All-Optical video-image encryption enforced security level using ICA

Ayman Alfalou, Ali Mansour

All-Optical video-image encryption with enforced security level using ICA

A. Alfalou†, A. Mansour‡

†Laboratoire Brest ISEN L@bISEN
29228 Brest Cedex, FRANCE
ayman.al-falou@isen.fr
www.isen.fr
‡E3I2, ENSIETA
29806 Brest Cedex09, FRANCE
mansour@ieee.org
ali.mansour.free.fr
†The author is an associate member of Département d'Électromagntisme appliqué et Télecoms (EMAT)
Université de Moncton 165
N.-B. Canada E1A 3E9

Abstract. In the last two decades, wireless communications have been introduced in various applications. However, the transmitted data can be, at any moment, intercepted by non-authorized people. That could explain why data encryption and secure transmission have gained enormous popularity. In order to secure data transmission, we should pay attention to two aspects: transmission rate and encryption security level.

In this manuscript, we address these two aspects by proposing a new video-image transmission scheme. The new system consists in using the advantage of optical high transmission rate and some powerful signal processing tools to secure the transmitted data.

The main idea of our approach is to secure transmitted information at two levels: at classical level by using an adaptation of standard optical technique and at second level (spatial diversity) by using independent transmitters. In the second level, a hacker should intercept not only one channel but all of them in order to retrieve information. At the receiver, we can easily apply ICA algorithms to decrypt the received signals and retrieve information.

Keywords: Multiple-image encryption, Optical Image Encryption / Decryption, ICA, Fourier transform, Blind Source Separation, Decorrelation, Second and Higher Order Statistics, Signal and Image Processing, Transmission, Whiteness.

1. Introduction

Any commercial, military or civil communication system should have at least a minimum security level, which depends on application, and an acceptable transmission rate.

To increase the confidence in the authenticity of communicating entities and ensure the confidentiality of exchanged information, advanced security tools have been proposed in the literature. Many of them use time consuming algorithms.

To reduce the amount of time required to carry out this encryption operation, methods using optical image processors have been recently developed thanks to commercial availability of Spatial Light Modulators (SLM). Indeed, image processing techniques with coherent optics based on filtering, can be used to perform image recognition [1][2]. Similar techniques can also be used to encrypt a two-dimensional information structure [3][4], figure (1). The authors of [3][4] proposed an encryption method based on optical filtering which is mainly interesting for two reasons:

(i) At first, the source image has an optical form, therefore an optical encryption of this image can simplify the encryption process by avoiding all digital conversion operations.

(ii) That algorithm allows us to deal with huge images using the potential of coherent optic parallelism.

The main idea of their approach consists in multiplying the target image spectrum with one or more masks. This modification of the spectral distribution is in fact the way of encrypting the image.

Image processing tools as well as spectral algorithms (based on spectral filtering) have also been used to encrypt images. In [5] [6], the authors propose a method using a random phase. A multiplication of the image spectrum by a pseudo-random phase is applied. Fractional Fourier transform was the key element in other optical encryption algorithms [7][8]. In such circumstances, hacking is easily performed by finding out this parameter. Figure 1 shows a generic encryption scheme with an optical system.

- New secure transmission system:

Today it is widely admitted by the scientific community that an encryption system should use keys to transform data and hide information. In a previous study [4], we proposed a new optical system based on spectral information clustering. The technique uses a new segmentation approach developed in another work [9][10]. This segmentation process has been used to generate a filter (i.e. a segmented filter) to improve the performance of optical correlator in terms of discrimination level [9] and to carry out an optical compression system [10]. By using the concept of segmented filter, the encryption process can be considered as an image encrypting with segmented phase masks playing the role of keys in conventional encryption techniques. In our case, these keys contain information gathered from different sub-keys according to a well-defined criterion. For decryption the correct segmented phase masks should be known. It is worth mentioning that the encryption keys are often generated by complex images. This

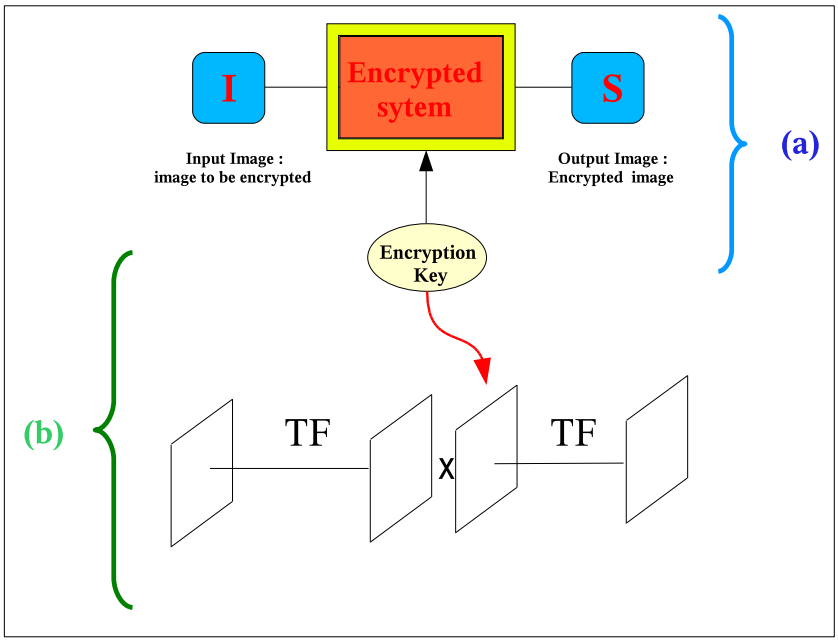

Figure 1. Encryption Scheme: (a) synoptic diagram (b) optical set-up of an encryption system based on segment key

means that they cannot be randomly generated in a reasonable time.

We note that by knowing the encryption keys, intercepted data can be easily decrypted and a non-authorized people can easily decode information. To increase the security of our transmission system, we propose a new secure transmission system which uses spatial diversity along with classical encryption scheme, as depicted in figure 2.

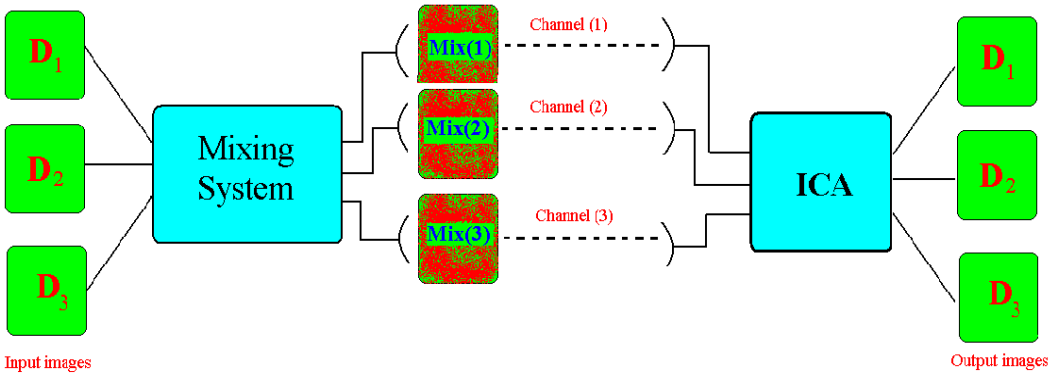

Figure 2. Transmission Encryption/Decryption Scheme: An input D_i can be an encrypted image (high security level: since two encryption techniques have been considered) or any image of interest I_i (normal security level: one encryption technique have been considered).

To decode the received signal, one should have at the same time all the required keys and receive all the transmitted information (i.e. a hacker should intercept at the same time not only one transmitted signal but many of them). The spatial diversity of our system 'ICA-EncryDe' is carried out using Independent Component Analysis (ICA) techniques. By adding ICA and spatial diversity to our transmitter and receiver systems, the image quality will not be affected [11].

Independent Component Analysis is a powerful tool recently introduced into the signal processing field in order to solve the Blind Source Separation (BSS) problem [12][13]. In fact, it can be applied in different situations and has many applications [13] such as wireless communication systems (mobile phone, Spatial Division Multiple Access, free hand phone), speech enhancement as well as face recognition problems [14][15]. The blind separation of sources problem (BSS) has been a topic of interest in signal processing since 1984 [16]. In the past decade, BSS has been studied by several research teams, and many algorithms have been proposed [17]. The BSS involves retrieving unknown sources (signals or images) by only observing a mixture of them [18, 19] (see Fig. 2). In general, authors assume that the sources are non-Gaussian signals (at most, one of the sources can be a Gaussian signal) and statistically independent of one another. Therefore, concepts of independent component analysis (ICA) [20] have been widely used and developed to solve the BSS.

While, the new structure contains two secure levels, only the second level (ICA level) is emphasized in this manuscript‡. In addition, ICA level can be used alone to reach a normal security transmission.

2. Optical image encryption system

Here, an optical encryption system is given. We introduced this system in an earlier study [4, 21].

2.1. Encryption system

Figure (3) shows an optical set-up and a synoptic diagram of the optical encryption system that we proposed in a previous study. According to our system, an image can be easily encrypted by performing its Fourier transform using a convergent lens ($L1$). The obtained image spectrum should be multiplied by a special encryption key. This key consists of many sub-keys. To produce the special key from sub-keys, we should use segmented techniques (developed below section(2.2)).

‡ More details about the first security level (optical encryption system) can be found in our previous studies [21, 4].

The obtained key is called Segmented Encryption Phase Mask "**SEPM**". After multiplying the image spectrum by this "**SEPM** Mask, the phase spectrum distribution of the image is changed which leads to image encryption in spectral domain. Finally, by using a second convergent lens ($L2$), another Fourier transform can be performed in order to obtain the final encrypted image "**D**" in the output plane.

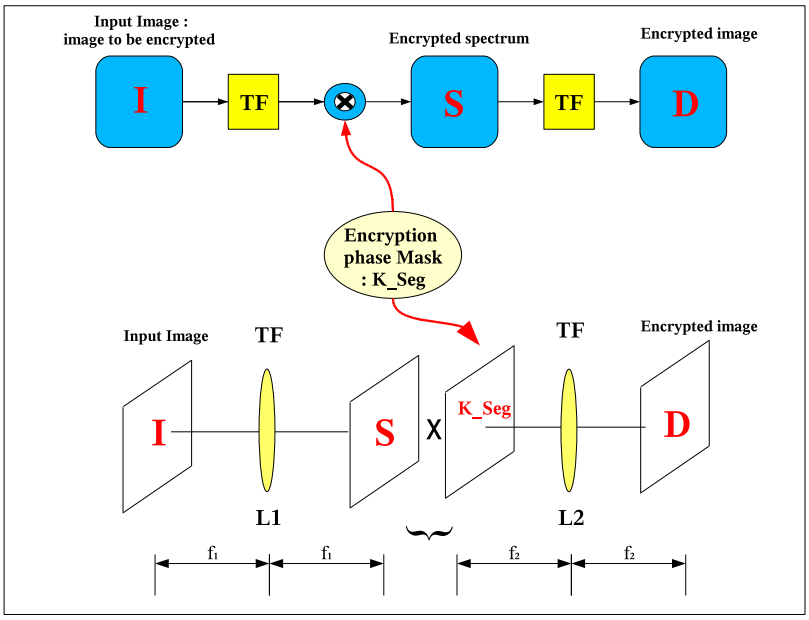

Figure 3. Optical set-up and synoptic diagram of optical encryption system using a segmented key

2.2. Segmented Encryption Phase Mask manufacturing

Using an adapted segmentation method§ and several encryption sub-keys, segmented encryption phase mask can be carried out, as depicted in figure 4. In fact, the segmentation gathers information from each encryption sub-key in the Fourier plane in order to obtain one specific mask called segmented encryption phase mask, SPEM, [3, 4, 21]. Moreover, this segmented method cancels the local saturation phenomena in the Fourier plane, by segmenting the Fourier plane in several domains and by assigning each of these domains to only one winner class (spectrum sub-key). Optimal segmentation can also be obtained using the minimization of phase energy functions, see figure 4. In this case, the energy ratio is given as the ratio between the real part of any sub-key spectrum pixel and the total energy. This energy ratio of each sub-key should be compared to the ratio of other sub-keys in order to select a winner class.

§ This method was initially proposed to make a segmented correlation filter [1, 9].

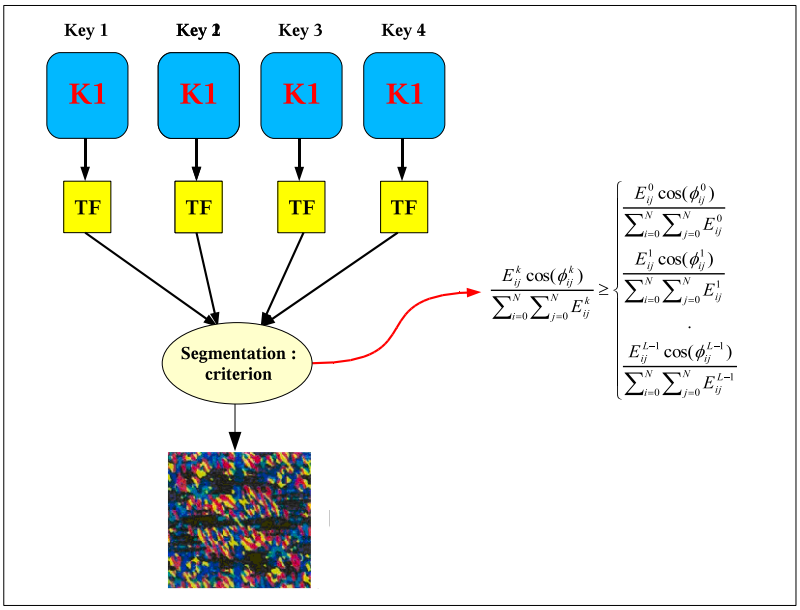

Figure 4. Synoptic diagram of a segmented encryption phase mask

Figure (4) presents an example of segmented encryption phase mask with a base made up of 4 encryption keys.

2.3. Decryption system

Image decryption can be conducted by a correlator using an adapted Segmented Composite Phase Only Filter (SCPOF) [1]. The goal of using this correlator is to recognize the Encryption Phase Mask introduced in the encryption process. To reach this purpose, SCPOF must be constructed using the same sub-keys of the Encryption Phase Mask. The choice of "SCPOF" filter is justified by its very selective nature [1]. In other words, that enables us to complete perfectly the decryption process by eliminating all effects of encryption.

3. Encryption enforced security level using ICA

In the previous section, an optical encryption system is presented. Here, we propose a new architecture based on ICA techniques to enforce security levels of the previously proposed system. We should mention that the modification carried out using ICA can improve the overall system performance [11]. In fact, we will show later that the security level will be improved, without seriously affecting the image quality and the transmission rate.

To explain our idea, let us consider the following application: In automatic face recognition system (for example, in a bank or an airport security system), we often have to transmit simultaneously some images to a central server for data base in order to be identified. Obviously, the image transmission must be done over a secure transmission channel and at a relatively high transmission rate. Let us consider that we have three images I_i, $i \in \{1, 2, 3\}$, $(N \times N)$ pixels each one, from a video sequence see figure 5. At first, selected images should be processed using a classical optical encryption algorithm (this procedure can allow compression processing), see figure 5-b. The obtained images 5-c (encrypted images D_i, $i \in \{1, 2, 3\}$) are mixed using a mixture procedure which is explained later. Thus, we obtained a mixed version (5-e) of our encrypted images (5-c).

The final encryption stage consists in transforming the images I_i ($N \times N$ pixels each one and $i = 3$) previously encrypted and mixed (Mix_i) into one vector ($1 \times 3N^2$). The pixel order (i.e. the coefficients of the vector) should be modified according to an pre-defined interlacement criterion. This step can be considered as adding a supplementary encoding key. We should mention that the interlacement technique is a well known and widely used technique in wireless digital communication protocols [22]. The final interlaced vector should be divided into p (p can or not necessarily equal to i) vectors which are transmitted using the same or different channels.

At this level, final images are coded using three layers. In the first layer, an optical encryption key is used. In the second layer, information are mixed up. In the final layer, after using an interlacement technique, we transmit it using same (but successively) or different (but simultaneously) transmission channel(s). In other words, our idea consists in sending the mixed encrypted data using various sequences. These sequences can be sent 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. We should mention here, that the sequence levels can be considered as new encryption keys.

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

Then, we will discuss different needed steps to mix up images, to apply ICA, to separate the mixed images and all the other details needed to achieve the decryption step.

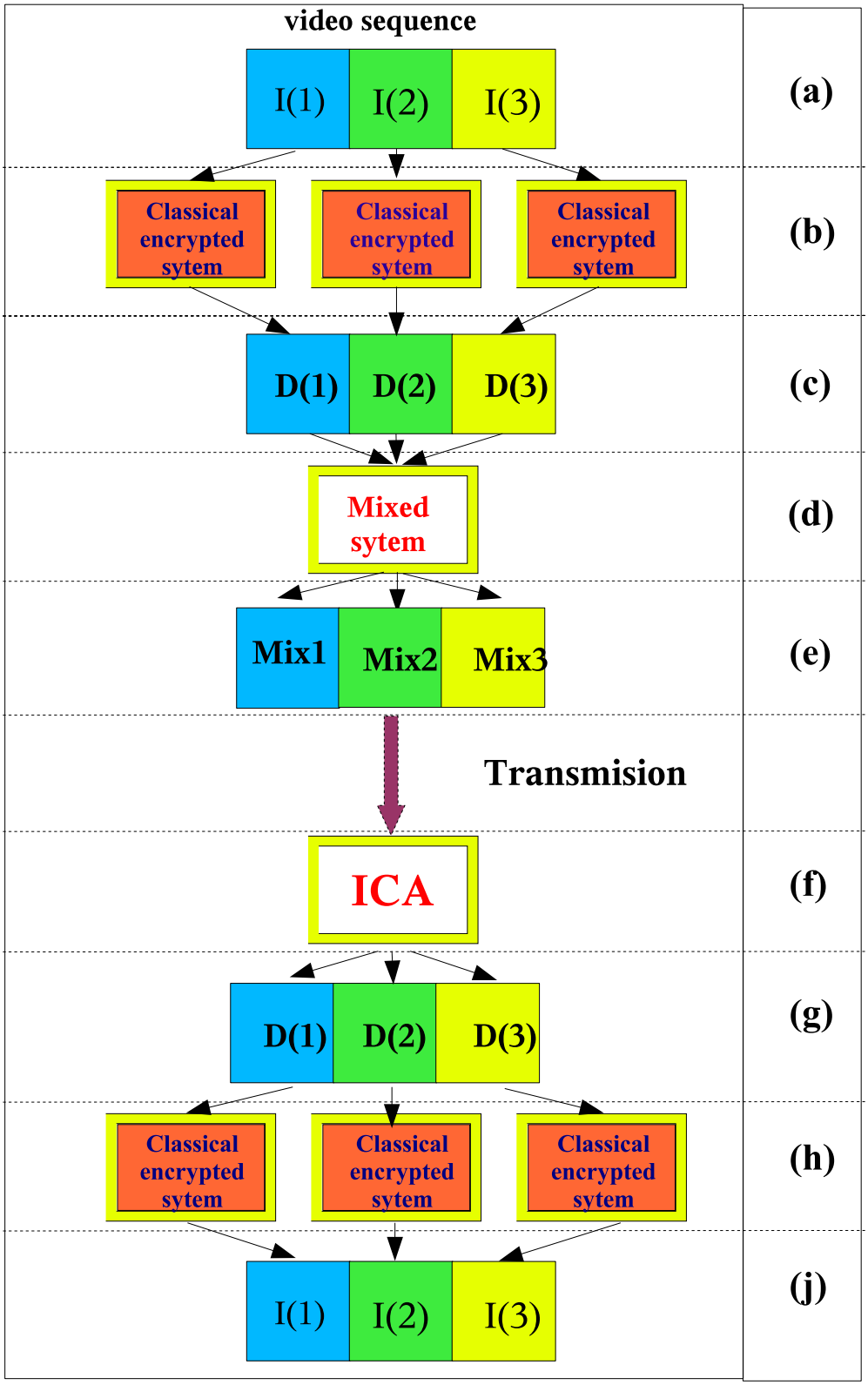

Figure 5. New Encryption-Decryption system using ICA techniques.

4. Model & Approach

As mentioned before, in the blind separation of sources (BSS) problem, we can retrieve "p" unknown mixed signals (sources) by only using "q" observed mixing signals [12, 17, 23]. The sources are assumed to be statistically independent of each other [20].

4.1. Mixing Model

To simplify the discussion and better explain our ideas, we consider firstly that we only have two images to transmit. The generalization to n images is straight forward. Let us consider by $s_1(t)$ and $s_2(t)$ the two images where "t" stands for a given pixel.

In this study, only linear mixture has been considered. In this case the mixed images $x_i(t)$ can be obtained as followed:

$$\begin{aligned} x_1(t) &= a_{11} * s_1(t) + a_{12} * s_2(t) \\ x_2(t) &= a_{21} * s_1(t) + a_{22} * s_2(t) \end{aligned} \tag{1}$$

where a_{ij} are real or complex coefficients used in order to hide better the information. We should mention here that the linear mixing process can be replaced by a non-linear one. For example, we can use a similar approach to the one presented in [5]. In the latest approach, the authors multiply the images by a random mask in order to modify the image spectrum. Actually, we will investigate the latter procedure among other non-linear procedures where the non-linear transformation will be made in Fourier plane. By introducing non-linearity in the mixing step, we can secure better transmitted data, however this procedure will be time consuming during the coding as well as the decoding procedures.

To easily generalize equation (1) to an arbitrary number of images, we can use the following matricial notation:

$$X(t) = A\left(I(t), \cdots, I(t-L)\right) \tag{2}$$

where $I(t) = \begin{pmatrix} s_1(t) \\ \vdots \\ s_n(t) \end{pmatrix}$ stands for the original images (i.e. the source images), $X(t)$ is the mixed images and A represents the channel effect and it can be any functional operator. It is well known that the latest equation, in generally case (without any assumption about A or $I(t)$), represents a generic problem that can not be solved. In the case of static memoryless channel, equation (2) can be simplified as followed:

$$X(n) = AI(n) \tag{3}$$

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 (3) can

be made using ICA techniques based on the independence assumption of sources and can be achieved up to a permutation and a scale factor [20].

4.2. Optical Image Mixer

The mathematical mixing operator presented in the previous subsection, can be completely realized using optical components. In figure 6, we present our optical set-up which allows to encrypt and mix (optically) two images ($I1$ and $I2$):

- At first a laser source is used.
- The obtained laser beam is divided into two laser beams using a beam separator (i.e. a laser polarizing beam-splitter cube).
- Each laser beam will be used to illuminate a specified image ($I1$ and $I2$).
- These two images are optically encrypted by using the method exposed in section (2). Thus, we obtain two encrypted images $D(1)$ and $D(2)$.
- Other beam-splitters cubes should be used again in order to generate copies of each encrypted image. The number of needed copies is equal to the desired number of mixed images.
- Different obtained images should be multiplied by correspondent coefficients. At this stage, we can use opto-electronic components (Spatial Light Modulator (**SLM**)).
- Finally, the mixed images are obtained by a simple addition done using properties of optical holography, on CCD Camera (equations 4,5):

$$CCD1 : X(1) = |a_{11} * D(1) + a_{12} * D(2)| \tag{4}$$
$$CCD2 : X(2) = |a_{21} * D(1) + a_{22} * D(2)| \tag{5}$$

4.3. Demixing Model using an ICA Algaorithm

The key point of our application is that the separation can be made without knowing the sources or the channel parameters. In the literature, we can find many algorithms to conduct the separation [17]. These algorithms generally use different approaches:

- the minimization of a cost function based on High Order Statistics (HOS) [24, 25],

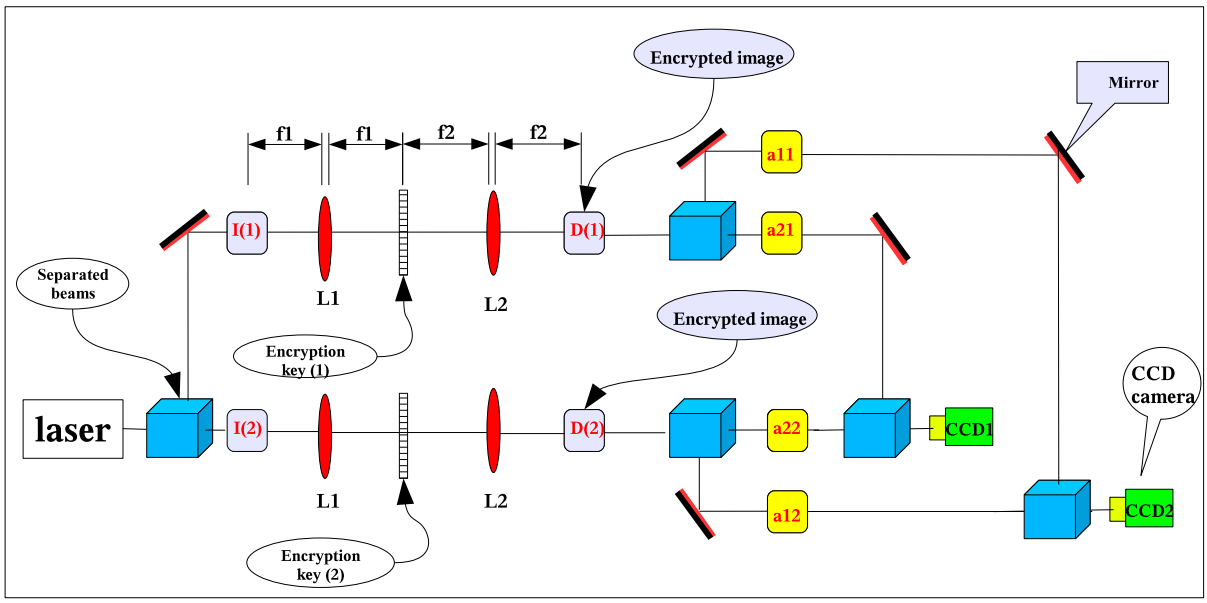

Figure 6. Optical Image Mixer

- the maximization of mutual information [26],
- using geometrical concepts [27], *etc.*.

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

In [28], 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 (i.e. a normalized fourth order cumulant [29]) of a Gaussian signal [24, 30] 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 [31].

Some ICA algorithms, such as FASTICA [28] require two computing stages:

- The first stage is a whitening procedure: Using Principal Component Analysis (PCA) [32] based on second order statistics of observed signals, we can simplify the mixing model by transforming the mixing matrix into a rotation mixing matrix. In fact, it is known that separation matrix A can be decomposed [33] as the product of two matrices $A = WU$, where W is a spatial decorrelation matrix and U is an unitary one. Common [34] proved that we can estimate W by using a simple Cholesky factorization [33] of the covariance matrix of the observed signals.

- Rotation: In this stage, high order statistics [29] criteria can be used to estimate the residual permutation mixing matrix, i.e. U.

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

Finally, FastICA can be considered as a deflation approach since the algorithm tries 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 kurtosis. The maximization is done with respect to a norm constraint according to a vector b using a Lagrangian method. Finally the vector b is updated using a gradient algorithm.

5. Image encryption method with enforced security level

Data encryption is mainly used for 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 be realized in 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 at reaching mainly two goals:

- First of all, we enforce security level of our encrypted image by mixing up "n" optical encrypted images. Then several mixed images should be transmitted using several channels.
- At receiver (destination), the decryption process should be fast and easily implemented. At the same time, the extracted image should be of high quality. This stage consists in demixing the received data using an ICA algorithm. Finally, the decryption should be carried out using the method described in section (2).

In order to achieve our task of image encryption (two levels: optical encryption and mixing) and decryption using ICA algorithms, pre- and post-processing steps have to be taken. To clarify this statement, a video sequence contains at least three images I1, I2, I3 of 256×256 pixels each, is described in figure (7).

5.1. First stage: Optical encryption

The first stage consists in encrypting the previous video sequence using our optical encryption system developed in section (2). Then, only two images ($I1$, $I2$) are encrypted

Figure 7. A sequence of video images contains three 256×256 pixels grayscale images : I1, I2 and I3

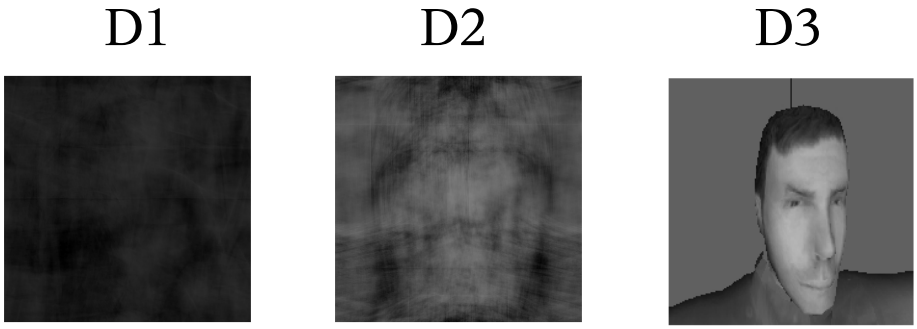

Figure 8. Two images of video sequence encrypted with the classical optical system (section (2))

and we don't consider the third image ($I3$) in order to keep it as an example to corroborate performances of our encryption enforced method. In this case, the first two images are encrypted using two security levels, but the last image is encrypted using only one security level.

The results of optical encryption, using a segmented phase mask carried out with two sub-keys, are shown in figure (8) : D1 and D2. The third image ($D3 \equiv I3$) presented in (8) is without encryption.

5.2. Second stage: Mixed Encryption process

The second stage of our system consists in mixing together different images (i.e. in our example, we should mix $D1, D2$ and $D3$ figure 8). However in order to apply ICA techniques, we should make sure that the mixed images are non-gaussian statistically independent images. From a practical point of view, the images independence can be justified when the images are chosen from different video sequences (or at least, they should be taken at different moments). In the following paragraphs we present a method

to enforce the selection of candidate images. The optically encrypted images D1, D2 and D3 should be modified to $D'1$, $D'2$ and $D'3$. The modified images can be obtained by multiplying encrypted images D_i with non-information images which are called auxiliary images (see section 5.2.1).

5.2.1. Generation of auxiliary images

The choice of auxiliary images is of great importance mainly to reach the following three goals:

- *G1*: Result multiplication between encrypted images (D_i) and auxiliary images should generate statistically independent images D'_i. This is the main assumption in any ICA algorithm.

- *G2*: It is well known that the separation of mixed sources can be make if at most one of the sources is a Gaussian signal. In this case, we should select auxiliary images that are statistically different from Gaussian signals.

- *G3*: The auxiliary images should be chosen so that the encrypted images ($D1$, $D2$ and $D3$) are completely hidden and can not be recognized from any obtained mixed image.

Our experimental study shows that a first auxiliary image $A1$, of 256×256 pixels, can be easily generated by considering all the pixels as randomly distributed variables, see figure 9-$A1$. It is clear that image $A1$ meets the first two goals $G1$ and $G2$. To reach $G3$, one should well select the variance of the pixels and the parameters of the mixing matrix A, see next subsection.

To generate another auxiliary image $A2$, we first create an image $L1$ in a similar way to the first auxiliary image $A1$. Then another image $L2$ has been generated by applying a low-pass filter on $L1$, see figure 10. Finally, the second auxiliary image $A2$ is the output of an inverse Fourier transform applied on $L2$, see figure 9-$A2$.

As already mentioned, to reach $G3$, we 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.

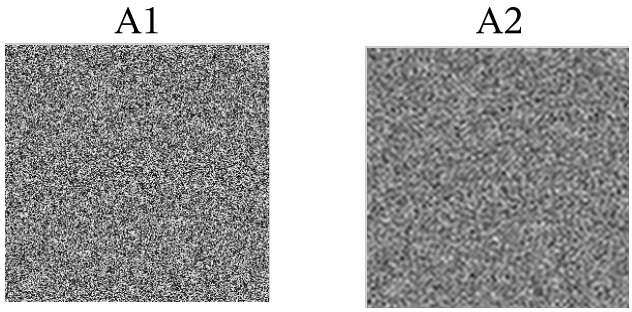

Figure 9. Two auxiliary images $A1$ and $A2$ used to be multiplied with the encrypted images D1, D2.

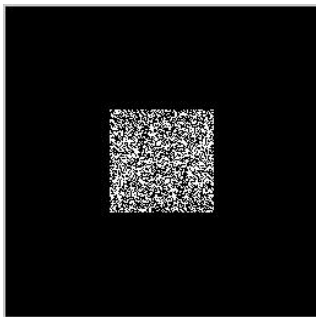

Figure 10. An image $L2$ obtained as the output of a low-pass filter when its input is a uniformly distributed random image.

5.2.2. Enforcing the security by adding Non-Linear Function

after several detailed studies, we have found that some candidate images are close to Gaussian. By applying some nonlinear functions to $D'1$, $D'2$ and $D'3$ as "tangent : **tan**" or "hyperbolic tangent : **tanh**", we can obtain images that are far from Gaussian signals.

In order to enforce the security level and improve the statistical properties of our treated image, we should apply a non-linear function‖ to each coded image. At this stage, the function can be the same for all the images. However, to add more security levels and improve the over-all performance of our algorithm, we considered different functions.

Let us call $D^{'} - i$, the result of multiplication between the optically coded images D_i and the auxiliary ones A_i (see the previous subsection). For the three obtained images, we chose three different functions: $f_1(X) = X^3$, $f_2(X) = tan(X)$ and $f_3(X) = tanh(X)$. Images at the output of the nonlinear functions are called $DI1$, $DI2$ and $DI3$ and

‖ The chosen function should be continues, derivative and invertible function.

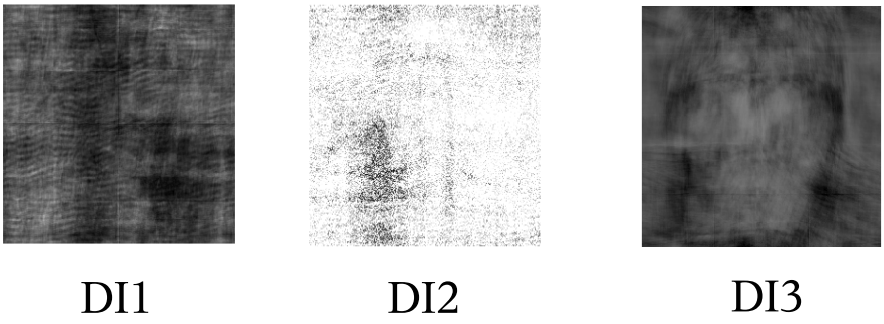

Figure 11. Images at the output of the nonlinear functions.

presented at figure 11.

5.3. Mixed images

The instantaneous model, see equation (3), can be applied in our application as followed:

$$X(n) = A\Big(\ Vec(DI1) \quad Vec(DI2) \quad Vec(DI3)\ \Big)^T \tag{6}$$

where $A = (a_i)$ is the mixing matrix, V^T is the transpose of V, $Vec(DI1)$ is a $(256)^2 \times 1$ colon vector and $X(n)$ is a $3 \times (256)^2$ real matrix which stands for the mixed signals. The coefficients a_i of A should be selected to meet 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 12 shows us the three mixed images. These images can be transmitted using wireless communication using two different ways:

- We can transmit them at the same time using three different channels.
- They can be transmitted at different moments using the same channel.

We should mention here that the encryption results are very satisfying since original images are completely hidden. The encryption techniques presented in this section can be generalized to encrypt any number of useful images I_i. In fact, we 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.

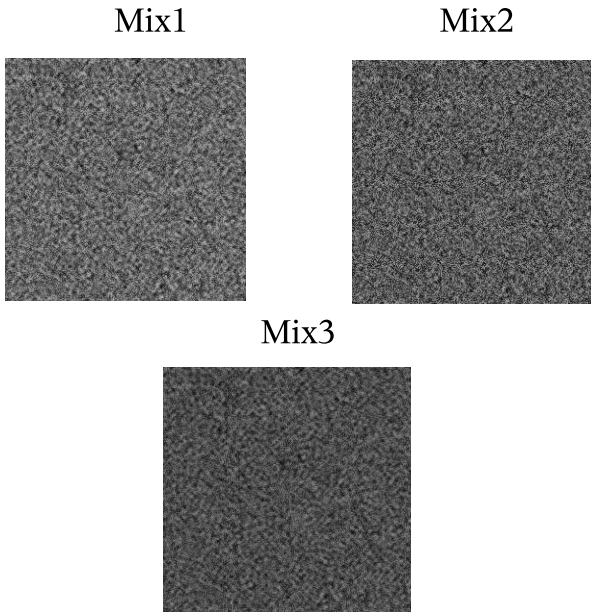

Figure 12. Three mixed images represent three encrypted images with three security levels.

Finally, we should mention that at this stage our images are encrypted using four security levels, see figure(2):

- At first, original images I_i are encrypted using an optical encryption system. The encrypted images are called D_i.
- Multiplying images D_i by auxiliary images A_i and using non-linear functions $f_i(X)$ give us second level encrypted images DI_i.
- A mixing process is used to encrypt again the already encrypted images DI_i. Let's call Mix_i the encrypted mixed images.
- At the final stage, pixels of encrypted mixed images Mix_i, are interlaced¶ and transmitted using different times using the same channel or simultaneously using different channels.

6. Decryption

As it was shown in previous section, the encryption of video sequence was successfully carried out using four security levels. After the encryption step, it is necessary to man-

¶ This technique is widely used in Digital Wireless Communication System.

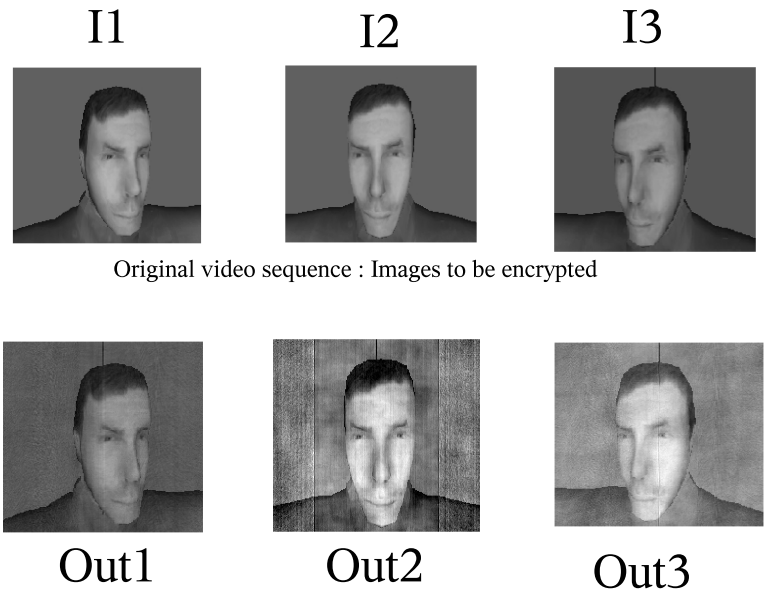

Figure 13. Various output images using classical optical encrypted system enforced using ICA

age the decryption, since the receiver should retrieve the information. The decryption scheme can be summarized as follows:

- At First, we must retrieve mixed encrypted images Mix_i by inverting the interlaced sequences.

- Once, we have obtained the mixed encrypted images Mix_i, the second level encrypted images DI_i can be easily found using an ICA algorithm. In our case, we applied FastICA. Further details concerning this stage can be found in our previous study [11].

- The first stage encrypted images D_i can be easily obtained by inverting the nonlinear function and considering the auxiliary images.

- During the final decryption stage, original images I_i can be obtained from D_i using the system described in section (2) : For that, we start by carrying out separately the Fourier transform of each demixed image (D1, D2 and D3). Then, we multiply their corresponding spectrum by an inverse of the segmented phase mask used in the encryption process. By carrying out a second Fourier transform of each decrypted spectrum, we retrieve the original images Out1, Out2 and Out3 (figure 13).

In order to corroborate our approach, many experimental studies have been conducted. In the following, standard simulation results are shown. Once we have optically encrypted and mixed the original images, we apply our method to these mixed images and we obtain decrypted images shown in figure (13). The last figure shows that the decryption of our video sequence have been successfully carried out.

As a performance index, we use MSE (Mean square error) which measures a difference between the output image (decrypted image) and the input one [35]. By calling I1 the first original image to be encrypted ($(N \times N)$ pixels), Out1 the estimated image (decrypted ($(N \times N)$ pixels)), the MSE equation is defined as followed:

$$MSE = \frac{1}{N^2} \sum_{i,j} (|I1(i,j)| - Out1|(i,j)|^2 \tag{7}$$

By applying the MSE to the decrypted images of figure (13), we obtain MSE values presented in table (1). The quality of obtained images as well as small obtained values of MSE prove the effectiveness of our approach.

	I1-Out1	I2-Out2	I3-Out3
MSE	0.0892	0.137	0.0936

Table 1. Results of the tests (MSE) carried out with our optical video-image encryption with enforced security level using ICA

7. Conclusion

In this manuscript, a new Encryption/Decryption scheme is presented. The main advantages of this scheme compared with classical systems are obtained by using optical instruments and ICA techniques. Concerning the optical part, it is used to increase the rate transmission. On the other hand, ICA are one of the recent and powerful signal processing tools which are introduced in our system in order to increase the security using spatial diversity and multi-transmission channels.

Our simulation studies show 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 someone who doesn't have the authorization from the sender.

For future works, we are going to improve the performance of our approach by adding compression techniques based on JPEG compression algorithms to minimize the processing time as well as the allocated memory. Video Sequence and color images are

under-consideration. Recently obtained results should be corroborated by more studies and simulations. The later study will be presented in future works.

Acknowledgment: The authors are thankful to CRV institute for providing us with needed images.

8. Bibliography

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

[2] A. Al Falou. **La corrélation optique : un outil de décision**. *IEEE-Canada Review*, No. 49, pp: 6-10, Winter 2005.

[3] R. El Sawda, A. Alfalou, G. Keryer and A. Assoum. **Image Encryption and Decryption by Means of an Optical Phase Mask**. Proceeding of IEEE, *2nd IEEE International Conference on Information and Communication Technologies: from Theory to Applications (ICTTA06-IEEE)*, ISBN: 0-7803-9522-0, April 24-28, 2006.

[4] R. EL SAWDA, A. Alfalou, M. Farhat, A. Assoum. **Colored Image Encryption System Based on an Optical Phase Mask**. Proceeding of IEEE, *4th international conference **SETIT 2007**: Sciences of Electronic, Technologies of Information and Telecommunications*, ISBN: 978-9973-61-475-9, March 25-29, 2007.

[5] P. Réfrégier and B. Javidi. **Optical image encryption based on input plane and Fourier plane random encoding**. *Optics. Letters.*, Vol. 20, pp: 767-769, 1995.

[6] F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, **Influence of a perturbation in a double phase-encoding system**. *J. Opt. Soc. Am. A*,Vol. 15, pp: 2629-2638, 1998.

[7] Guohai Situ and Jingjuan Zhang. **Position multiplexing for multiple-image encryption**. *Journal of Optics A: Pure and Applied Optics*, Vol. 8, No 5, pp: 391-397, May 2006.

[8] Zhou Xin, Yuan Sheng, Wang Sheng-wei and Xie Jian. **Affine cryptosystem of double-random-phase encryption based on the fractional Fourier transform**, *Applied Optics*, Vol. 45, Issue 33, pp: 8434-8439, 2006.

[9] A. AL Falou, G. Keryer, J. L. de Bougrenet. **Optical implementation of segmented composite filtering**. *Applied Optics*, N. 38, pp: 6129-6135, 1999.

[10] S. Soualmi, A. Alfalou, H. Hamam. **Optical image compression based on segmentation of the Fourier plane: New approaches and critical analysis**. *Journal of Optics A: Pure and Applied Optics*, Vol. 9, pp: 73-80, 2007.

[11] A. Alfalou, A. Mansour. **New image encryption method based on ICA**. *IAPR Conference on Machine Vision Applications*, Tokyo, Japan, May 16-18, 2007.

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

[13] 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.

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

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

[16] J. Hérault, B. Ans. **Réseaux de neurones à synapses modifiables: Décodage de messages sensoriels composites par un apprentissage non supervisé et permanent**. *C. R. Acad. Sci. Paris*, Vol. série III, pp: 525-528, 1984.

[17] 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), pp: 1498 - 1512, August 2000.

[18] C. Jutten and J. Herault. **Blind separation of sources, Part 1: An adaptive algorithm based on neuromimetic architecture**, *Signal Processing*, Vol. 24, N. 1, pp: 1-10, 1991.

[19] P. Comon, C. Jutten, and J. Herault. **Blind separation of sources, Part *II*: Problems statement**, *Signal Processing*, Vol. 24, N. 1, pp: 11-20, 1991.

[20] P. Comon. **Independent component analysis, a new concept?**. *Signal Processing*, vol. 36, N. 3, pp: 287-314, April, 1994.

[21] A. Boumezzough. **Vers un processeur optoélectronique holographique de cryptage des données haut débit pour les télécommunications**. Phd,*Thèse de doctorat de l'université de louis Pasteur Strasbourg (ULP)*, Janvier 2005.

[22] J. Proakis, **Digital Communications**, *McGraw-Hill*, 1983.

[23] A. Mansour, A. AL-Falou. **Performance indexes of BSS for real-world applications**. *EUSIPCO2006-EURASIP, 14th European Signal Processing Conference*, Italy, September 4-8, 2006.

[24] M. Kendall and A. Stuart. **The advanced theory of statistics: Distribution theory**, *Charles Griffin & Company Limited*, Vol. 1, 1961.

[25] 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, N. 11, pp: 3172-3175, November, 1999.

[26] A. J. Bell and T. J. Sejnowski. **An information-maximization approach to blind separation and blind deconvolution**, *Neural Computation*, Vol. 7, N. 6, pp: 1129-1159, November, 1995.

[27] 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.

[28] A. Hyvaerinen and E. Oja. **A fast fixed point algorithm for independent component analysis**, *Neural computation*, Vol. 9 , pp: 1483-1492, 1997.

[29] M. Kendall and A. Stuart. **The advanced theory of statistics: Distribution theory**, *Charles Griffin & Company Limited*,Vol. 2, 1961.

[30] A. Mansour and C. Jutten. **What should we say about the kurtosis?**. *IEEE Signal Processing Letters*, Vol. 6, N. 12, pp: 321-322, December, 1999.

[31] A. Papoulis. **Probability, random variables, and stochastic processes**, *McGraw-Hill*, New York, 1991.

[32] J. karhunen and J. Joutsensalo. **Generalizations of principal component analysis, optimization problems, and neural networks**, *Neural Networks*, Vol. 8, N. 4, pp: 549-562, 1995.

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

[34] 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.

[35] A. Mansour, M. Kawamoto and N. Ohnishi. **A survey of the performance indexes of ICA algorithms**, *21st IASTED International Conference on Modelling, Identification and Control (MIC 2002)*, pp: 660-666, 18-21 February, 2002.