Image encryption via projection-pursuit based blind source separation*

Luo Shiguang[1],Luo Changri[2],Cai Zhaoquan[3]

Abstract:A novel image cryptosystem by using projection pursuit based blind source separation is proposed in this work, where the plaintexts need to be neither independent nor sub-independent. In the proposed cryptosystem, for encryption, the plaintexts are mixed linearly with each other first, and then mixed nonlinearly with the ciphers. As for decryption, a projection pursuit based blind source separation method is employed. The processes of both encryption and decryption are fast, thus it is suitable for large scale of images. In addition, the ciphers can be used repeatedly. Simulations are given to illustrate the availability and the security of our cryptosystem.

Key Words: Image encryption, blind source separation, projection pursuit

I. Introduction

With the fast development of the electronic commerce, a large number of image signals are needed to transmit by public networks every day. Since current network systems are far from perfect, the information security has been attracting more and more attention. To protect the kernel information, image encryption becomes a natural choice. There exist several encryption methods, such as the traditional data encryption standard (DES) and Rivest, Shamir, and Adleman (RSA) [1]-[3], the analog encryption [4], the chaotic system based method [5], etc.

Recently, a new technology based on blind source separation (BSS) has been applied to image cryptosystem, where the decryption is cast into a BSS problem which aims to separate the mixtures (ciphertexts) into the product of the mixing coefficients and the sources (plaintexts) [6][7]. The security of this kind of cryptosystem relies on the difficulty of solving ill-conditioned BSS problem, instead of the traditional apparently intractability of the computational problem. The BSS based scheme has brought a new viewpoint for image

* This work was supported in part by the National Natural Science Foundation of China under Grant 61104053 and 61170193).

[1] LuoShiguang ,Department of Applied Mathematics, GuangDong University of Finance, Guangzhou 510521,China

[2] LuoChangri(luocr1@sina.com),National Engineering Research Center for E-Learning, College of Vocational and Continuing Education,CCNU,Wuhan, 430079, P.R. China.

[3] Cai Zhaoquan,Huizhou University, Huizhou, 516007, P.R. China.

encryption, however, regarding as the practical BSS methods, it suffers from the respective troubles, e.g., in BSS based on independent component analysis, the plaintexts are required to be mutually independent [7], and in nonnegative matrix factorization based method, the mixing matrix should be nonnegative [6].

In this paper, a projection-pursuit (PP) based BSS method is utilized for image encryption. In the proposed cryptosystem, the plaintexts are mixed nonlinearly for encryption and the fast PP algorithm is invoked for decryption [8]. Compared with the existing BSS based encryption method, the proposed scheme can achieve the decryption results in a short time. Thus, it has advantages for the encryption of large scale of images. Also, due to the usage of the non-negativity of the images, it gets out of the plaintext-independence restriction.

The remainder of this paper is organized as follows. In Section II, the PP based BSS method is introduced, and the image cryptosystem is proposed in Section III. In Section IV, the proposed cryptosystem is tested by different kinds of images. Finally, conclusions are given in Section V.

The following notations are used in the whole paper:

$\mathbf{x}, x_i$ Column vector, the i th element of $\mathbf{x}$.

$\mathbf{X}, \mathbf{x}_j, x_{ij}$ Matrix, the j th column of $\mathbf{X}$,the (i, j) th entry of $\mathbf{X}$

$\mathbf{X}_t$ Matrix with t columns

II. PP based BSS

2.1 BSS Model

BSS aims to separate the source signals from their mixtures, where the mixing matrix is unknown. Typical BSS model is as following [8] [9]:

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

where $\mathbf{X}$ denotes the observed mixtures, $\mathbf{A}$ denotes the mixing matrix, and $\mathbf{S}$ denotes the source matrix.BSS algorithms can be able to recover the sources $\mathbf{S}$ from their mixtures $\mathbf{X}$, without knowing the mixing matrix. This is very helpful for signal decryption, and there are lots of practical algorithms for solving BSS problem. Here, for processing the image signals whose values are nonnegative, we introduce the following fast and efficient projection pursuit (PP) algorithm.

2.2 PP Algorithm

The PP algorithm is mainly developed in [8], and it is used for the process of nonnegative signals. Based on the analysis in [8], this algorithm is much faster than traditional methods, with higher precision, and its main steps are as follows for a given $\mathbf{X}$:

Step 1: Calculate $\mathbf{u} = [u_1, u_2, \ldots, u_n]^T$ by solving the following problem:

$$Min: \gamma$$
$$s.t. \begin{cases} \gamma - \sum_{i=1}^{n} u_i x_{ij} < 0 \quad \forall j \\ \gamma > \delta \end{cases} \tag{2}$$

where x_{ij} is the (i, j) th entry of $\mathbf{X}$ and δ is a small positive constant(typically, $\delta = le-6$).

Step 2: Suppose $u_q \neq 0$, and let $\mathbf{U}$ be the $n \times n$ identity matrix with the q th row replaced by $\mathbf{u}^T$ and compute the diagonal matrix $\mathbf{D}$ by :

$$\mathbf{D} = diag\left(\mathbf{1}^T \square \left(\mathbf{u}^T \mathbf{X}\right)\right) \tag{3}$$

where $\square$ denotes the componentwise division. And Map $\mathbf{X}$ into $\tilde{\mathbf{X}}$ by

$$\tilde{\mathbf{X}} = \mathbf{UXD} \tag{4}$$

Step 3: Set $\mathbf{v} = 0$, and randomly generate a full-rank square matrix $\mathbf{W}$. Update $\mathbf{v}$ by

$$\mathbf{v} := \mathbf{v} + \lambda_i \mathbf{w}_i \tag{5}$$

where if $\max\left(\mathbf{w}_1^T \tilde{\mathbf{X}}\right) > 0$,select λ_i by the following rule,

$$\begin{cases} \lambda_i \geq 0, and \\ \lambda_i \left(\max\left(\mathbf{w}_i^T \tilde{\mathbf{X}}_{\Gamma_{i-1}}\right) - \max\left(\mathbf{w}_i^T \tilde{\mathbf{X}}_{\Gamma_0 - \Gamma_{i-1}}\right)\right) > \max\left(\mathbf{v}^T \tilde{\mathbf{X}}_{\Gamma_0 - \Gamma_{i-1}}\right) - \max\left(\mathbf{v}^T \tilde{\mathbf{X}}_{\Gamma_{i-1}}\right) \end{cases} \tag{6}$$

Then, the updating process in (5) stops if $\mathbf{W}\tilde{\mathbf{x}}_j = \mathbf{W}\tilde{\mathbf{x}}_k \quad for\ all\ \ j, k \in \Phi\left(\mathbf{v}, \tilde{\mathbf{X}}\right)$, and $\hat{\mathbf{a}}_1$ is estimated by

$$\hat{\mathbf{a}}_1 = \mathbf{x}_j, j = \arg\max\left(\mathbf{v}^T \tilde{\mathbf{X}}\right) \tag{7}$$

Otherwise, select λ_i by

$$\begin{cases} \lambda_i > 0, and \\ \lambda_i \left(\min\left(\mathbf{w}_i^T \tilde{\mathbf{X}}_{\Gamma_{i-1}}\right) - \min\left(\mathbf{w}_i^T \tilde{\mathbf{X}}_{\Gamma_0 - \Gamma_{i-1}}\right)\right) < \min\left(\mathbf{v}^T \tilde{\mathbf{X}}_{\Gamma_0 - \Gamma_{i-1}}\right) - mn\left(\mathbf{v}^T \tilde{\mathbf{X}}_{\Gamma_{i-1}}\right) \end{cases} \tag{8}$$

Then, the updating process of (5) stops if $\mathbf{W}\tilde{\mathbf{x}}_j = \mathbf{W}\tilde{\mathbf{x}}_k$ *for all* $j,k \in \Psi\left(\mathbf{v}, \tilde{\mathbf{X}}\right)$, and $\hat{\mathbf{a}}_1$ is estimated by

$$\hat{\mathbf{a}}_1 = \mathbf{x}_j,\ j = \arg\min\left(\mathbf{v}^T \tilde{\mathbf{X}}\right) \tag{9}$$

In (6) and (8), $\Gamma_i = \begin{cases} \left\{t \mid \mathbf{w}_i^T \tilde{\mathbf{x}}_t = \max\left(\mathbf{w}_i^T \tilde{\mathbf{X}}_{\Gamma_{i-1}}\right), t \in \Gamma_{i-1}\right\} \ \textit{if}\ \max\left(\mathbf{w}_1^T \tilde{\mathbf{X}}\right) > 0 \\ \left\{t \mid \mathbf{w}_i^T \tilde{\mathbf{x}}_t = \min\left(\mathbf{w}_i^T \tilde{\mathbf{X}}_{\Gamma_{i-1}}\right), t \in \Gamma_{i-1}\right\} \ \textit{if}\ \max\left(\mathbf{w}_1^T \tilde{\mathbf{X}}\right) \le 0 \end{cases}$

Step 4: Estimate the other columns of $\mathbf{A}$ in the following way:

for $r = 1,2,\ldots,n-1$;

update $\hat{\mathbf{A}}_r$ by $\hat{\mathbf{A}}_r = \left[\hat{\mathbf{a}}_1,\ldots,\hat{\mathbf{a}}_r\right]$

update $\hat{\mathbf{A}}_r^{\perp}$ by $\hat{\mathbf{A}}_r^{\perp} = \left(\mathbf{I} - \hat{\mathbf{A}}_r\left(\hat{\mathbf{A}}_r^T \hat{\mathbf{A}}_r\right)^{-1} \hat{\mathbf{A}}_r^T\right)\mathbf{H}$

update $\mathbf{W}$ by $\begin{cases} \mathbf{W}(1:n, 1:n-r) = \hat{\mathbf{A}}_r^{\perp} \\ \mathbf{W}(1:n, n-r+1:n) = \hat{\mathbf{A}}_r \end{cases}$

estimate $\hat{\mathbf{a}}_{r+1}$ by (7) [or (9)] using the meshod in Step 3;

end for

Step 5: Let $\hat{\mathbf{A}}_n = \left[\hat{\mathbf{a}}_1,\ldots,\hat{\mathbf{a}}_n\right]$, and estimate the source matrix by $\hat{\mathbf{S}} = \hat{\mathbf{A}}_n^{-1}\mathbf{X}$.

III. Proposed Image Cryptosystem

3.1 Preprocessing and Encryption

First of all, the original image signal is divided into N frames by using the segment splitter in [7], and each frame is put into P segments with the same length T. Then, each segment is normalized to be in [0, 1], and the corresponding waveform information is stored in a definite format. Finally, the parameters N, P, T and this information are inserted into the head data of the encrypted signal in a pre-definite format for transmission.

After preprocessing, the signals (called plaintexts) $s_1, s_2, \ldots, s_n$ are encrypted through the following steps:

Step 1: generate mixing matrix $\mathbf{A}$ randomly with distribution in [-1, 1], and construct the linear mixtures: $\mathbf{X} = \mathbf{AS}$, where $\mathbf{S} = [s_1^T, s_2^T, \ldots, s_n^T]^T$;

Step 2: obtain the cipher signal matrix $\mathbf{U}$ using the key generator with secret seed, and construct the following nonlinear mixtures

$$\mathbf{Y} = \exp(\mathbf{X} + \mathbf{U}) + \alpha \log(|\mathbf{U}| + 1) \tag{10}$$

where α is a parameter used for fully masking the plaintexts.

The plaintexts are encrypted frame by frame using the model (10), where the cipher $\mathbf{U}$ can be used repeatedly.

3.3 Decryption and Reconstruction

After receiving the encrypted frames (i.e., ciphertexts $\mathbf{Y}$) from public network, one can obtain the following mixtures, combing with the regenerated ciphers and the transmitted parameter:

$$\mathbf{X} = \log(\mathbf{Y} - \alpha \log(|\mathbf{U}| + 1)) - \mathbf{U} \tag{11}$$

Note that $\mathbf{X}$ is calculated analytically. Thus, it is a copy of the sources $\mathbf{S}$ mixed by the matrix $\mathbf{A}$. Then, we can invoke the PP based method shown in Section II to decrypt the plaintexts from $\mathbf{Y}$. However, just like other BSS based decryption methods, the output is the matrix composed of several segments with ambiguities of permutation and scale. To solve the permutation problem,a simple method based on the number of zero-crossings (nzc) is used in [7]. However, the index nzc is often unstable. Here, we utilize the sparsity degree index to sort the sources and the recoveries [10][11].

3.4 Requirements of the Ciphers and the Mixing Matrix

The ciphers can be generated randomly by computer. Unlike the ICA or the sub-band ICA based method, there is no special requirement for the ciphers in the proposed image cryptosystem. Usually, the cipher matrix has the same size with the plaintext matrix, and the values are nonnegative for better masking the latter. As for the mixing matrix, it needs to be neither nonnegative nor sparse. The only requirement is that it should be full rank, and it is quite easy to satisfy this condition by normal computer software.

IV. Simulations

In this section, two simulations are given to verify the performance of the proposed cryptosystem, and the results are compared with other BSS based encryption method, where the compared algorithms are ICA used in [7], WPSDICA [12] and TF [13]. Eachmethod is implemented using MATLAB R2009a installed ina personal computer with Intel(R) Celeron(R) 2.4 GHz CPU,2 GB memory and Microsoft Windows 7 operational system.The elapsed CPU time is used to measure the computingspeed. The source separation performance is measured bythe mean of the sum square error (M-SSE) index defined as [14]

$$e(\mathbf{S}, \hat{\mathbf{S}}) = \frac{1}{n} \min_{\pi \in \Pi_n} \sum_{i=1}^{n} \left\| \mathbf{s}^i - \hat{\mathbf{s}}^{\pi_i} \right\|^2 \tag{12}$$

where $\mathbf{s}^i$ is the i th row of the source matrix $\mathbf{S}$, $\hat{\mathbf{s}}^i$ is the i th row of the estimated source matrix $\hat{\mathbf{S}}$, $\pi = (\pi_1, \ldots, \pi_n)^T$, and $\Pi_n = \left\{ \boldsymbol{\pi} \in \Re^{n\times 1} \mid \pi_i \in \{1,2,\ldots,n\}, \pi_i \neq \pi_j, \forall i \neq j \right\}$ is the set of all permutations of $\{1,2,\ldots,n\}$. Here, the L2-norms of $\mathbf{s}^i$ and $\hat{\mathbf{s}}^i, \forall i$ are normalized to be 1.The optimization in (12) aims to find the best match between the original sources and the estimated sources, which can be solved by the algorithm in [15].

4.1 Simulation 1

In this simulation, four parts of the widely used Lena face image (see Fig. 1(a)) are used as the sources (or plaintexts) to test the proposed image cryptosystem, in which the parameters are set as $N = 1, P = 4, T = 128.$ The model (10) is used for encryption, where the key signal matrix $\mathbf{U}$ is generated randomly by Matlab software, and $\alpha = 2$. Fig. 1(b) and (c) show the ciphers and the encrypted signals, respectively. Table I gives the M-SSE and the computation time (t) indices of the compared methods. One can see that our method has the highest precision and the least time cost. The corresponding decrypted images are given in Fig. 1(d)-(g), respectively. From the visual comparison, our method is superior to other methods.

Table I Indices of M-SSE and t (s) of the compared methods for face images

	PP	ICA	WPSDICA	TF
M-SSE	0.0000	0.3472	0.8743	3.1392
t	0.2496	0.3276	4.9920	1.0920

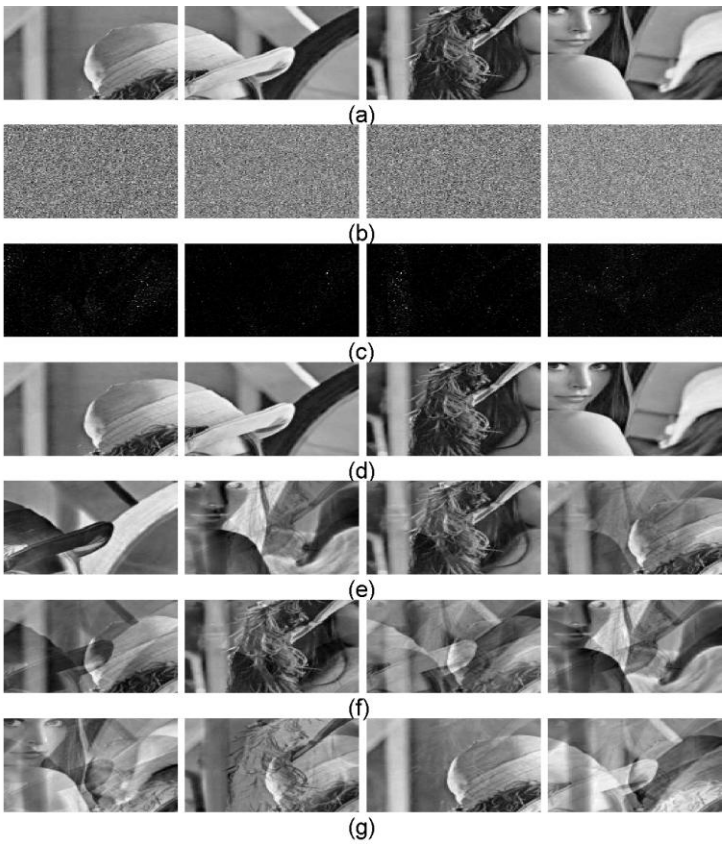

Fig. 1 Sources, ciphers, ciphertexts, and the decryptions using different methods for face images; (a) Sources; (b) Ciphers; (c) Ciphertexts; (d) Decryptions using PP; (e) Decryptions using ICA; (f) Decryptions using WPSDICA; (g) Decryptions using TF.

4.2 Simulation 2

In this simulation, an architectural design drawing is used to test the proposed image cryptosystem. It is split into four segments or sources. Similar to simulation 1, the key signal matrix $\mathbf{U}$ is generated randomly, and the involved parameters are $N=1, P=4, T=128$, $\alpha=2$. Table II gives the M-SSE and the time t indices of the compared methods. And the sources, ciphers, encryptions and decryptions are show in Fig. 2(a)-(g), respectively. Compared with Fig. 2(a) and Fig. 2(d), one can see that our method decrypts the sources perfectly which is consistent to the results in Table II.

Table II Indices of M-SSE and t (s) of the compared methods for drawing images

	PP	ICA	WPSDICA	TF
M-SSE	0.0000	2.0913	1.8603	0.7422
t	0.2808	0.2964	3.8688	0.6396

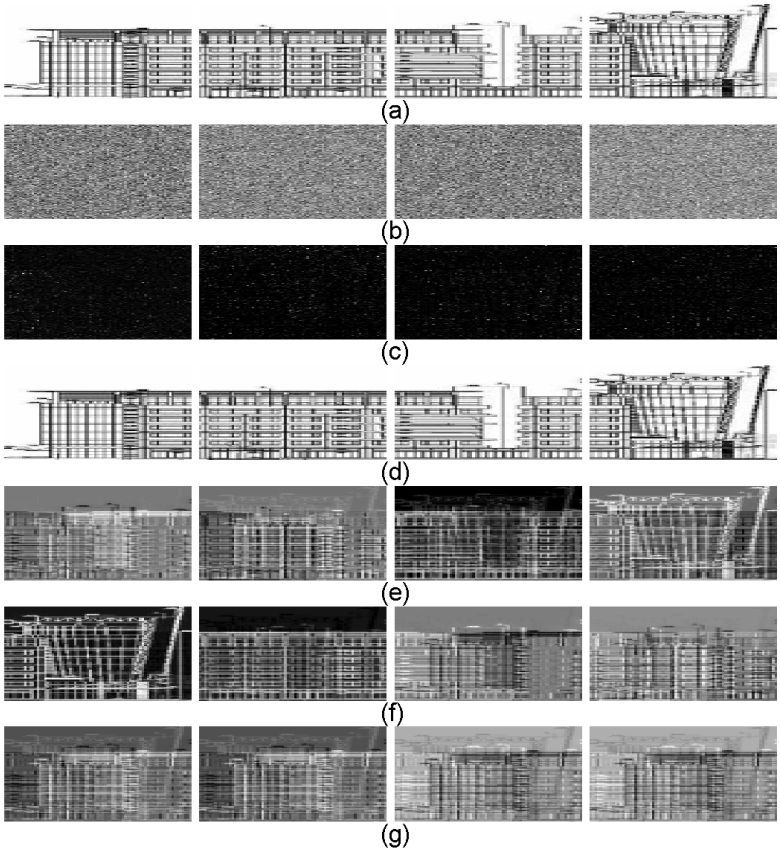

Fig. 2 Sources, ciphers, ciphertexts, and the decryptions using different methods for drawing images; (a) Sources; (b) Ciphers; (c) Ciphertexts; (d) Decryptions using PP; (e) Decryptions using ICA; (f) Decryptions using WPSDICA; (g) Decryptions using TF.

V. Conclusions

In this paper, a new image cryptosystem is proposed, where a complex nonlinear system is used for encryption and a PP based BSS method is used for decryption. The structure of the cryptosystem is introduced in detail, including the encryption and the decryption processes.

Finally, simulations of face images and architecturaldesignpaper pictures are given to verify the availability and the advantages of the proposed cryptosystem.

References

[1] MenezesA, OorschotP, and Vanstone S(1996) Handbook of AppliedCryptography. Boca Raton, FL: CRC

[2] Denning DE(1982) Cryptograghy and Data Security. Reading, MA:Addison-Wesley

[3] ChakravarthyKK and SrinivasMB(2003)Speech encoding and encryptionin VLSI,in Proc. Design Automation Conf. ASP-DAC, pp.569–570

[4] Ma FL,Cheng J, and Wang YM(1996) Wavelet transform-based analogspeech scrambling scheme, Electron. Lett., vol. 32, no. 8, pp. 719–721

[5] Li K., SoYC, and Li ZG(2003) Chaotic cryptosystem with high sensitivityto parameter mismatch,IEEE Trans. Circuits Syst. I, Fundam.Theory Appl., vol. 50, no. 4, pp. 579–583, Apr.

[6] Xie S, Yang Z, and Fu Y(2008)Nonnegative matrix factorization applied to nonlinear speech and image cryptosystems,IEEE Transaction on Circuits and Systems I, vol. 55, no. 8, pp. 2356-2367

[7] Lin QH, Yin FL, Mei TM, and Liang HL(2006) A blind sourceseparation-based method for speech encryption,IEEE Trans. CircuitsSyst. I, Reg. Papers, vol. 53, no. 6, pp. 1320–1328

[8] Yang Z, Xiang Y, RongY, XieS(2013) Projection-pursuit-based method for blind separation of nonnegative sources, IEEE Transactions on Neural Networks and Learning Systems, vol. 24, no. 1, pp.47-57

[9]YangZ, Zhou G, XieS, et al(2011)Blind spectral unmixing based on sparse nonnegative matrix factorization, IEEE Transactions on Image Processing, vol. 20, no. 4, pp. 1112-1125

[10] HoyerPO(2004) Non-negative matrix factorization with sparseness constraints,J. Mach. Learn. Res., vol. 5, no. 1, pp. 1457–469

[11] YangZ, XiangY, XieS, and DingS(2012) Nonnegative blind source separation by sparse component analysis based on determinant measure,IEEE Transactions on Neural Networks and Learning Systems, vol. 23, no. 10, pp. 1601-1610

[12] KoprivaIand Serši´cD(2008) Wavelet packets approach to blind separationof statistically dependent sources,Neurocomputing, vol. 71, nos. 7–9,pp. 1642–1655

[13] RejuVG, KohSN, and SoonIY(2009) An algorithm for mixing matrixestimation in instantaneous blind source separation,Signal Process.,vol. 89, no. 3, pp. 1762–1773

[14] ChanTH, MaWK, ChiCY, and WangY(2008) A convex analysisframework for blind separation of non-negative sources, IEEE Trans.Signal Processing, vol. 56, no. 10, pp. 5120-5134

[15] Tichavsk ýP and Koldovsk ýZ(2004) Optimal pairing of signal componentsseparated by blind techniques,IEEE Signal Processing Letters, vol. 11,no. 2, pp. 119-122