2014 International Joint Conference on Neural Networks (IJCNN)
July 6-11, 2014, Beijing, China

Image Encryption Based on Compressed Sensing and Blind Source Separation

Zuyuan Yang
Faculty of Automation
Guangdong University of Technology
Guangzhou, 510006, China
School of Information Technology
Deakin University
Melbourne, VIC 3125, Australia
Email: yangzuyuan@aliyun.com

Yong Xiang
School of Information Technology
Deakin University
Melbourne, VIC 3125, Australia
Email: yxiang@deakin.edu.au

Chuan Lu
Faculty of Automation
Guangdong University of Technology
Guangzhou, 510006, China
Email: Luchuan@gmail.com

***Abstract*—A novel image encryption scheme based on compressed sensing and blind source separation is proposed in this work, where there is no statistical requirement to plaintexts. In the proposed method, for encryption, the plaintexts and keys are mixed with each other using a underdetermined matrix first, and then compressed under a project matrix. As a result, it forms a difficult underdetermined blind source separation (UBSS) problem without statistical features of sources. Regarding the decryption, given the keys, a new model will be constructed, which is solvable under compressed sensing (CS) frame. Due to the usage of CS technology, the plaintexts are compressed into the data with smaller size when they are encrypted. Meanwhile, they can be decrypted from parts of the received data packets and thus allows to lose some packets. This is beneficial for the proposed encryption method to suit practical communication systems. Simulations are given to illustrate the availability and the superiority of our method.**

I. Introduction

In the modern society, people can access different information conveniently and signal communication or information exchange becomes more and more frequent. Since visual information plays a very important part in human sensing, lots of image signals need to be transmitted from equipments or persons by public networks every day. In these data, many of them are private and not permitted to be accessed by someone else. However, current network systems are far from perfect [1]. As a result, how to protect the kernel information attracts more and more attention, and encryption becomes a natural choice. Regarding signal encryption, there exist lots of methods, such as the traditional data encryption standard (DES) and method of Rivest, Shamir, and Adleman (RSA) [2]-[4], the analog encryption [5], the chaotic system based method [6], etc.

As we know, for images, the original plaintexts are composed of partly distorted samples. It is acceptable to recover the plaintext approximately and not analytically. Thus, the blind source separation (BSS) based schemes are invoked for image encryption [7]-[9]. In this attractive scheme, encryption relies on the difficulty of solving ill-conditioned BSS problem, rather than the traditional apparently intractability of the computational problem. It provides a strong security for the corresponding cryptosystems. Regarding the decryption, it often needs special features of the sources or plaintexts, such as the independence [10] [11], nonnegativity [12]-[15], etc. However, these features may be lost during data transmission sometimes, leading to a hard decryption for the plaintexts, especially when the ciphertexts are transmitted in a unstable network environment.

In this paper, motivated by that the newly developed compressed sensing (CS) technology can reconstruct signals from parts of the samples [16] [17], we embed CS into traditional BSS based encryption scheme, and propose a novel CS and BSS based image encryption method (called CS-BSS scheme). In the proposed method, for encryption, it forms an ill-conditioned BSS problem which is hard to solve and thus the system security is comparable to current BSS based encryption schemes. Regarding the decryption, given the key, the mentioned BSS problem will be simplified and transformed into a typical CS problem which can be solved using a number of existing algorithms, such as the matching pursuit algorithms [18] [19], the L1-norm based methods [20] [21], the threshold algorithm [22], etc. Due to the usage of CS technology, the plaintexts can be not only encrypted but also compressed into the data with smaller size. Furthermore, the CS method can reconstruct the plaintexts from parts of the samples and thus allows to lose some data packets, leading to a more convenient transmission for the ciphertexts in current network environments.

The remainder of this paper is organized as follows. In Section II, the BSS and CS models are introduced, and the image encryption and decryption methods are proposed in Section III. In Section IV, the proposed encryption method is tested using different kinds of images. Finally, conclusions are given in Section V.

II. BSS and CS Models

In this section, the BSS and CS models will be introduced briefly.

A. BSS Model

Mathematically, instantaneous mixing BSS model is as follows:

$$\mathbf{H} = \mathbf{AS} \tag{1}$$

978-1-4799-1484-5/14/$31.00 ©2014 IEEE

where $\mathbf{H} \in \Re^{m\times N}$ is the observation matrix or signals, $\mathbf{A} \in \Re^{m\times n}$ is the mixing matrix, $\mathbf{S} \in \Re^{n\times N}$ is the source matrix or signals, and m, n, N denote the numbers of the observations (or outputs), the sources (or inputs) and the samples, respectively.

Generally, if the mixing matrix is full column rank and the source signals are mutually independent, one can recover the sources from the observations. However, in the case that the mixing matrix is underdetermined, i.e., the column number is larger than the row number, the BSS problem will become much more difficult, especially when the sources are neither independent nor sparse. Actually, in the underdetermined mixing case, the number of $\mathbf{S}$ satisfying (1) is infinite. When the real $\mathbf{S}$ is not sparse, it is hard to access it from the observations, and this feature will be developed to encrypt the sources or plaintexts in our paper. Regarding the decryption, the following CS based method is employed.

B. CS Model

CS aims to reconstruct a signal from several linear measurements of its samples. The typical sensing model is as follows:

$$\mathbf{y} = \mathbf{\Phi s} \tag{2}$$

where $\mathbf{y}$ denotes the sensing vector, $\mathbf{\Phi}$ stands for the project matrix, $\mathbf{s}$ is the original signal. In the above model, the row number of $\mathbf{\Phi}$ is often much smaller than its column number, and $\mathbf{s}$ has a sparse representation under a known square basis matrix, i.e.,

$$\mathbf{s} = \mathbf{\Psi c} \tag{3}$$

where $\mathbf{\Psi}$ denotes the basis matrix and $\mathbf{c}$ is the representation coefficient.

Given the project matrix $\mathbf{\Phi}$ and the basis matrix $\mathbf{\Psi}$, one can reconstruct the original high dimensional signal $\mathbf{s}$ from the low dimensional CS signal $\mathbf{y}$ by using a series of existing methods [18]-[22]. Since image signals are often sparse under some known bases (such as discrete cosine transfom (DCT) basis [23] and wavelet basis [24]), the CS reconstructing algorithms will be utilized for decryption in our method, after the difficult underdetermined BSS problem is transformed into the CS frame.

III. Proposed Image Encryption

In this section, the proposed CS-BSS based encryption scheme is presented and analyzed, including the encryption, the decryption, and the analysis to the keys and the project matrix.

A. Preprocessing and Encryption

Regarding the preprocessing, it mainly includes dividing frames and splitting segments for original images. By using the method in [9], we get M frames from the original images and each frame is split into P segments with the same length L. Then, each segment is normalized to be in [0, 1], and the corresponding waveform information is stored in a definite format. Finally, the parameters M, P, L and this information are inserted into the head data of the encrypted signal in a pre-definite format for transmission. After preprocessing, the signals $\mathbf{S} = [\mathbf{s}_1^T, \mathbf{s}_2^T, \cdots, \mathbf{s}_n^T] \in \Re^{n\times N}$ (called plaintexts), where $\mathbf{s}_i, i = 1, 2, \cdots, n$ denotes the ith row of $\mathbf{S}$, are encrypted through the following steps:

Step 1: generate a random mask matrix $\mathbf{U} \in \Re^{n\times N}$, and let $\mathbf{V}$ be the combination of $\mathbf{S}$ and $\mathbf{U}$, i.e.,

$$\mathbf{V} = [\mathbf{S}; \mathbf{U}] \tag{4}$$

Step 2: design a project matrix $\mathbf{\Phi} \in \Re^{p\times N}$, and compress $\mathbf{V}$ into $\mathbf{Y}$ by

$$\mathbf{Y} = \mathbf{V\Phi}^T \tag{5}$$

Step 3: construct a underdetermined mixing matrix $\mathbf{A} \in \Re^{n\times 2n}$, and mix the compressed $\mathbf{Y}$, then, the ciphertext is calculated by

$$\mathbf{X} = \mathbf{AY} = \mathbf{AV\Phi}^T \tag{6}$$

The plaintexts are encrypted frame by frame using the model (6).

B. Decryption and Reconstruction

In the process of decryption, after receiving the encrypted frame (i.e., ciphertext $\mathbf{X}$) from public network, one can regenerate $\mathbf{A}$ and $\mathbf{U}$ first, and construct

$$\mathbf{B} = [\mathbf{A}; \mathbf{0}, \mathbf{I}] \tag{7}$$

and

$$\tilde{\mathbf{X}} = [\mathbf{X}; \mathbf{U\Phi}^T] \tag{8}$$

where $\mathbf{0} \in \Re^{n\times n}$ denotes a matrix whose entries are zero, and $\mathbf{I} \in \Re^{n\times n}$ denotes the identity matrix with order n. Then, the compression $\tilde{\mathbf{S}}$ of the plaintext $\mathbf{S}$ can be obtained by

$$\tilde{\mathbf{S}} = [\mathbf{B}^{-1}\tilde{\mathbf{X}}]_{1:n} \tag{9}$$

where $[\mathbf{X}]_{1:n}$ denotes a submatrix composed of the first n rows of $\mathbf{X}$.

Since $\tilde{\mathbf{S}}$ can be rewritten as

$$\tilde{\mathbf{S}} = \mathbf{S\Phi}^T \tag{10}$$

and under a known Ψ (e.g., DCT basis [23] and wavelet basis [24]), $\mathbf{S}$ can be represented by

$$\mathbf{S} = \mathbf{C}^T\mathbf{\Psi}^T \tag{11}$$

where $\mathbf{C}$ is sparse, then, combing with (9)-(11), one can calculate $\mathbf{C}$ using existing methods in [18]-[22], and finally obtain the decryption $\mathbf{S}$ using (11).

C. Requirements of the Keys and the Project Matrix

Generally, the keys are generated randomly by computer. Unlike the ICA or the sub-band ICA based method, there is no special requirement for the keys in the proposed image encryption method, except that it should mask the plaintexts well. As for the mixing matrix, a basic requirement is that the first n columns should be full rank, and it is often constructed to make plaintexts mix with the keys as sufficient as possible. It is easy to satisfy this condition by normal computer software, e.g., a random matrix with uniform distribution is a practical candidate. Regarding the project matrix, one has a number of choices, such as the Gaussian matrix, Fourier matrix, etc [16].

IV. SIMULATIONS

In this section, two simulations are given to verify the performance of the proposed CS-BSS encryption method, and the results are compared with the existing BSS based encryption method, where the compared algorithms are PP [7], ICA [9], and TF [25]. Each method is implemented using MATLAB R2009a installed in a personal computer with Intel(R) Celeron(R) 2.4 GHz CPU, 8 GB memory and Microsoft Windows 8 operational system. The decryption performance for each segment is measured by the signal-noise-ratio (SNR) index defined as

$$SNR_i = 10 \log \frac{1}{\|\mathbf{s}_i - \hat{\mathbf{s}}_i\|^2} \tag{12}$$

where $\mathbf{s}_i$ is the ith row of the source matrix $\mathbf{S}$, $\hat{\mathbf{s}}_i$ is the ith row of the estimated source matrix $\hat{\mathbf{S}}$. Here, the L2-norms of $\mathbf{s}_i$ and $\hat{\mathbf{s}}_i$, $\forall i$ are normalized to be one and their means are zero. Clearly, the larger the SNR index is, the better the decryption performs.

A. Simulation 1

In this simulation, the proposed encryption method is tested using the widely used 256×256 Lena image (see Fig. 1(a)). The plaintext is set to have one frame, and each frame has 4 segments with 16384 samples, i.e., $M = 1, P = 4, L = 16384$. The model (6) is used for encryption, where $\mathbf{A}$, $\mathbf{U}$, and $\mathbf{\Phi}$ are generated randomly by Matlab software. Four segments are encrypted each time, i.e., $n = 4$, and the plaintexts are compressed 25%. Fig. 1(b) shows the the encrypted signals $\mathbf{X}$, where the pure black part is virtual and added for visual comparison, as $\mathbf{X}$ is a compression of $\mathbf{S}$. In the process of decryption, the DCT matrix is used as the basis matrix $\mathbf{\Psi}$ and the L1-LS method in [20] are invoked for reconstruction for our CS-BSS based scheme.

Table I gives the SNR indices of the compared methods. One can see that our method has the largest SNR index for each segment, implying the highest precision. Since the plaintext is compressed, the features of local dominance, independence, and time-frequency are damaged. As a result, the compared existing methods can hardly get a satisfied decryption. The corresponding decrypted images are given in Fig. 1(c)-(f), respectively.

TABLE I. $SNRs$(DB) OF DIFFERENT METHODS FOR HUMAN IMAGE

	CS-BSS	PP	ICA	TF
$\mathbf{s}_1$	21.0562	5.3421	4.3419	5.2150
$\mathbf{s}_2$	22.7631	5.7827	4.9082	3.3758
$\mathbf{s}_3$	20.9872	4.2314	4.8903	3.4370
$\mathbf{s}_4$	24.2317	5.0967	5.2574	6.4452

B. Simulation 2

In this simulation, a natural image is used to test the proposed method. It is split into four segments or sources. Similar to simulation 1, $\mathbf{A}$ and $\mathbf{U}$ are generated randomly, and the involved parameters are $M = 1, P = 4, L = 16384, n = 4$. Table II gives the SNR indices of the compared methods. And the plaintexts, the encryptions and the decryptions are show in Fig. 2(a)-(f), respectively.

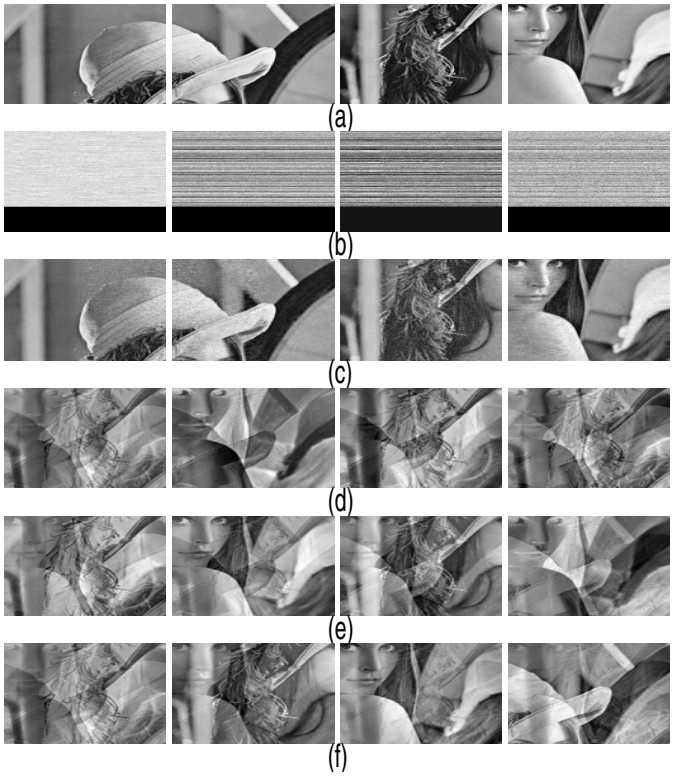

Fig. 1. Plaintexts, keys, ciphertexts, and the decryptions using different methods for human image; (a) Plaintexts; (b) Ciphertexts; (c) Decryptions using our CS-BSS; (d) Decryptions using PP; (e) Decryptions using ICA; (f) Decryptions using TF.

We also test the cases that some data packets of the ciphertexts are lost during transmission in the public networks. The experimental results that about 10% packets are lost are provided here. Table III shows the corresponding decryption results in five random experiments (only the results of our CS-BSS method are given, as the compared methods performs not good even no packet is lost), where the lost packets are different in each experiment. One can see that the SNR indices decrease slightly, but still acceptable. It is worth noting that the results are nearly not changed when different packets are lost, implying the robustness of the proposed method in the unstable network environments.

TABLE II. $SNRs$(DB) OF DIFFERENT METHODS FOR NATURAL IMAGE

	CS-BSS	PP	ICA	TF
$\mathbf{s}_1$	23.1325	4.8722	4.2091	4.9962
$\mathbf{s}_2$	24.3349	5.0238	5.0187	4.1937
$\mathbf{s}_3$	23.7693	4.3390	4.3306	4.2115
$\mathbf{s}_4$	25.5328	4.8904	5.0028	5.1572

TABLE III. $SNRs$(DB) OF THE PROPOSED METHOD FOR NATURAL IMAGE IN THE DATA PACKETS LOST CASES

	First	Second	Third	Fourth	Fifth
$\mathbf{s}_1$	22.0375	22.1002	22.0921	21.9982	21.8909
$\mathbf{s}_2$	21.9803	21.8301	22.0012	22.0125	21.9937
$\mathbf{s}_3$	21.6429	21.7639	21.5349	21.7192	21.7830
$\mathbf{s}_4$	24.3371	24.3518	24.4013	24.4011	24.5916

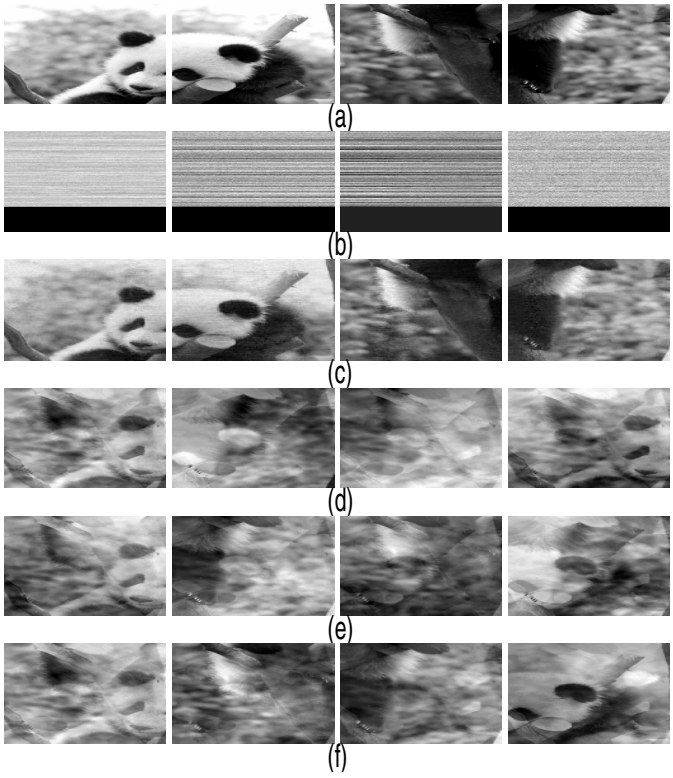

Fig. 2. Plaintexts, ciphertexts, and the decryptions using different methods for natural image; (a) Plaintexts; (b) Ciphertexts; (c) Decryptions using our CS-BSS; (d) Decryptions using PP; (e) Decryptions using ICA; (f) Decryptions using TF.

V. Conclusion

In this paper, a new image encryption method based on CS and BSS is proposed, where the difficult underdetermined BSS system is designed for encryption and the CS based technology is utilized for decryption. The proposed method has the advantage of simultaneous encryption and compression. Furthermore, it allows to lose some data packets during the transmission of the ciphertexts and thus has a wide application in practical data communication securely. Finally, simulations of human image and natural image are given to verify the availability and the advantages of the proposed method.

Acknowledgment

The authors would like to thank the anonymous reviewers and the financial support from the National Natural Science Foundation of China under grant 61104053 and 61271210, the Program for NCET, and the Natural Science Foundation of Guangdong Province under grant S2011030002886.

References

[1] N. Merhav, "Perfectly secure encryption of individual sequences," IEEE Trans. Information Theory, vol. 59, no. 3, pp. 1302-1310, 2013.

[2] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996.

[3] *http://www.rsa.com/rsalabs.*

[4] D. E. Denning, *Cryptograghy and Data Security*. Reading, MA: Addison-Wesley, 1982.

[5] F. L. Ma, J. Cheng, and Y. M. Wang, "Wavelet transform-based analog speech scrambling scheme," Electronic Letters, vol. 32, no. 8, pp. 719-721, 1996.

[6] K. Li, Y. C. So, and Z. G. Li, "Chaotic cryptosystem with high sensitivityto parameter mismatch," *IEEE Trans. Circuits Systems I, Fundamental Theory Applications*, vol. 50, no. 4, pp. 579-583, 2003.

[7] S. Luo, C. Luo, Z. Cai, "Image encryption via projection-pursuit based blind source separation," *International Conference on Multimedia Technology (ICMT)*, pp. 787-795, 2013.

[8] Q. Lin, F. Yin, T. Mei, and H. Liang, "A blind source separation-based method for multiple images encryption," Image Vision Comput, vol. 26, no. 6, pp. 788-798, 2008.

[9] Q. Lin, F. Yin, T. Mei, and H. Liang, "A blind sourceseparation-based method for speech encryption," *IEEE Trans. Circuits Systems I*, vol. 53, no. 6, pp. 1320-1328, 2006.

[10] J. Vía, D. P. Palomar, L. Vielva, and I. Santamaría, "Quaternion ICA from second-order statistics," *IEEE Trans. Signal Processing*, vol. 59, no. 4, pp. 1586-1600, 2011.

[11] G. Chabriel and J. Barrre, "A direct algorithm for nonorthogonal approximate joint diagonalization," *IEEE Trans. Signal Processing*, vol. 60, no. 1, pp. 39-47, 2012.

[12] Z. He, S. Xie, R. Zdunek, G. Zhou, and A. Cichocki, "Symmetric nonnegative matrix factorization: algorithms and applications to probabilistic clustering," *IEEE Trans. Neural Networks*, vol. 22, no. 12, pp. 2117-2131, 2011.

[13] Z. Yang, G. Zhou, S. Xie, etc, "Blind spectral unmixing based on sparse nonnegative matrix factorization," *IEEE Trans. Image Processing*, vol. 20, no. 4, pp. 1112-1125, 2011.

[14] G. Zhou, A. Cichocki, S. Xie, "Fast nonnegative matrix/tensor factorization based on low-rank approximation," *IEEE Trans. Signal Processing*, vol. 60, no. 6, pp. 2928-2940, 2012.

[15] G. Zhou, Z. Yang, S. Xie, J. Yang,"Online blind source separation using incremental nonnegative matrix factorization with volume constraint," *IEEE Trans. Neural Networks*, vol. 22, no. 4, pp. 550-560, 2011.

[16] D. Donoho, "Compressed sensing," *IEEE Trans. Information Theory*, vol. 52, no. 4, pp. 1289-1306, 2006.

[17] A. V. Sreedhanya and K. P. Soman, "Secrecy of Cryptography with Compressed Sensing," *International Conference on Advances in Computing and Communications (ICACC)*, pp. 207-210, 2012.

[18] S. Mallat and Z. Zhang, "Matching pursuits with time-frequency dictionaries," *IEEE Trans. Signal Processing*, vol. 41, no. 12, pp. 3397-3415, 1993.

[19] M. Davenport and M. Wakin, "Analysis of orthogonal matching pursuit using the restricted isometry property," *IEEE Trans. Information Theory*, vol. 56, no. 9, pp. 4395-4401, 2010.

[20] S. Kim, K. Koh, M. Lustig, S. Boyd, and D. Gorinevsky, "An interior-point method for large-scale L1-regularized least squares," *IEEE J. Selected Topics in Signal Processing*, vol. 1, no. 4, pp. 606-617, 2007.

[21] M. Figueiredo, R. Nowak, and S. Wright, "Gradient projection for sparse reconstruction: application to compressed sensing and other inverse problems," *IEEE J. Selected Topics in Signal Processing*, vol. 1, no. 4, pp. 586-597, 2007.

[22] T. Blumensath and M. Davies, "Iterative hard thresholding for compressed sensing," *Applied and Computational Harmonic Analysis*, vol. 27, no. 3, pp. 265-274, 2009.

[23] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete cosine transfom," *IEEE Trans. Computers*, vol. 23, no. 1, pp. 90-93, 1974.

[24] S. Berlemont and J. C. Olivo-Marin, "Combining local filtering and multiscale analysis for edge, ridge, and curvilinear objects detection," *IEEE Trans. Image Processing*, vol. 19, no. 1, pp. 74-84, 2010.

[25] V. G. Reju, S. N. Koh, and I. Y. Soon, "An algorithm for mixing matrix-estimation in instantaneous blind source separation," *Signal Processing*, vol. 89, no. 3, pp. 1762-1773, 2009.