Sigma J Eng & Nat Sci 36 (1), 2018, 99-111

Sigma Journal of Engineering and Natural Sciences
Sigma Mühendislik ve Fen Bilimleri Dergisi

Research Article

SIMULTANEOUS COMPRESSIVE SENSING WITH OPTICAL ENCRYPTION OF SIGNALS AND IMAGES AGAINST ATTACKS

Ertan ATAR*[1], Okan ERSOY[2], Lale ÖZYILMAZ[3]

[1] *Türk Telekom, İSTANBUL;* ORCID:0000-0002-3902-7011
[2] *School of ECE., Purdue University, Indiana, USA;* ORCID:0000-0002-7626-0584
[3] *Electronics&Com. Eng. Dept., Yildiz Technical Univ., İSTANBUL;* ORCID:0000-0001-9720-9852

Received: 19.07.2017 Revised: 16.11.2017 Accepted: 10.01.2018

ABSTRACT

Compressive Sensing (CS), which makes it possible to reduce the amount of data and thereby greatly simplify the sensor system has become a very important research area. In this method, data is compressed before measurements whereas data is first measured and then compressed in the current technology. This approach leads to reducing the number of sensors. In this study, simultaneous compressive sensing and optical cryptography is developed as a new approach for encryption and decryption of signals and images. In the current work, CS is achieved with the orthogonal matching pursuit (OMP) algorithm. Then, the CS-OMP algorithm is combined with the double random phase/amplitude encyrption (DRPAE) method to achieve both compression and encyrption of data. In order to achieve high security, the keys used in DRPAE are transmitted to the receiver by an asymmetric cryptography method, such as the RSA method. Thus, the overall cryptographic system is a hybrid optical system (both symmetric and asymmetric) since DRPAE is a symmetric optical encyrption method. In this approach, the use of the detection matrix in CS also protects DRPAE phase/amplitude keys against well-known attacks which no longer function. The data size is also decreased.

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

1. INTRODUCTION

According to classical signal processing methods, when the signal is sampled, Nyquist criterion must be satisfied to avoid loss of information. After sampling, if the signal is compressible, the signal is further compressed typically by a transform method [1-4].

In the CS method, the signal is supposed to be sparse in the sense that most signal values are assumed to be negligibly small (close to zero). In practice, this can be achieved with a transform such as the discrete cosine transform with commonly used 1-D signals such as audio signals and 2-D signals such as natural images. In the CS method, the sparse signal is further transformed by a measurement matrix to another space. The measurement matrix must be such that the original signal can be recovered without loss by using a CS method such as OMP [5-8].

[*] Corresponding Author: e-mail: ertan.atar@turktelekom.com.tr, tel: (506) 351 52 39

Cryptography in volves encryption and decryption of information. The mathematical methods for security of information, data integrity and identity validation are significant topics of cryptography [8, 9].

In this study, we propose a method for encyrption and decryption of signals and images by simultaneous use of compressive sensing and optical cryptography. In the current work, OMP is used for compressive sensing. The measurement matrix used in CS makes attack on the DRPAE method extremely difficult. For this purpose, the detection matrix is not considered to be another cryptographic key in the current work.

2. PREVIOUS STUDIES

Amir and Ester proposed EEG signals to be encrypted by using the measurement vector of the EEG signal [10]. Minal and Rajankar proposed to change the rows and columns of the detection matrix for encryption [11]. Rachlin et al. and Dwork et al. proposed using CS for data security and encryption [12], [13]. Özdemir et al. proposed using a random detection matrix as an encryption key [14]. Ramezani et al. also proposed using a detection matrix for encryption and decryption [15]. Zhang et al. proposed an encryption and decryption method by using two different detection matrices [16]. Moreover, Zhang et al. used two different transform methods to generate a detection matrix for encryption and decryption [17]. Mo et al. proposed to use the Hadamard matrix as detection matrix for encryption and decryption [18]. In the proposed method in this paper, CS is used to make attack on DRPAE method extremely difficult. References on optical cryptography are given in the succeeding sections.

3. 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 [1, 2, 4, 7, 19, 20].

The procedure for the OMP algorithm 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

$\left|\bullet\right|_2$ = 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

```
$h_l = A^t r_l$
$\Lambda_{l+1} = \Lambda_l \cup \arg\max(h_l)$
$A'_{l+1} = A[\Lambda_{l+1}]$
$x_{l+1} = \arg\min_z |y - A'_{l+1} z|_2$
$l = l + 1$
end while
Output:
$\hat{x} = x_l$
```

In the OMP program utilized, the detection matrix was generated by using one of fast transforms, namely, 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] with pre and post permutation matrices. 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.

4. A DISCUSSION OF CRYPTOGRAPHY

Cryptography refers to the methods of encryption and decryption of information. Cryptoanalysis involves methods to investigate the strengths and weaknesses of cryptographic systems [22-24].

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 [22-24]. In the proposed method, the RSA algorithm was used for asymmetric encryption of the DRPAE keys [25]. Its procedure is given below.

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* is an integer less than and coprime to *Q= (p-1)(q-1*), d is found by

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

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

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

$$C = M^e \bmod N \qquad (2)$$

Decryption is achieved by recovering *M* from *C* by using

$$C^{d} = M \bmod N \qquad (3)$$

Using asymmetric and symmetric encryptions together is named hybrid cryptography.

5. SIMULTANEOUS COMPRESSIVE SENSING AND OPTICAL ENCRYPTION

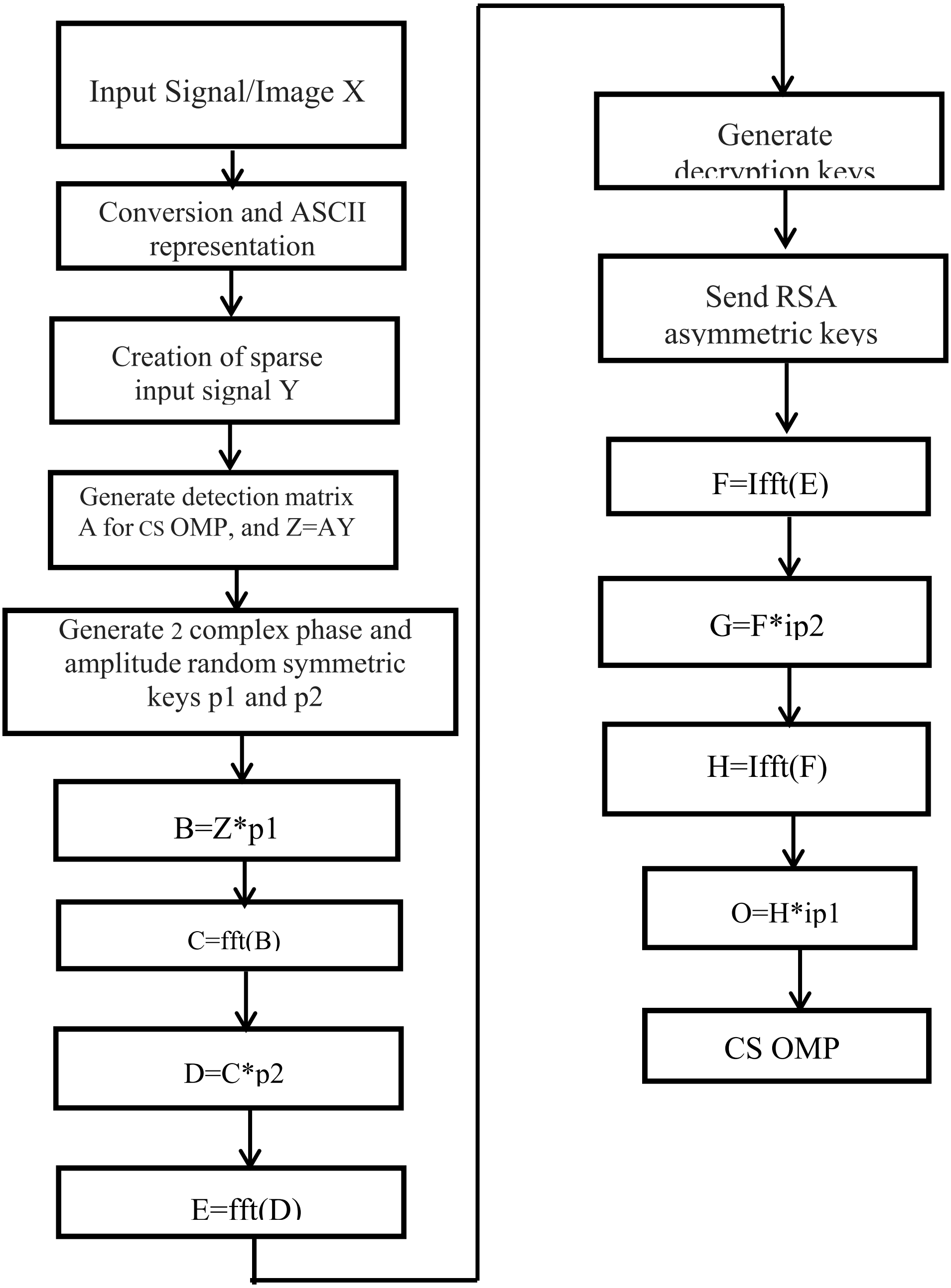
Simultaneous compressive sensing and optical encryption (SCOE) is proposed for efficient processing and secure transmission of signals and images. In this work, CS is achieved with the orthogonal matching pursuit (OMP) algorithm.

Figure 1 shows the flow diagram of SCOE. 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.

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 SCOE method is applied per block (vector) as shown in Figure 1. 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. 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.



Input Signal/Image X
Conversion and ASCII representation
Creation of sparse input signal Y
Generate detection matrix A for CS OMP, and Z=AY
Generate 2 complex phase and amplitude random symmetric keys p1 and p2
B=Z*p1
C=fft(B)
D=C*p2
E=fft(D)
Generate decryption keys
Send RSA asymmetric keys
F=Ifft(E)
G=F*ip2
H=Ifft(F)
O=H*ip1
CS OMP

Figure 1. Flowchart diagram of SCOE

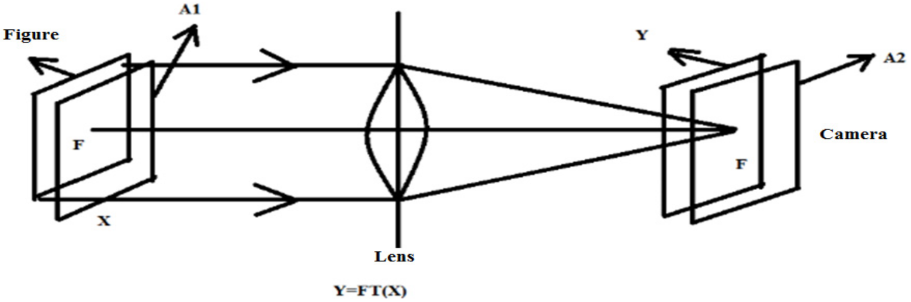


Figure 2. 2-f optical encryption system

6. EXPERIMENTAL RESULTS

The experimental results with images are shown in Figures 3, 4, 5 and 6.

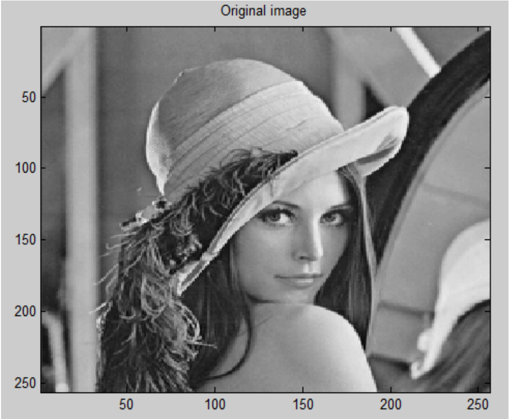


Figure 3. Original image

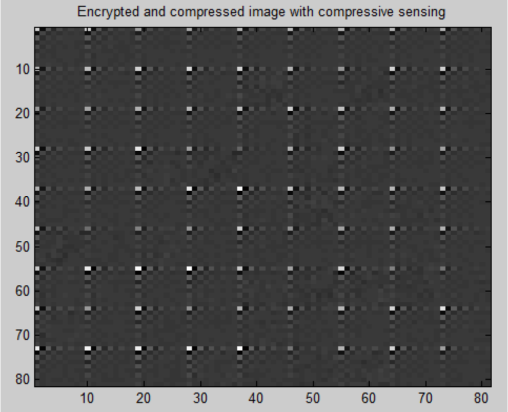


Figure 4. Encrypted image by SCOE method and blockwise processing

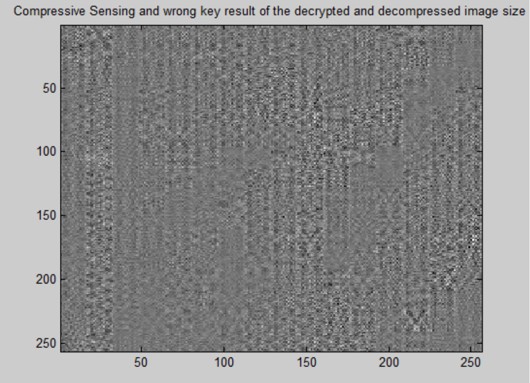


Figure 5. Decrypted image when the wrong key was used

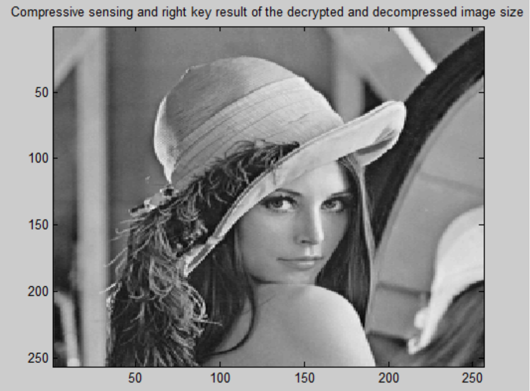


Figure 6. Decrypted image when the correct key was used.

Figure 3 shows the original LENA image. Figure 4 shows the encrypted image obtained with the SCOE method and blockwise processing. Figure 5 shows the result obtained after decryption when the wrong key was used. The image is totally unrecognizable. Figure 6 shows the result obtained after decryption when the correct key was used. The image is essentially the same as the original image.

Examples of encryption with 1-D signals are shown in Figures 7 thru 18. Figures 7 and 13 show two 1-D signals. Comparative encrypted results with the optical method using only phase keys and the proposed method with phase/amplitude keys are shown in Figures 9 and 15.

Only the phase ($e^{j\theta}$) key is used in the phase-only key generation in the studies [26-29]. Examples of such keys are shown in Figures 11 and 12. In our study, the phase/ amplitude (A* $e^{j\theta}$) key was used to generate the key. Examples of such keys are shown in Figures 17 and 18. Comparison of Figures 9 and 15 shows that the proposed method has obtained much more complex encrypted signal. This means that the encrypted signal is safer.

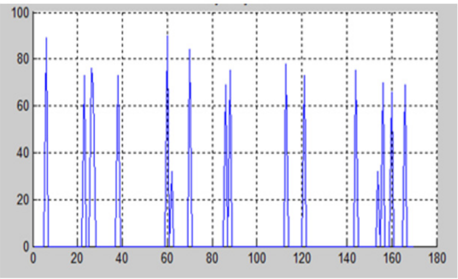


Figure 7. Original 1-D signal

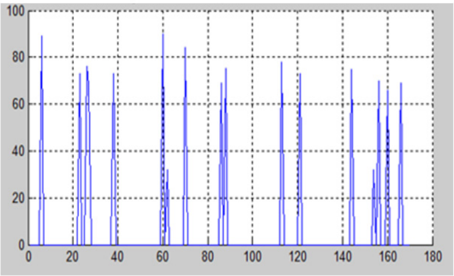


Figure 8. Decrypted signal when the correct key was used

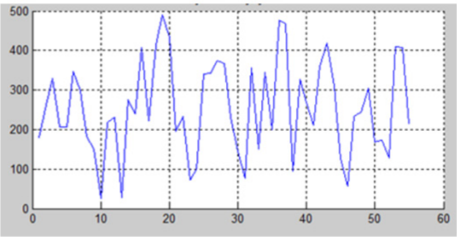


Figure 9. Encrypted signal with the optical method using phase only keys

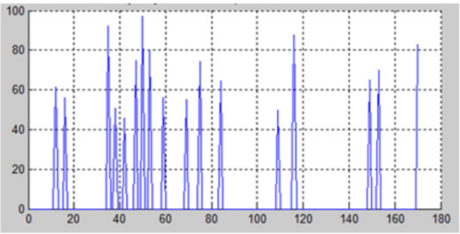


Figure 10. Decrypted signal when the wrong key was used

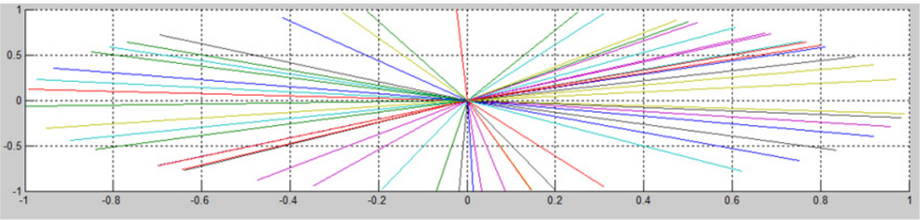


Figure 11. First phase key

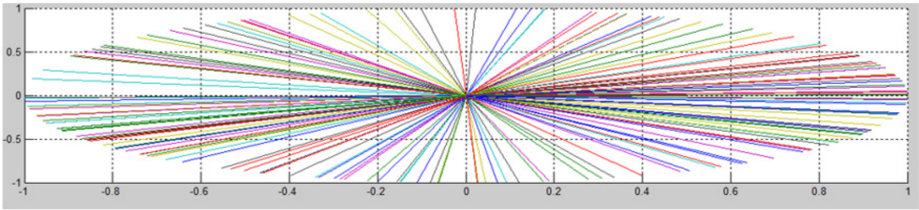


Figure 12. Second phase key

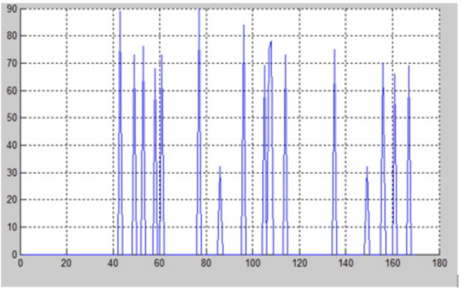


Figure 13. Original 1-D signal

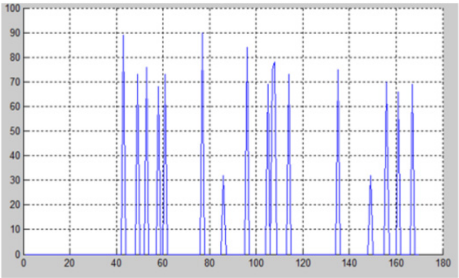


Figure 14. Decrypted signal when the correct key was used

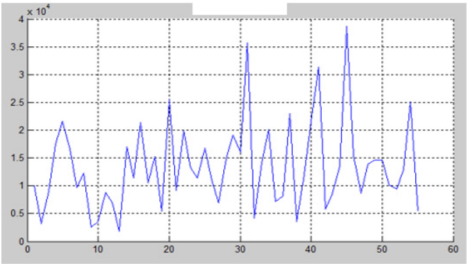


Figure 15. Encrypted signal by CSOE method

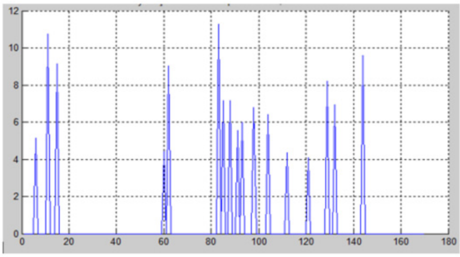


Figure 16. Decrypted signal when the wrong key was used

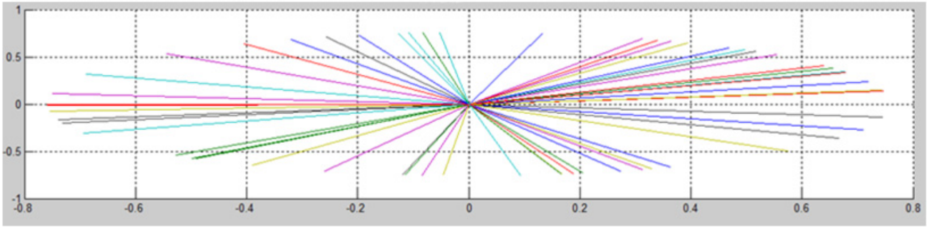


Figure 17. First phase/amplitude key

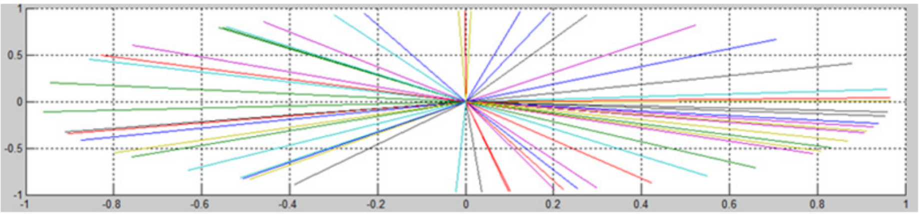


Figure 18. Second phase/amplitude key

7. CRYPTOANALYSIS OF SCOE

Usually, there are two different types of attack for analysis of optical encyrption. These attacks usually use phase recovery methods and the method based on the Dirac delta function. KPA (Known-Plaintext Attack) method used for these attacks is assumed to have access to more than one plaintext/ ciphertext pairs encrypted by using the same keys.

First, the phase recovery method will be discussed. The flow diagram of the cryptographic method studied by Zhang et al is shown in Figure 19 [26]. They did not use compressive sensing and asymmetric cryptography.

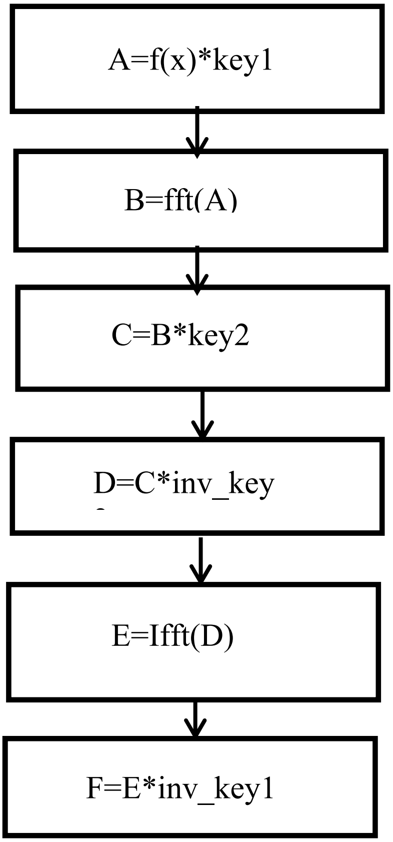


Figure 19. Flowchart diagram of the method studied by Zhang and Wei [26]

According to flowchart in Figure 19, *f(x)* and *C*, key1 and key2 are to be obtained. When the keys are based on phase only, their modulus is unity, and the problem is equivalent to recovery of phase from known amplitudes in the signal and frequency domains [26-30]. Because the keys are phase only, the retrieval of key 2 is sufficient for decryption. An example of phase recovery method is the ER (Error Reduction) algorithm. Here the lost phase is recovered by alternating between the image domain and its transform domain, and by using a priori information at each iteration such as known amplitude.

When the keys are based on both amplitude and phase, as proposed in this paper, the keys can not be retrieved with this approach. The experimental results are shown in Figures 20 and 21.

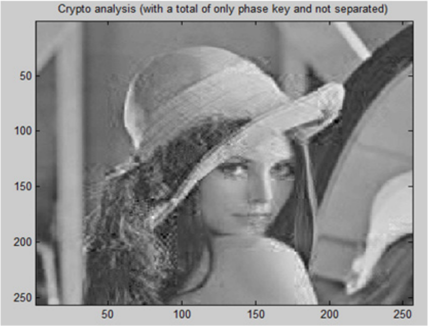

Crypto analysis (with a total of only phase key and not separated)
50
100
150
200
250
50
100
150
200
250

Figure 20. Crypto analysis result when the keys are phase only

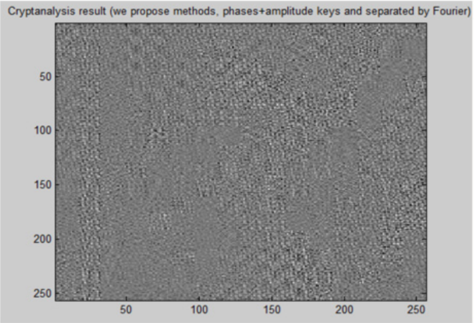

Cryptanalysis result (we propose methods, phases+amplitude keys and separated by Fourier)
50
100
150
200
250
50
100
150
200
250

Figure 21. Cryptoanalysis result with the proposed method using phase/amplitude keys

In another attack method, the Dirac-delta function is used. The Dirac delta function shown in Figure 22 is defined by

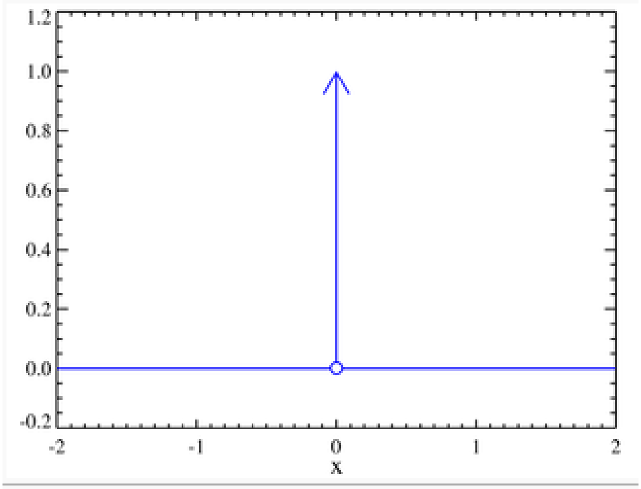


Figure 22. Dirac delta function

$$\delta(x-x_0)=\begin{cases}\mathbf{1} & x=x_0\\ \mathbf{0} & x\neq x_0\end{cases} \tag{4}$$

By repeated use of the Dirac delta function originating at each pixel or signal element, the overall encryption matrix can be obtained. This is not sufficient for decryption in the proposed method due to use of CS which requires the measurement matrix is known. The measurement matrix is part of the overall encryption matrix retrieved by the Dirac delta function method, and is otherwise not known to the attacker.

Thus, attacks based on methods such as the phase recovery technique and the Dirac delta technique fail with SCOE due to the use of phase/amplitude keys and CS utilizing a measurement matrix.

8. CONCLUSIONS

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

The phase/amplitude keys were used in a 4f optical cryptography system in one dimension. The measurement matrix for the OMP algorithm was also 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) together with random permutation matrices before and after the transform matrix. In the experiments, DC3T gave the best results in terms of complexity of the operations and the accuracy of the decryption results.

In this study, Orthogonal Matching Pursuit is used as the Compressive Sensing method. When phase-only keys are used as in references [26-29], plain text attack methods, for example, by using phase retrieval techniques, are successful in breaking the encryption algorithm. In the proposed method, phase/amplitude keys and 4f optics are used. As a result, the method is secure against previously used phase recovery attack methods.

The other type of attack on optical cryptography is based on the Dirac delta function method, which is effective in recovering the complete encryption matrix, but this is not usable for decryption in the proposed method since OMP requires the measurement matrix which is part of the complete encryption matrix, and is not available by itself.

The experimental results with signals and images used for encryption/decryption showed that the method is capable of high accuracy encryption and decryption with correct keys. It was not possible to achieve correct decryption when the proposed attack methods were used.

REFERENCES

[1] Candes E., “Compressive sampling”, *International Congress of Mathematicians (ICM)*, vol. 3, pp. 1433–1452, 2006. Madrid, Spain.

[2] Foucart S., Rauhut H., “Mathematical Introduction to Compressive Sensing”, 2013, Springer New York Heidelberg Dordrecht London, ISBN 978-0-8176-4947-0

[3] http://users.ece.gatech.edu/_justin/ssp2007.

[4] Gilbert A., Indyk P., “Sparse recovery using sparse matrices”, *Proceedings of the IEEE*, Vol. 98, No. 6, pp. 937–947, 2010.

[5] Donoho D., “Compressed Sensing”, *IEEE Tran. Information Theory*, 52(4), pp. 1289 - 1306, April 2006.

[6] Shannon C. E., “Communication in the Presence of Noise”, Proc. Institute of Radio Engineers, Vol. 37, pp. 10–21, 1949.

[7] http://infonet.gist.ac.kr/.

[8] Baraniuk R., “Compressive sensing”, *IEEE Signal Processing Magazine*, 24(4), pp. 118-121, July 2007.

[9] Baron D., Wakin M. B., Duarte M. F., Sarvotham S., Baraniuk R. G., “Distributed Compressed Sensing”, *Tech. Rep. TREE-0612*, Rice University, Department of Electrical and Computer Engineering, 2006.

[10] Amir M. A, 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.

[11] Minal C., Rajankar S., “Study the Effects of Encryption on Compressive Sensed Data” *International Journal of Engineering and Advanced Technology* (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.

[12] Rachlin Y., Baron D., "The Secrecy of Compressed Sensing Measurements", *Communication, Control, and Computing*, 2008 46th Annual Allerton Conference, 813 – 817, Urbana-Champaign, IL.

[13] Work F., McSherry M., Talwar K., "The Price of Privacy and the Limits of LP Decoding", *Symp. on Theory of Computing (STOC)*, June 2007.

[14] Örsdemir A., Altun H. O., Sharma G., "On the Security and Robustness of Encryption via Compressed Sensing", *Proceedings of the IEEE military communications conference MILCOM*, 2008.

[15] 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.

[16] 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.

[17] 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.

[18] Mo Y., Zhang A., Zheng F., Zhou N., "An Image Compression-Encryption Algorithm Based on 2-D Compressive Sensing", *Journal of Computational Information Systems* 9: 24, 10057-10064, 2013.

[19] Donoho D., Chen S., Saunders M., "Atomic Decomposition by Basis Pursuit", *SIAM Journal on Scientific Computing*, Vol. 20 p.33-61, 1998.

[20] 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.

[21] Ersoy O., Nouira A., "Image Coding with the Discrete Cosine-III Transform", IEEE *Journal On Selected Areas in Communıcation*s, Vol. 10. No. 5, June 1992.

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

[23] Washington L. C., 2003, *Elliptic Curves, NumberTheory and Cryptography,* Chapman&Hall/Crc.

[24] Menezes A. J., *Handbook of Applied Cryptography*, Boca Raton: CRC Press, 1997.

[25] RivestR., Shamir A., Adleman L. A., "Method for Obtaining Digital Signatures and Public-Key Crypto Systems", *Communications of the ACM*, 21 (2), 120-126, 1978.

[26] Peng X., Zhang P., Wei H., "Known-Plain Text Attack on Optical Encryption Based on Double Random Phase Keys", *Optics Letters*, Vol. 31, No. 8, April 15, 2006.

[27] Peng X., Wei H.,Zhang P., "Chosen Plaintext Attack on Lensless Double Random Phase Encoding in the Fresnel Domain", *Optics Letters*, Vol. 31, No. 22, November 15, 2006.

[28] Carnicer A.,Usategui M., Arcos S., Juvells I., "Vulnerability to Chosen Ciphertext Attacks of Optical Encryption Schemes Based on Double Random Phase Keys",*Optics Letters,* Vol. 30, No. 13,July 1, 2005.

[29] Frauel Y., Castro A., Naughton T., Javidi B., "Resistance of the Double Random Phase Encryption against Various Attacks", *Optics Express*, Vol. 15, No. 16, 6 August 2007.

[30] Atar E., Ersoy O., Özyılmaz L., "Hybrid Data Compression and Optical Cryptography with Orthogonal Matching Pursuit"*, Journal of theFaculty of Engineering and Architecture of Gazi University*, 32:1 (2017) 139-147, 2017.