Color Video Sequences Encryption/Decryption Processes Using Several Color Keys Images

Rami El Sawda, Ayman Alfalou
ISEN-Brest Laboratory L@bISEN
20 rue cuirassé Bretagne
CS 42807, 29228 Brest cedex 2, France
rami.el-sawda@isen.fr, ayman.al-falou@isen.fr

Habib Hamam
EMAT Laboratory
University of Moncton
165 Massey av.,
Edmundston (N.-B.), Canada E3V 2S8
Habib.Hamam@umoncton.ca

Abstract

An optical encrypted color video sequence based on a spectral fusion of information has been proposed. Each color image of the sequence is decomposed into three basic color components. Pertinent information fusion is considered as segmentation. Encrypting consists in modulating each of these three components of the image spectrum by a corresponding phase mask. This phase mask includes pertinent information collected from various encrypted color keys according to a fusion criterion. As encrypting keys are formed by real images, it becomes an impossible task to get the target image by any trial and error random images techniques. For decrypting, a simple algorithm based on segmented correlation filters is proposed. Simulation results corroborate the effectiveness of our algorithm.

1. Introduction

Security and confidentiality are essential elements in telecommunication systems. Cryptography is a very effective way to protect transmitted information. Optical techniques are of great importance to deal with huge quantities of information, such as in the cases of high bit rate transmission and storage of high-resolution images. Recently, several methods of optical encryption, based on Fourier Transform or Fractional Fourier Transform, were proposed [1-7] to prevent the access or the use of information by unauthorized people. Images encryption by an optical processing has many inherent advantages, for examples the possibility of parallel processing and increase the level of security by adding other keys such as the focal distances of the lenses. Another advantage of optical techniques of encryption is the possibility of implementing them in all-optical systems or in hybrid system (holographic-electronic).

In this article, we are using the property of coherent optics to enable carrying out encrypting all-pixels in parallel way by a simple use of convergent lens. This coherent optics property is intensively used for real time target identification [8-10] to perform real time high-resolution image encryption.

Using our optical method, the target image can be encrypted while remaining in an optical form. Conversion into an electric form for transmission and/or storage purposes is performed

after encryption. Thus, the electronic hacking becomes very complex to be achieved since various keys are necessary. A combination of optical and digital protection is not likely to be circumvented by hackers and remains very complicated to carry out. In order to increase the level of security of our technique, it is obvious that the image must also be decrypted in an optical way.

A method of optical encryption of the images with a random white noise is proposed in [1]. This method uses two keys generated randomly to encrypt the input image. The first key is multiplied by the input image while the second is multiplied by the spectrum of the input image. In linear coding (based on the modification of the amplitude), the target image is generally supposed to be real and positive and it is coded in the encrypted image [1]. In non-linear coding (entirely based on the modification of the spectral distribution of the target image spectrum), only the phase of the target image is coded [3]. The two possibilities were analyzed in the presence of a perturbation in the encrypted image and the results show high performance in terms of robustness against the noise [3]. We propose a new method to encrypt color images inspired from the optical encryption techniques, in particular, that developed in [7]. This method is based on a developed criterion of the energetically segmentation technique [11], best adapted in our study. This method allows us to optically encrypt color images by using three parameters in an independent way for the purpose of improving the encryption performance of our method:

- The use of several key color images.
- The criterion of the segmentation or the criterion of information used spectral fusion.
- Optical system components.

2. Color image encryption by the proposed method

Compared to conventional electronic techniques, the use of all-optics encryption has the advantage of processing the image globally but not pixel wise. As shown by the diagram in fig. 1, after the image is Fourier transformed, the encryption of its spectrum can be simply obtained by algebraically multiplying this spectrum by one or more well-defined masks. This operation aims at changing the spectral distribution of the image and therefore encrypting it. At the output of our processor, we obtain the encrypted image by Fourier transforming this multiplication product [7].

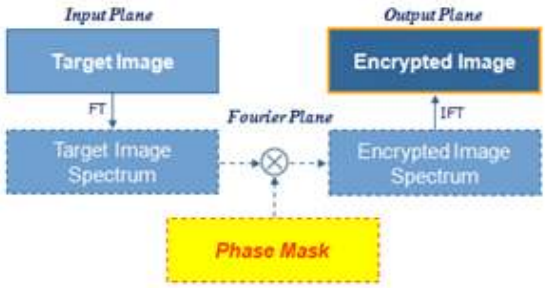

Figure 1. Synoptic diagram of the optical encryption method.

Our architecture will present how to convert color images. A phase mask obtained from other color images will serve as key images. Because color images are used, the first step consists in decomposing the color image into its three basic color components namely the red (R), green (G) and blue (B) components as shown in fig. 2. A color image is obtained by an

additive synthesis of its three components [12]. To adapt it to our optical system, we will convert each of its components R, G and B in a grayscale image [13,14].

Then, we will encrypt each of these three images separately with an adapted color phase mask. For this purpose, we separately Fourier transform each component (converted to grayscale image). Thereafter, each of these obtained spectra (S_{IR}, S_{IG}, *and* S_{IB}) is multiplied (pixel by pixel) by a color phase mask (S^{IKR}, S^{IKG} *and* S^{IKB}). The three colors of this phase mask are obtained by segmenting several color keys (each of these keys is decomposed into its three basic color component). Fabrication of this color phase mask will be presented in the following section. In the output plane, we make separately Fourier transform for each of the three products. We thus obtain three encrypted grayscale images. To decrypt the color image we only need to recover its three color components, then to add them together.

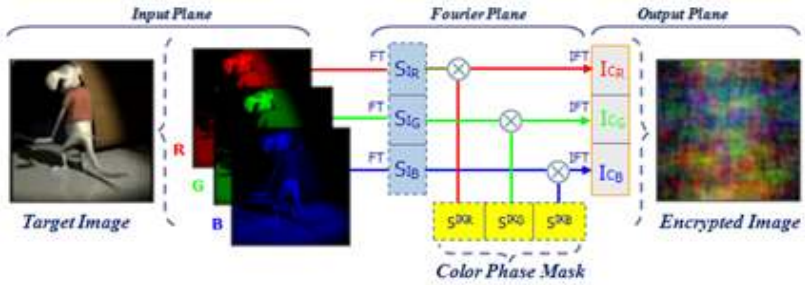

Figure 2. Model of color image encryption.

2.1. Manufacturing of the phase mask

To encrypt a color image, we first use only two other color images as key images. Second, we use several key color images in order to further secure encryption (increase the encryption level). These two images are merged together in the Fourier plane, by a spectral fusion technique. We used this technique to optimize the space bandwidth product in the Fourier plane. This technique was defined in fig. 3. The latter compares (for each of these three basic component converted into grayscale image) the real part of the pixel *(i,j)* of the first key color image $S^{Ik(1)}$ with the pixel *(i,j)* at the same position in the second key color image $S^{Ik(2)}$. We retain for each position *(i,j)* the pixel having the highest value. To design our color phase mask, we chose two images: (the key color image 1) and (the key color image 2) as represented in fig. 4. These images must have the same size.

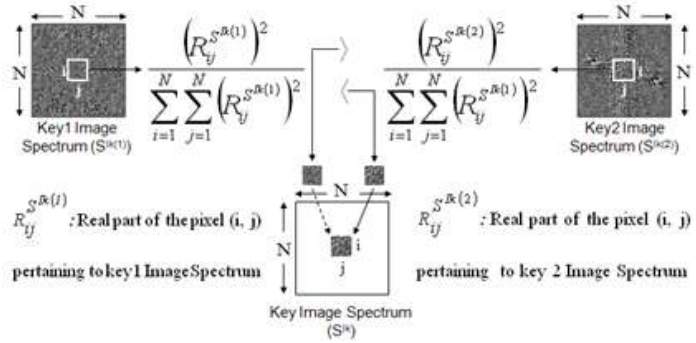

Figure 3. Segmentation criterion based on a real part comparison.

Moreover, it is necessary to avoid local saturation. Indeed this problem arises when we segment the Fourier plane in several zones and when we assign only one key image to each zone. Due to the segmentation, the fusion of keys 1 and 2, we obtain the segmented key.

In this paper, we compare respectively the real part of the pixel *(i,j)* of the first key color image (divided into three basic components spectra : S^{Ik1R}, S^{Ik1G} *and* S^{Ik1B}) with the real part of the pixel *(i,j)* of the second key color image (also divided into three basic components : S^{Ik2R}, S^{Ik2G} *and* S^{Ik2B}) in fig. 4. Thus we obtain three segmented color key components (S^{IKR}, S^{IKG} *and* S^{IKB}) representing the segmented key (color phase mask).

As mentioned above, the proposed method of encryption consists of modifying the phase of the target image by multiplying its spectrum by an adapted binarized phase mask, and by using the technique of real part pixel comparison. This binarization is necessary to reduce the size of the phase mask and also to allow us an optical implementation of this method by using a spatial light modulator "SLM" of binary nature. The binarisation consists of assigning value +1 (the optical phase is 0) to each pixel having a positive real part and value -1 (the optical phase is π) in the contrary case. Thus starting from two key color images, we could make a binarisation of the three segmented color component key (phase mask) as explained in fig. 4.

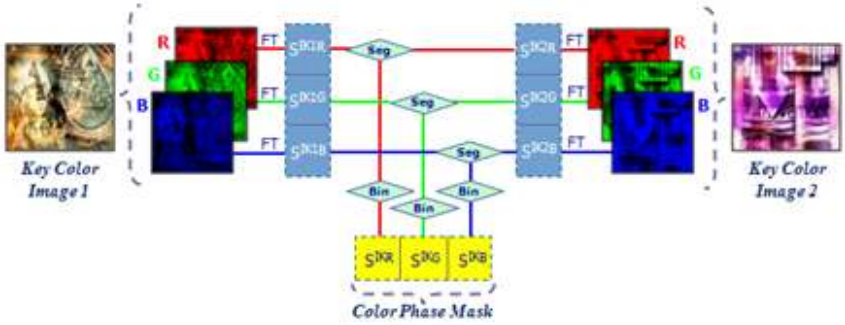

Figure 4. Synoptic diagram of the color phase mask fabrication.

2.2. Optimization of phase mask manufacture

In the previous paragraph, we described the implementation method of the encryption phase mask which is based on spectral fusion. In order to improve the encoding efficiency, we multiplied each key image, used to implement the mask of phase, by its own phase profile [15,16]. We conclude that the spectra of the various key images are better distributed over the entire Fourier plans. Thus, we obtain a better fusion and therefore a better encryption.

With this optimization method, we note an increase in the value of *MSEc* (**M**ean **S**quare **E**rrors between the target image and the encrypted image) with an increase in the number of amalgamated images (i.e.: increase in the security level).

2.3. Optical encryption of color images

Figure 2 shows the proposed architecture to encrypt a color image. This color image is placed in the input plane of our optical processor. To separate the three components from the color image, we can illuminate this image by three respective laser beams (Red, Green and Blue). The color components obtained will be recorded on optical elements such as optoelectronics interfaces. These elements are composed of photosensitive material, such as

amorphous silicon to record the intensity of light exiting the image. Thus, these three color components become grayscale images.

The Fourier transformation is carried out optically by simply using a convergent lens. We obtain in the Fourier plane the spectra corresponding to the three components of the color image (S_{IR}, S_{IG} *and* S_{IB}). We multiply the three resulting spectra of the input image by a phase mask mentioned above consequently, each of these three components modulated by the corresponding phase mask is separately Fourier transformed by means of a second convergent lens. The obtained encrypted image is then displayed on a CCD camera placed at the output of our optical processor. To test the performance of our method, we simulated our technique of encryption with Matlab. For this purpose, we have encrypted the image presented in fig. 6(a) with a phase mask using two keys images figs. 6(b) and (c). The obtained encrypted image is shown in fig. 6(d). These results show that we succeeded in encrypting the target color image while using color keys.

3. Decryption of a color image by the suggested method

Any encryption phase requires a decryption phase. Decryption in our technique is based on the use of the correlation method in order to recognize the color phase mask used in the step encryption. By definition, the correlation measures the degree of resemblance between two images. In this section, we use this method to decrypt the received image. The decryption technique, described by the synoptic diagram in fig. 5, consists in multiplying the spectrum of the encrypted image (received) by a segmented correlation filter. The latter is made with the same color keys used in the phase of encryption as we detailed before. The choice of this filter is justified by its very selective nature [7].

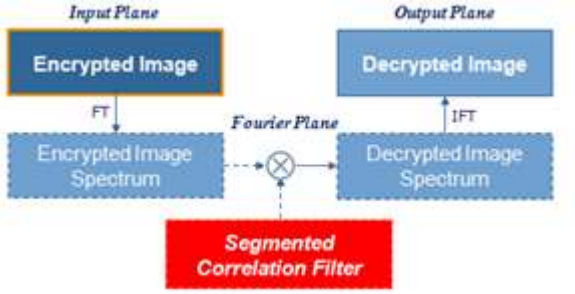

Figure 5. Synoptic diagram of the decryption method.

As we have a color encrypted image, the first step consists in decomposing the encrypted image into its three basic colors components. Then we multiply respectively in the Fourier plane the spectrum of each component by the corresponding correlation filter. Finally we realize an inverse Fourier transformation for each multiplication obtained in the aim to restore the three basic components of the target image previously encrypted. Regrouping these three components makes it possible to obtain the decrypted color image.

4. Video encryption/decryption application

In this section an application of our image encryption method is proposed to encrypt and decrypt all colored images in a video sequence. As shown by the diagram in fig. 6, the video sequence is decomposed into several color images. Each color image is decomposed into its three basic color components namely the red (R), green (G) and blue (B) components, an example of an image decomposition is shown in fig. 2. Then, to encrypt all sequence images

with the adapted color phase mask shown in fig. 4, we multiply separately each phase mask component spectrum by the corresponding color component spectrum for all sequence images. We make separately an inverse Fourier transform for each product and we regroup for each sequence image its three encrypted color components. Thus, we obtain a video sequence where all images are encrypted.

To decrypt the encrypted video sequence, the first step consists in decomposing each encrypted image of the video sequence, into its three basic colors components. Then we multiply respectively in the Fourier plane the spectrum of each component by the corresponding segmented correlation filter. Finally we realize an inverse Fourier transformation for each multiplication obtained in the aim to restore the three basic components of each image previously encrypted in the video sequence. Regrouping these three components makes it possible to restore decrypted video sequence.

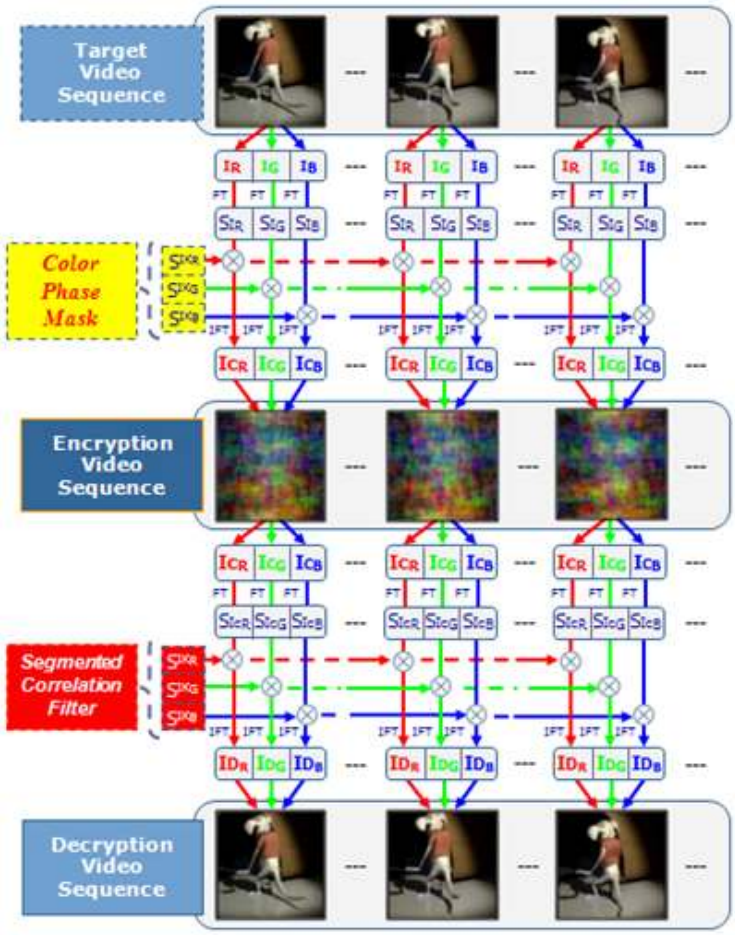

Figure 6. Synoptic diagram of the video sequence encryption/decryption

5. Results of the digital simulations

Good encryption performances of our technique are shown using normalized images: target image, encrypted image and decrypted image. In our example to decrypt the encrypted image presented in fig. 6(d), we use our optical correlation filter conceived with images presented in figs. 7(b) and (c) which were used as key images. The decrypted image is

represented in fig. 7(e). This result shows the presence of the decrypted input image centered on the correlation peak. Figure 7(e) shows a very good visual quality of the decrypted image at the output.

Figure 7. Encryption and decryption color image: (a) target image, (b) key image 1, (c) key image 2, (d) encrypted image, (e) decrypted image.

In order to quantify performance results, **M**ean **S**quare **E**rrors (***MSE***) have been considered: first between target and encrypted images, then between target and decrypted images:

$$MSE = \frac{1}{N.N}\sum_{i=1}^{N}\sum_{j=1}^{N}\left|f^{'}(i,j) - f(i,j)\right|^{2} \quad (1)$$

We evaluate two MSE(s):

MSE_c: is the difference between the encrypted image and the target image.

MSE_d: is the difference between the decrypted image and the target image.

The obtained results using color images are shown in the Table 1. The first column (Table 1-a) shows that we successfully encrypted the target image with a very good security level (a big value of MSE_c). In addition, the very small MSE_d value (5.7639e-033) corroborates good decrypted performances. The second column (Table 1-b) shows our optimized MSE_c1 values (MSE_c2) as we detailed in section 2.2. We prove that we succeeded in increasing the encryption security level by increasing the MSE_c2 values by our optimized method as shown in fig. 8.

Table 1. Comparison of MSE_c Value

		MSE_C1	MSE_C2
Number of Keys	1	0,0640	0,0640
	2	0.0561	0.0670
	3	0.0598	0.0686
	4	0.0650	0.0690
	5	0.0617	0.0705
	6	0.0730	0.0706
	7	0.0766	0.0746
	8	0.0850	0.0968
		(a)	(b)

Our experimental results prove that encryption becomes more robust when we increase the number of keys. The decryption is not altered by this operation and the decrypted image keeps its good quality. As shown in Table 1, these values clearly show the very good behavior of our color images encryption technique.

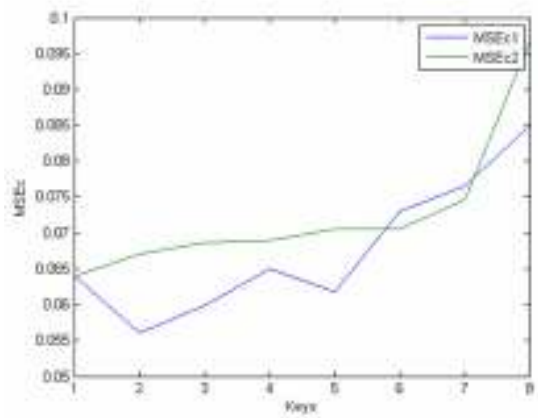

Figure 8. Performances of our optimized method.

6. Conclusions

In this article, we proposed and validated a new optical method to encrypt and decrypt color video sequences. This technique is based on fusion in the Fourier plane of several keys information. It allows us to encrypt images of a color video sequence by multiplying respectively each of three spectra image (corresponding to its three basic color components R.G.B) with their corresponding binarized color phase mask. This operation is followed by an inverse Fourier transformation for each multiplication. The regrouping of the three obtained encrypted components allows us to obtain the encrypted image. We succeeded in retrieving the target image by decrypting it with our optical correlation technique. For that, we begin by decomposing the encrypted color image into its three basic components. Then, the spectrum of each component is multiplied by its adapted correlation filter.

Simulation results show that this optical technique of encryption does not affect the quality of the target image (very small value of the MSE_d). A good compromise between quality of the color decrypted image and security level has been reached. The major point of the proposed method resides in its simplicity and the possibility to increase in the encryption level by using several color image keys. Finally, simulation results clearly prove very good visual and quantitative results of the system and a low MSE_d. An improved encryption level can be achieved by increasing number of keys.

Acknowledgment: This work is supported by University of Moncton - Canada

7. References

[1] P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding, " Opt. Lett. 20, 1995, pp. 767-769.

[2] F. Goudail, F. Bollaro, B. Javidi, and P. Refregier, "Influence of perturbation in a double phase-encoding system", J. Opt. Soc. Am. A, 15, 1998, 2629-2638.

[3] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor", J. Opt. Soc. Am. A, 16, 1999, pp. 1915-1927.

[4] J. Ohtsudo and A. Fujimoto, "Practical image encryption and decryption by phase-coding technique for optical security systems", Appl. Opt. 41, 2002, pp. 4848-4855.

[5] Guohai Situ and Jingjuan Zhang "Position multiplexing for multiple-image encryption", Journal of Optics A: Pure and Applied Optics, 8, 2006, pp. 391-397.

[6] Z. Xin, Y. Sheng, W. Sheng-wei, and X. Jian, "Affine cryptosystem of double-random-phase encryption based on the fractional Fourier transform", Appl. Opt. 45, 2006, pp. 8434-8439.

[7] R. El Sawda, A. Alfalou, G. Keryer and A. Assoum. "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 2006, pp.1474-1477.

[8] P.G. Martinez, J. Otón, J.J. Vallés and H.H. Arsenault, "Nonlinear Pattern Recognition Correlators Based on Color Encoding Single Channel Systems", Appl. Opt. 42, 2004, 425-432.

[9] A. AlFalou, M. ElBouz and H. Hamam "Segmented phase-only filter binarized with a new error diffusion approach" Pure Appl. Opt. 7, 2005, 183-191.

[10] J.L. Tribillon, Book Traitement optique de l'information et reconnaissance des formes par voie optique, Teknea, 1998.

[11] A. AlFalou, G. Keryer, and J.L. de Bougrenet de la Tocnaye, "Optical implementation of segmented composite filtering", Appl. Opt. 38, 1999, pp. 6129-6135.

[12] J.P. Cocquerez, S. Philipp, Book Analyse d'images, filtrage et segmentation, Dunod, 1997.

[13] 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, 9, 2007, 73-80.

[14] A. Alkholidi, A. Alfalou and H. Hamam, "A new approach for optical colored image compression using the JPEG standards", Signal Processing, 87, 2007, pp. 569-583.

[15] F Membrey and J Duvernoy,"Pattern recognition and size determination by means of a multiple matched filter" Nouvelle Revue d'Optique, 4, 1973, pp. 83-86.

[16] W. J. Dallas, "Deterministic diffusers for holography", Appl. Opt, 12, 1973, 1179-1187.

Authors

Rami El Sawda obtained his BSc in Telecommunication from Lebanese University in 2001, and MSc degree in Software Systems and Network Engineering from Antonine University of Beirut, Lebanon, in 2004. His research thesis is to perform an optoelectronic processor of high rate images encryption**.** He is currently pursuing a Ph.D. degree in Telecommunications from Western Brittany University (UBO), France. He is a Student Member of the Institute of Electrical and Electronics Engineers (IEEE) and professional member of Engineering and Scientific Research Groups (ESRGroups). His research interests include optical information processing, security systems and optical correlators.

Ayman Al Falou obtained his PhD in Telecommunication and signal processing from the French National Telecommunication Graduate Engineering School of Brittany (ENSTB-France) and of the university of Rennes (1), in 1999. He obtained his French Qualification under-lecturer certificate in Electronics, optronics and systems (French Education Ministry), 2000. He received the HDR : Habilitation of Conducting Research in Science University of Brest (UBO) – ISEN-Brest, France in 2006 (Habilitation de Diriger les Recherches en Sciences). He is a Professor of Telecommunication and signal processing at ISEN-Brest (the Graduate School of electronic Engineering). He is head of the Optoelectronic Laboratory at ISEN-Brest. His research interests are Signal processing and image processing, Telecommunication, optical systems, optical Processing, optoelectronics, Laser, Opto-electronic Encoding/Decoding, Independent Components Analyses (ICA).

Habib Hamam obtained the B. Eng. and M.S. degrees in information processing from the Technical University of Munich, Germany, 1988 and 1992, and the Ph.D. degree in telecommunication from University of Rennes. He conjointed with France Telecom Graduate School, France 1995. He is currently a Full Professor in the Department of Electrical Engineering at the University of Moncton. He is currently an Associate Editor for IEEE Canadian Review. His research interests are in optical and wireless telecommunications, diffraction, fiber components, optics of the eye, biomedical engineering, and E-Learning.