7-4

MVA2007 IAPR Conference on Machine Vision Applications, May 16-18, 2007, Tokyo, JAPAN

NEW IMAGE ENCRYPTION METHOD BASED ON ICA

A. Alfalou, IEEE Senior Member

Laboratoire Brest ISEN **L@bISEN**
29228 Brest Cedex, FRANCE
ayman.al-falou@isen.fr
www.isen.fr

A.Mansour, IEEE Senior Member

E3I2, ENSIETA
29806 Brest, FRANCE.
mansour@ieee.org.
ali.mansour.free.fr

ABSTRACT

In the last decade, Independent component analysis (ICA) becomes one of the most important signal processing tools. Many algorithms have been proposed to separate successfully monodimensional signals from their observed mixed signals. Recently, ICA has been applied to face recognition problem. In this manuscript, a new idea for image encryption and decryption schemes, based on ICA, is proposed. Using some mixing procedure as an encryption method, one can hide useful information transmitted over wireless channels. The main idea of our approach is to secure the transmitted information at two levels: classical level using standard keys and second level (spatial diversity) using independent transmitters. In the second level, a hacker should intercept not one channel but all of them in order to retrieve the information. At designed receiver, one can easily apply ICA algorithms to decrypt the received signals and retrieve the information.

Keywords: Decorrelation, Second order Statistics, Whiteness, Blind separation of sources, Image Encryption / Decryption.

1. INTRODUCTION

Nowadays, advanced wireless communication systems have been widely used in different fields such as internet connections (WIFI), mobil phone, some security systems, *etc*. Transmitted signals can be generally intercepted by non authorized persons. For that reason, it becomes highly recommended to transmit encrypted data.

To reduce needed time to carry out this encrytion operation, methods using optical images processors have been recently developed thanks to commercial availability of Spatial Light Modulators (SLM). Indeed, image processing techniques in coherent optics based on filtering, can be used to carry out image recognition [1]. Similar techniques can also be used to encrypt a two-dimensional information [2]. The authors of [2] propose an encryption method based on optical filtering which is particularly interesting to deal with huge images. Its main idea consists of multiplying the image spectrum with one or more defined masks. This results can be considered as a modification of the spectral distribution in order encrypt images.

Using Independent Component Analysis (ICA), we propose, here, new image encryption and decryption schemes. In fact, ICA has been used to solve Blind Source Separation (BSS) problem [3,4,5]. Actually, BSS has been found in many applications [3] such as: Wireless communication systems (Mobile phone, Spatial Division Multiple Access, free hand phone), speech enhancement. Recently, BSS has been introduced in face recognition problems [6,7].

To our knowledge, image encryption algorithms content special techniques based on keys to hide information, see fig. 1. By known these keys, one can easily decode the secure information. To enforce this level, we are suggesting one use spatial diversity to increase the security level of our transmitted data, see fig. 2. Figure 2 shows the scheme of our ecryption/decription system. In previous papers [1,2], we proposed algorithms using classical technic. Eventhough, the new structure are using two secure levels, we only emphasis, here, the second level (ICA level). We should mention here that the ICA level can be used alone to reach a normal security transmission.

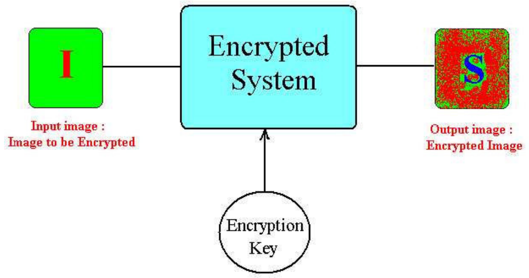

Fig. 1. A classical Encryptio/Decryption Scheme.

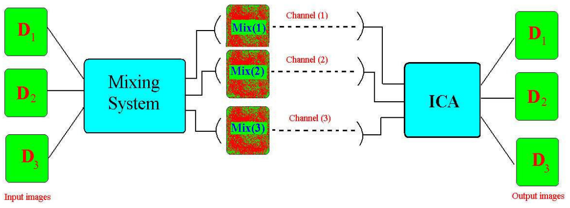

Fig. 2. A new Encryptio/Decryption Scheme: The inputs D_i can be encrypted images S_i (high security level: since two encryption techniques have been considered) or images of interest I_i (normal security level).

In this manuscript, ICA along with some mixing techniques are used to enforce data encryption using spatial or temporal diversity. In fact, our idea consists on sending the mixed encrypted data using divers sequences. These sequences can send in two different ways:

- Spatial diversity: using different independent transmitters.
- Temporal diversity: over the same channel, the sequences are transmitted in different orders, i.e. in similar way to ”interlaced” algorithms used in digital communication. One should mention here, that the sequence levels can be considered as new encryption keys.

Using the new encryption scheme and in order to retrieve transmitted information, a hacker should, at same time, know the keys and successfully intercept our different independent transmitted sequences.

The authors would like to thank Bougusz for his contributions to simulations.

2. MODEL & APPROACH

In blind separation of sources (BSS) problem, one should retrieve p unknown mixed signals (sources) by only using q observed mixing signals [3,4]. The sources are assumed to be statistically independent from each other [8]. Let $S(n) = (s_i(n))$ denotes the source vector and $X(n) = (x_i(n))$ be the mixing (observed) signals. The relationship between $S(n)$ and $X(n)$ can be written as following:

$$X(n) = A\left(S(n), \cdots, S(n-L)\right) \tag{1}$$

where A represents the channel effect and it can be any functionial. It is well known that the last equation, in general case (without any assumption about A or $S(n)$), represents a generic problem that can not be solved. In the case of static memoryless channel, equation (1) can be simplified as following:

$$X(n) = AS(n) \tag{2}$$

In this case, A becomes a real or a complex scalar matrix. This channel is called an instantaneous mixture model. It is well known that the separation of model (2) can be done using ICA techniques based on the independence assumption of sources [8]. We should mention here that the separation can be achieved up to a permutation and a scale factor.

The key point to our application consists on the fact that the separation can be done without knowledge on sources or channel parameters. In the literature, one can find many algorithms to conduct the separation [3]. These algorithms, generally, use different approaches: The minimization of a cost function based on High Order Statistics (HOS) [9,10], the maximization of mutual information [11], using geometrical concepts [12], *etc.*

Most of ICA algorithms deal with the separation of mon-dimensional signals (i.e speech, telecommunication signals, $\cdots$). However, in our application, the sources consists of images. In order to apply ICA algorithms in our application, preprocessing and post-processing steps are required.

2.1. Preprocessing & Post-Processing

Our images which can be considered matrices of pixels, should firstly transformed to vectors. The last transformation can be done using Vec operator[1] as a preprocessing step at the transmitter. To inverse this transformation, one should use Mat[2] operator as a post-processing step at the receiver.

Most of ICA algorithms consider the signals as zeros mean-signals. This statement can not be justified in our application. However, one can easily make our transformed images by Vec as zero mean vector by using a simple mean estimator $V_c = Vec(image1) - E\{Vec(image1)\}$. Once the separation of the received transformed images is done, one should add constant values to our images to get positive values of our pixels.

Some ICA algorithms, such as FASTICA [13] (see the following subsection), consist of two steps:

- Whitening: Using Principal Component Analysis (PCA) based on second order statistics of observed signals, one can simplify the mixing model by transforming the mixing matrix to a permutation mixing matrix. In fact, it is know that separation matrix A can be decomposed [14] as the product of two matrices $A = WU$, where W is a spatial decorrelation matrix and U is an unitary one. Comon [15] proved that one can estimate W by using a simple Cholesky factorization [14] of the covariance matrix of the observed signals.
- Rotation: In this stage, high order statistics criteria can be used to estimate the residual permutation mixing matrix, i.e. U.

We should mention that at the output of whitening stage the signals are spatially decorrelated. In other words, the correlation matrix of these signals becomes a definite positive diagonal matrix. After whitening process, one can apply FastICA algorithm to separate the received signals (the vectors of our images).

2.2. FastICA

In [13], Hyvarinen and Oja proposed an algorithm called FastICA which stands for "Fast Fixed Point Algorithm for Independent Component Analysis". Their algorithm uses the fact that the kurtosis[3] of a Gaussian signal [16,17] is zero. On the other hand, it is well known that mixing signals generates close to Gaussian signals, as the application of central limit theorem.

FastICA can be considered as a deflation approach since the algorithm try to separate the mixing by extracting one signal after another. In their approach, Hyvarinen and Oja suggest the maximization of a contrast function based on a simplified version of the kyrtosis. The maximization is done with respect to a norm constraint according to a vector b. The maximization is done using a Lagrangian method. Finally the vector b is updated using a gradient algorithm.

3. IMAGE ENCRYPTION METHOD

Data encryption is mainly used for some security reasons. This process consists in making illegally intercepted data as useless as possible. In other words, information will be hidden and lost in any intercepted data without the authorization of the sender. This permission can realized by many ways: already known passwords, a given hardware circuit, known decryption methods or by splitting information or data into many parts which should be sent separately.

By using ICA algorithms, such as FASTICA, we are aiming to reach mainly two goals:

- First of all, we encrypt our principal image by mixing up N images. Then several mixed images should be transmitted.
- At receiver (destination), the decryption process should be fast and easily implemented. At the same time, the extracted image should be of high quality.

In order to achieve our task of image encryption and decryption using ICA algorithms, pre- and post-processing steps have to be done, see previous section. To clarify the idea, let us consider the case of encrypt one useful image I1 which is 256×256 pixels, as example, we consider the image of LENA figure (3).

In the following, we present a method to generate useless images and to mix these images with our original image I1. From hereinafter, the useless generated image is called auxiliary images. At this level, it seems that we are increasing the dimension of the transmitted images, since we are adding auxiliary images. In real world applications, multi-media data should be transmitted over secure channel. In order to encrypt a video sequence, auxiliary images can be easily generated using images from our video sequence.

3.1. Generation of statistically independent images

It has been mentioned before that the useful image I1 should be mixed up with other images. However, we should pay attention to the choice of auxiliary images which is of great importance mainly to reach the following three goals:

[1] The vec operator creates a column vector from a matrix A by stacking the column vectors of A.

[2] Mat operator is the inverse of Vec operator.

[3] The kurtosis is a normalized fourth order cumulant.

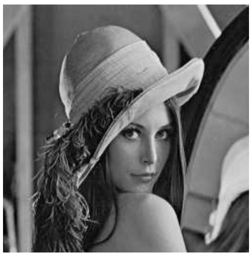

Fig. 3. Information image I1 is a 256×256 pixels grayscale image of "LENA"

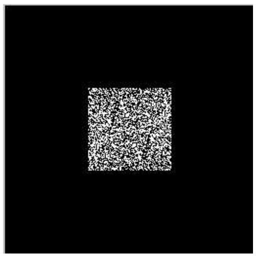

Fig. 4. An image $L2$ obtained as the output of a low-pass filter when its input is an uniformly distributed random image.

- *G1*: Auxiliary images should be statistically independent of each other and independent of image I1. This is the main assumption in any ICA algorithms.
- *G2*: It is well known that the separation of mixed sources can be done if at most one of the sources is a Gaussian signal. In this case, we should select auxiliary images such that their vector is as far as possible from Gaussian signals.
- *G3*: The auxiliary images should be chosen such that the original image I1 is completely hidden and it can not be recognized from any obtained mixed image.

Our experimental study show that a first auxiliary image $A1$, of 256×256 pixels, can be easily generate by considering all the pixels as uniformly distributed random variables. It is clear that image $A1$ satisfies the first two reasons $G1$ and $G2$. To reach $G3$, one should well select the variance of the pixels and the parameters the mixing matrix A, see next subsection.
To generate another auxiliary image $A2$, we firstly create an image $L0$ similar to the first auxiliary image $A1$. Then another image $L2$ has been generated by applying a low-pass filter on $L0$, see figure 4. Finally, the second auxiliary image $A2$ is the output of an inverse Fourier transform applied on $L2$.

As it has been already mentioned, that to reach $G3$, one can modify the generation parameters (variance, low-pass filter parameters) of the two auxiliary images. However, this is not the only way since the mixing parameters (i.e. the coefficients of the mixing matrix A) have great influences on the separation performances.

3.2. Mixed images

The instantaneous model, see equation (2), can be applied in our application as following:

$$X(n) = A \begin{pmatrix} Vec(I1) & Vec(A1) & Vec(A2) \end{pmatrix}^T \quad (3)$$

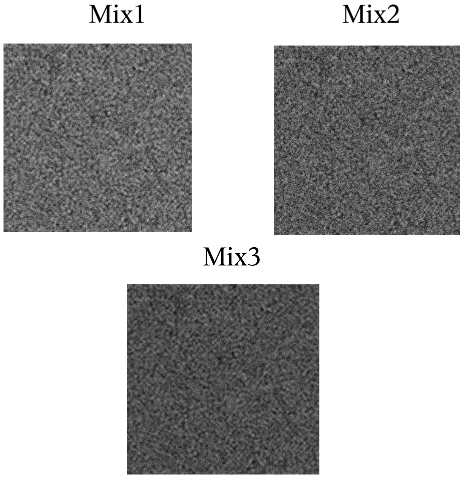

Fig. 5. Three mixed images (encrypted images).

where $A = (a_i)$ is the mixing matrix, V^T is the transpose of V, $Vec(I1)$ is a $(256)^2 \times 1$ colon vector and $X(n)$ is a $3 \times (256)^2$ real matrix who stands for the mixed signals. The coefficients a_i of A should be selected to satisfy two constraints:

- To achieve the separation, matrix A should be an invertible matrix, i.e. $det(A) \neq 0$.
- The values of a_i have great influences on the third encryption goal $G3$.

Figure 5 show us the three mixed images. These images can be transmitted using wireless communications using two different way: one can transmit them at the same time using three different channels or they can be transmitted at different instances using the same channel.

We should mention here that the encryption results are very nice since the LENA image is completely hidden. The encryption technic presented in this section can be generalized to encrypt any number of useful images I_i. In fact, one can consider the other images as auxiliary images. However, we should pay attention that at the decryption stage, at most one of useful image can have Gaussian distribution.

4. DECRYPTION

As it was shown in previous section, the encryption of useful image ("Lena") was successfully done. After the encryption step, it is necessary to manage the decryption, so that the receiver can retrieve the information. In this part, we will present and validate a decryption method that will help us to find back the useful data by treating the 3 mixed images Mix1, Mix2 and Mix3 with an ICA algorithm. By applying FastICA over the mixed signals, one can retrieve the originals signals (i.e. the Vec of our original images), so that we can decrypted Lena. The main point[4] here is that the decryption can be done without any knowledge about the mixing matrix, or original images (auxiliary and useful images). Once the three Vec have been obtained, three Mat operators should applied in order to retrieve the original images. We should mention that the decryption is only possible when the original images are statistically independent.
In order to corroborate our approach, many experimental studies have been conducted. In the following, a standard simulation results are shown. Once we encrypt and obtain the 3 mixed images

[4] This point can be considered as flexibility degree at the transmission stage.

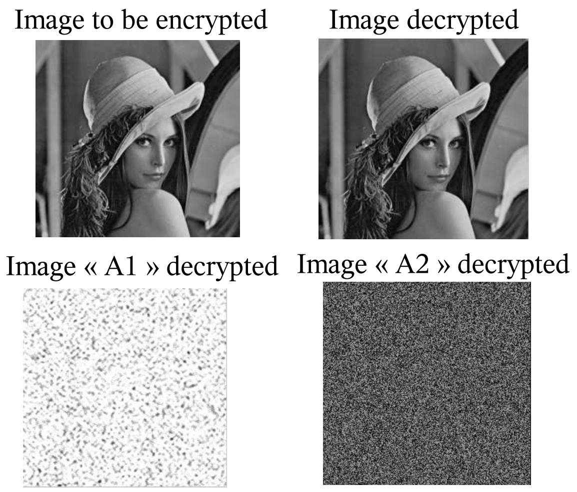

Fig. 6. Input and output images using our Encryption /decryption method

Mix1, Mix2 and Mix3, we apply our method to these mixed images and we obtain images shown on figure (6) as outputs. The last figure shows that the decryption of LENA image is successfully done. As a performance index, we use MSE (Mean square error) which measures the difference between the output image (decrypted image) and the input one. By calling LENA the image to be encrypted ($(N \times N)$ pixels), LENA-EST the estimated image (decrypted ($(N \times N)$ pixels)), the MSE equation is presented on Equ(4.

$$MSE = \frac{1}{N}\sum_{i,j}(|LENA(i,j)| - |LENA - est(i,j)|) \quad (4)$$

By applying the MSE to the mixed images of figure (6), we obtain: $MSE = 0.0692$. The quality of the obtained images and the small obtained value of MSE prove the effectiveness of our approach [18].

5. CONCLUSION

Here, it has been shown that by using ICA algorithm one can obtain an effectiveness image encryption tool. To illustrate this effectiveness, simulation results using three images are presented. Obviously, this approach can be generalized for N images which implies a significant increasing of computational efforts and processing time.

Our method shows that it is now possible to transfer data using a bi-dimensional signal while protecting it from an unspecified user. The useful signal will just have to be mixed with other independent signals. The data is encrypted since it can not be used by whoever doesn't have the authorization from the sender.

For our future works, we are looking to improve the performances of our approach and to minimize the processing time needed in order to consider much more useful images. Color images should be also considered.

Finally, we should mention that we are succeeded to develop a new encryption/compression algorithm using the idea presented here along with other techniques based on special transformations. The new algorithm is beyond the scop of this manuscript and it will presented in future work.

6. BIBLIOGRAPHY

[1] A. A. Al Falou, M. El Bouz and H. Hamam, "Segmented phase on ly filter binarized with a new approach of error diffusion method". Journal of Optics A : Pure and Applied Optics, 7, 2005, pp: 183-191.

[2] R. Elsawda, A. Afalou et al. "Image Encryption and Decryption by Means of an Optical Phase Mask". 2nd IEEE International Conference on Information and Communication Technologies: from Theory to Applications (ICTTA06-IEEE), April 24 - 28, 2006.

[3] A. Mansour, A. Kardec Barros and N. Ohnishi, "Blind Separation of Sources: Methods, Assumptions and Applications". In Special Issue on Digital Signal Processing in IEICE Trans. on Fund. of Elect., Com. and Comp. Sciences. Vol E83-A (8), pages 1498 - 1512 August 2000.

[4] Hyvarinen, A. and Oja, E., "Independent componenet analysis: algorithms and applications", Neural Networks, vol. 13, pp 411-430, 2000.

[5] A. Mansour, and M. Kawamoto, "ICA papers classified according to their applications & performances.", IEICE Trans. on Fund. of Elect., Com. and Comp. Sciences, vol. E86-A (3), pp. 620-633, March, 2003.

[6] A. Cichocki, and S. -I. Amari, "Adaptive blind signal and image processing: Learning algorithms and applications", John Wely & Sons, 2002.

[7] O. Deniz, M. Castrillon, and M. Hernandez, "Face recognition using independent component analysis and support vector machines", Pattern Recognition Letters, pp. 2153-2157, vol. 24, 2003.

[8] P. Comon, "Independent component analysis, a new concept?", Signal Processing, vol. 36 (3), pp. 287-314, April 1994

[9] M. Kendall and A. Stuart, "The advanced theory of statistics: Distribution theory", Charles Griffin & Company Limited, volume 1, 1961.

[10] A. Mansour and N. Ohnishi, "Multichannel blind separation of sources algorithm based on cross-cumulant and the Levenberg-Marquardt method.", IEEE Trans. on Signal Processing, vol. 47 (11), pp. 3172-3175, November 1999.

[11] A. J. Bell and T. J. Sejnowski, "An information-maximization approach to blind separation and blind deconvolution", Neural Computation, vol. 7 (6), pp. 1129-1159, November 1995.

[12] A. Mansour, N. Ohnishi, and C. G. Puntonet,"Blind multiuser separation of instantaneous mixture algorithm based on geometrical concepts", Signal Processing, vol. 82 (8), pp. 1155-1175, 2002.

[13] A. Hyvaerinen and E. Oja, "A fast fixed point algorithm for independent component analysis", Neural computation, vol. 9 , pp. 1483-1492, 1997.

[14] G. H. Golub, and C. F. Van Loan, "Matrix computations", Johns hopkins press- London, 1984.

[15] P. Comon, "Separation of stochastic processes whose a linear mixture is observed", In Workshop on Higher-Order Spectral Analysis, Vail (CO), USA, pp. 174-179, June 1989.

[16] M. Kendall and A. Stuart, "The advanced theory of statistics: Distribution theory", Charles Griffin & Company Limited, 1961.

[17] A. Mansour and C. Jutten, "What should we say about the kurtosis?", IEEE Signal Processing Letters, vol. 6 (12), pp. 321-322, December 1999.

[18] Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing". By Prentice Hall, Second Edition,ISBN : 0-13-094650, 2002