while Sampling to Compressing and Securing while Sampling’’, *32nd Annual International Conference of the IEEE EMBS,* Buenos Aires, Argentina, August 31 - September 4, 2010.

10. Minal C. andRajankar S., ‘’StudytheEffects of Encryption on CompressiveSensed Data’’, *International Journal of Engineeringand Advanced Technology (IJEAT)* ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.

11. Rachlin Y. and Baron D., “The Secrecy of Compressed Sensing Measurements, Communication, Control, and Computing”, 2008 46th Annual Allerton Conference, 813 – 817, Urbana-Champaign, IL.

12. C. Dwork, F. McSherry, and K. Talwar, “The Price of Privacy and the Limits of LP Decoding,” Symp. *on Theory of Computing (STOC)*, June 2007.

13. Orsdemir A, Altun H.O., Sharma G., et al., “On the Security and Robustness of Encryption via Compressed Sensing”, *Proceedings of the IEEE military communications conference MILCOM*, 2008.

14. Ramezani M., Seyfe, B., Bafghi, H.G.,“Perfect Secrecy via Compressed Sensing”, Communication and Information Theory (IWCIT), Iran Workshop on, 8-9 May 2013, Tehran, 1-5, 2013.

15. Zhang Y., Wong K., Xiao D., Zhang L.Y., Li M., “Embedding Cryptographic Features in Compressive Sensing”, *Cryptography and Security, Information Theory,*arXiv:1403.6213.

16. Zhang X., Ren Y., Feng G., Qian Z., “Compressing Encrypted Image Using Compressive Sensing”, Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011 Seventh International Conference, 222 – 225, Dalian, 14-16 Oct. 2011.

17. Yan Mo, Aidi Zhang, Fen Zheng, Nanrun Zhou, ‘‘An Image Compression-Encryption Algorithm Based on 2-D Compressive Sensing’’, *Journal of Computational Information Systems* 9: 24, 10057-10064, 2013.

 doi:10.20944/preprints201807.0258.v1

18. Gilbert A., Indyk P., "Sparse recovery using sparse matrices", *Proceedings of the IEEE*, Vol. 98, No. 6, pp. 937–947, 2010.

19. Tropp J., Gilbert A.C., "Signal Recovery from Partial Information via Orthogonal Matching Pursuit", IEEE Trans. Inform. Theory, Vol. 53, No. 12, p. 4655-4666, 2007.

20. Menezes, A. J., ''*Handbook of Applied Cryptography''*, Boca Raton: CRC Press, 1997.

21. Rivest, R., Shamir A. ve Adleman, L., " A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, 21 (2),120-126, 1978.

22. K. Ersoy, O. And Nouira, A., ''Image CodingWithTheDiscreteCosine-III Transform'', *IEEE Journal On SelectedAreasInCommunıcations*, Vol. 10. No. 5, June 1992.