A new simultaneous compression & encryption method for images suitable to recognize form by optical correlation

Ayman Alfalou, Marwa Elbouz, Maher Jridi, Alain Loussert

A new simultaneous compression & encryption method for images suitable to recognize form by optical correlation

Ayman Alfalou*, Marwa Elbouz, Maher Jridi Alain Loussert
Département optoélectronique, Laboratory L@BISEN
20 rue cuirassé Bretagne CS 42807, 29228 Brest Cedex 2, France2

ABSTRACT

In some recognition form applications (which require multiple images: facial identification or sign-language), many images should be transmitted or stored. This requires the use of communication systems with a good security level (encryption) and an acceptable transmission rate (compression rate). In the literature, several encryption and compression techniques can be found. In order to use optical correlation, encryption and compression techniques cannot be deployed independently and in a cascade manner. Otherwise, our system will suffer from two major problems. In fact, we cannot simply use these techniques in a cascade manner without considering the impact of one technique over another. Secondly, a standard compression can affect the correlation decision, because the correlation is sensitive to the loss of information. To solve both problems, we developed a new technique to simultaneously compress & encrypt multiple images using a BPOF optimized filter. The main idea of our approach consists in multiplexing the spectrums of different transformed images by a Discrete Cosine Transform (DCT). To this end, the spectral plane should be divided into several areas and each of them corresponds to the spectrum of one image. On the other hand, Encryption is achieved using the multiplexing, a specific rotation functions, biometric encryption keys and random phase keys. A random phase key is widely used in optical encryption approaches. Finally, many simulations have been conducted. Obtained results corroborate the good performance of our approach. We should also mention that the recording of the multiplexed and encrypted spectra is optimized using an adapted quantification technique to improve the overall compression rate.

Keywords: Optical correlation, BPOF, Optical compression, optical encryption, FFT, DCT, Fusion in the Fourier plane.

1. INTRODUCTION

Nowadays, the diversity and the increased number of modern image communication systems are the major motivation for many researchers around the globe to focus on this research direction. Several methods of compression and encryption have been proposed. Among these methods, coherent optical ones are very promising [1].

At the origin and ends of any application, images are light and optical matters. Otherwise, computers, hard drive memories, internet and wireless communication systems require images in digital formats. In order to transmit, store, compress, and/or encrypt images, important computing time and resources are needed to convert the optical images to digital ones. A major advantage of optical approaches compared to digital methods lies in their capability to realise huge number of real-time parallel operations in a two-dimensional space. Optical pre-processing approaches are of great interest from both academic and practical perspectives, as shown in the special Appl. Opt. issue on Specific Tasks Sensing [Appl. Opt. **45** (2006)].

In [2], Drakis and Soraghan proposed a compression method for interference patterns based on off-axis (phase-shifting) digital holography. Recently, same authors proposed the hologram compression PSIDH scheme [3]. The originality of their approach manifest in a compression step, based on quantification and BWT [4], in the reconstruction plane rather than in the spatial domain (complex wavefront or interference pattern). Wijaya *et al*. also developed a compression method for pattern recognition on mobile devices based on JPEG2000 [5]. This approach deals with a wavelet-based compression engine used to compress face images with low bit rates suitable for transmission on low bandwidth communication channels. At the receiver end, transmitted images are reconstructed using a JPEG2000 decoder [5]. The authors of [6] proposed another compression method based on multiplexing operations in the Fourier domain. The latest

* ayman.al-falou@isen.fr; phone + 33 2 98 03 84 09; fax + 33 2 98 03 84 10

Optics and Photonics for Counterterrorism and Crime Fighting V, edited by Colin Lewis,
Proc. of SPIE Vol. 7486, 74860J · © 2009 SPIE · CCC code: 0277-786X/09/$18 · doi: 10.1117/12.830180

method consists in gathering the spectra of various images according to a predefined criterion. In their approach, a suitable phase term should be added to each spectrum in order to separate the various obtained images in the output plane which is the Fourier transform of the original segmented Fourier plane. The segmentation is done, in Fourier plane, by comparing pixel energy levels for all pixels (x,y) in two different images. To optimize this segmentation, a reorganization of various Fourier planes should be carefully done to prevent the overlapping of specific important zones of each image, further details can be found in [7]. The arrangement of Fourier planes is obtained by shifting the centres of various spectra [7].

Thanks to the advantages and simplicity of JPEG compression technique [8, 9], Alkholidi *et al.* successfully developed all optical set-up. As JPEG compression is based on the DCT which can be considered as a real Fourier transform and FT can be optically implemented using a simple convergent lens. Therefore, Alkholidi *et al.* proved that DCT can be carried out using FFT [8, 9]. In fact, by duplicating the target image (i.e. the image which should be compressed), they eliminate the sinus part of the FT. Later on, holograms were used as the optical implementation of DCT. Finally, a simple low-pass filter has been included to reduce the amount of stored or transmitted data.

For facial or sign language recognition, multiple images or video should be processed, stored or transmitted. Powerful security level (encryption) and transmission rates (compression rate) should be then deployed. To solve conventional compression and encryption problems, a new approach for simultaneously encryption and compression of images is developed hereinafter. This approach is based on Discrete Cosine Transformation "DCT" and on the use of several encryption keys (biometric keys and random phase ones). To the Best of Our Knowledge, there is no important previous works on the simultaneous compression and encryption using frequential filtering and so well-suitable with correlation's technique.

2. OPTICAL CORRELATION

Different recognition systems based on various schemes have been considered in our previous works. As these works are beyond the scope of this communication, no further details concerning them are given hereinafter (more details can be found in the web site of ISEN-Brest and further information can be obtained upon request from the authors). In this manuscript, a recognition system based on optical multidecision correlators has been investigated. The later scheme has two major advantages a reconfigurable architecture and a multidecision optical correlator based on a composite filter previously discussed in [10-12]. The segmented composite filter divide the Fourier plane into several domains and assign each one to just one reference. Figure (1) illustrates the principle of an optical correlator multidecision using spatial light modulators (SLM) which display the Segmented Composite Phase Only Filters (SCPOF) in a Fourier plane. It is worth to notice that the phase filters are required in practical optical set-ups with optimised energy for a multidecision correlation [13,14].

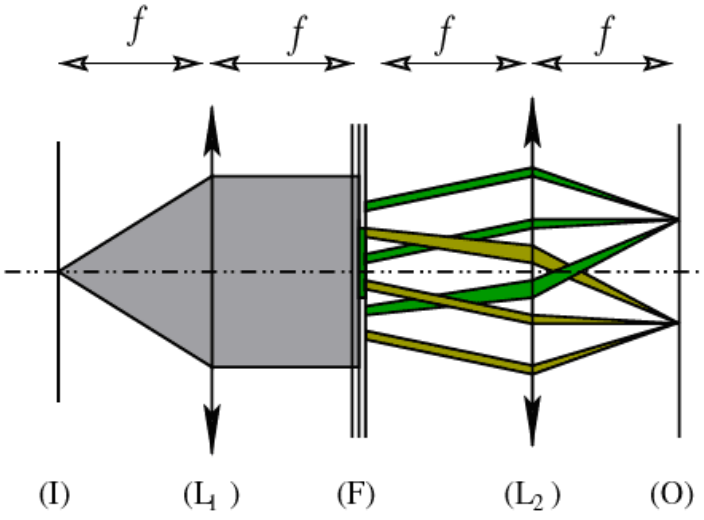

Figure 1. Principle of a multidecision correlator using a segmented composite POF filter.

Possibilities of parallelism in suitably designed filters, namely the segmented composite filters, significantly increase the processing capacity. Additionally, an optimal use of the space bandwidth product available in correlator can be reached, especially into the inter channels diaphony: i.e. assigning one channel to every correlation. Indeed according to [11], the local saturation phenomenon in the Fourier plane is much more important in classical composite filters than in segmented filters. The latter fact is due to the implementation of composite filters, which can locally add spectral information coming from different references. On the other hand, the structure of segmented composite filter cancels out this phenomenon by segmenting the Fourier plane in several areas and each of them corresponds to the spectrum of one image. An optimal segmentation is strictly related to the optimisation of a criterion. In [11], we proposed an energetic criterion insensitive to phase information. By neglecting the phase information, some important information could be lost. To rectify this problem, we propose the optimization of the following criterion:

In the Fourier plane we assign the pixel (i,j) to the class labelled "k" if and only if:

$$\frac{E_{ij}^{k}\cos(\phi_{ij}^{k})}{\sum_{i=0}^{N}\sum_{j=0}^{N}E_{ij}^{k}} \geq \begin{cases} \dfrac{E_{ij}^{0}\cos(\phi_{ij}^{0})}{\sum_{i=0}^{N}\sum_{j=0}^{N}E_{ij}^{0}} \\ \dfrac{E_{ij}^{1}\cos(\phi_{ij}^{1})}{\sum_{i=0}^{N}\sum_{j=0}^{N}E_{ij}^{1}} \\ \cdot \\ \dfrac{E_{ij}^{L-1}\cos(\phi_{ij}^{L-1})}{\sum_{i=0}^{N}\sum_{j=0}^{N}E_{ij}^{L-1}} \end{cases} \qquad (1)$$

where L stands for the reference number, N is the size of the filter plane, E_{ij}^{k} and ϕ_{ij}^{k} denote respectively the spectral energy the phase of class "k" at a pixel location (i,j). To relate this pixel to a reference, equation (1) should be satisfied. The separation at the output plane is achieved by adding a spatial-frequency dependent phase distribution to every class.

3. SIMULTANEOUS COMPRESSION & ENCRYPTION METHOD

Correlation methods is a very simple and have a good discriminating performance. However, they are very sensitive to any deformation target images that could be carried out by a traditional technique of compression. In this case, the performances of the correlator will be drastically decreased [15]. To solve this problem, we proposed a new method [16,17] which can carry out compression and simultaneous encryption based on a biometric key and Discrete Cosine Transform (DCT) which is widely used in digital compression techniques such as JPEG. The main idea of our approach consists in taking advantage of optical compression based on FT and encryption methods, on the one hand, and, on the other hand, by using powerful signal processing tools to secure the transmitted data by using independent transmitters.

In our method, DCT is used to regroup relevant information in order to propose an optical compression and encryption approache. Indeed, an optical compression requires filtering of DCT image spectrums (Figure 2). Using an appropriate filter, we can reduce the size of the original spectrum from (NxN) pixels to the size of ($c\times c$) pixels with $c<<N$, *see* Figure 2-b. This results notably in releasing a large part of the spectral plane. While regrouping, in a non-destructive way, these various spectra in a single plane, we obtained the compression and the multiplexing of these various images. The maximum number of images which can be multiplexed together depends on the minimum required size of their spectra. This non-destructive regrouping also changes significantly the frequency distribution in the spectral plane resulting in the encryption of our images. In order to ensure a good encryption level against any hacking attempt, we proposed to modify by a frequency rotation the various images before gathering them (Figure 2-c). This ensures that, whoever does not have the necessary information about the spectra number and their distribution in the spectral plane, will not be able to decrypt this information (with reference to Fig. 2 -d). Without the frequency rotation, the shape of the spectra obtained with the DCT can easily retrieved because the spectrum amplitude drops gradually while moving away from the top left-hand corner towards the bottom right-hand corner of the spectrum. This problem can be resolved by

multiplying the multiplexed spectrum by a random mask. This multiplication modifies the characteristic spectral distribution of the DCT. The key-mask will be sent separately as a private encryption key. Once secure and compressed information safely reach the authorized receiver; the image extraction can be easily done by reversing the various steps used in the whole process:

1. Multiply the received image by the inverse of random mask.
2. Make an inverse frequency rotation.
3. Run an Inverse DCT (IDCT).

Preliminary experimental results corroborate the performance of the proposed scheme. However, further simulations and experimental results will be conducted to measure the encryption rate and the compression ratio using different images.

To reinforce the security of our system, we can multiply the obtained spectrum, figure (2-d), by the spectrum of the corresponding fingerprint person figure (2). This multiplication can drastically modify the characteristic spectral distribution of the DCT figure(2-e).

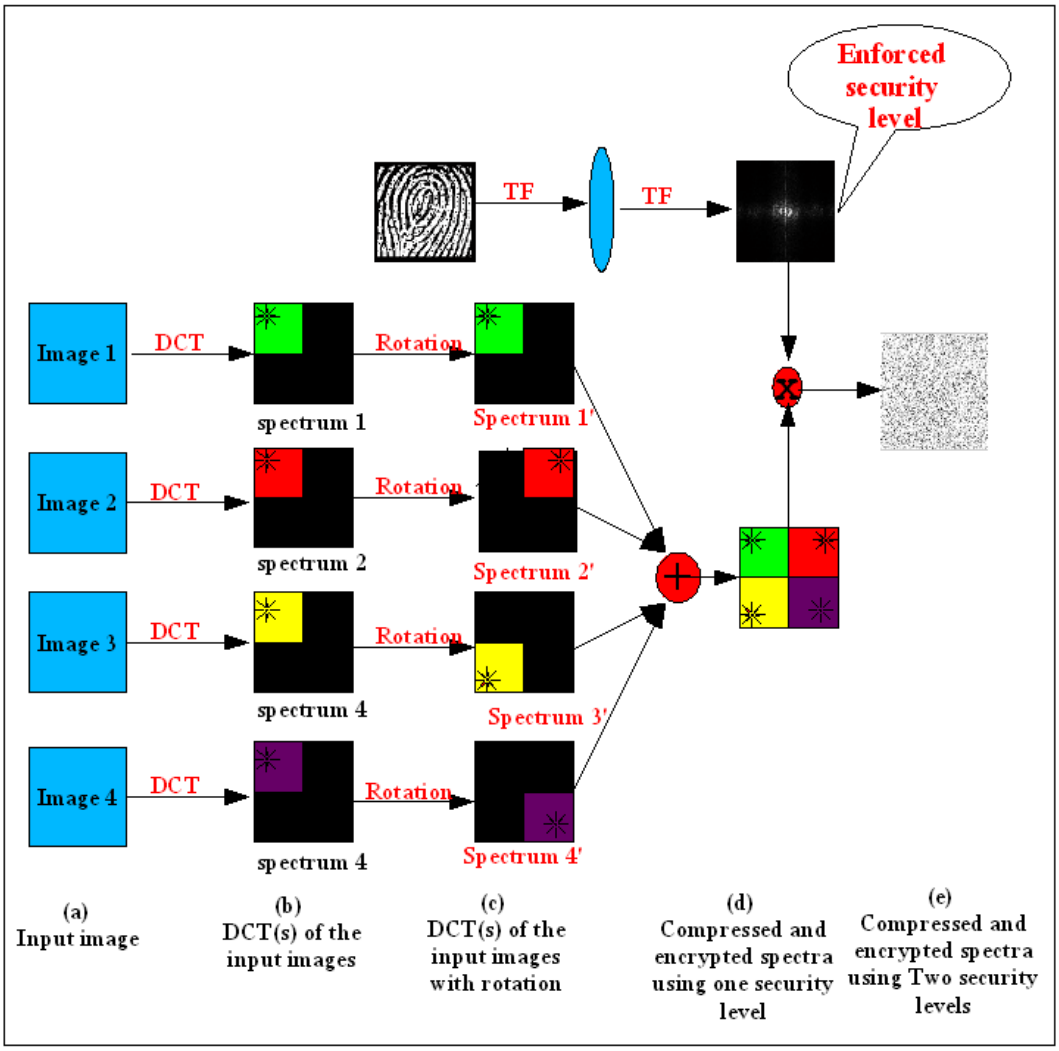

Figure 2. Synoptic diagram of our compression and encryption system using two serenity levels.

4. SIMULATION RESULTS

To validate our approach, a face recognition application is considered. Several numerical simulations have been conducted to test the robustness of the proposed technique as well as to show that the proposed simultaneous compression and encryption do not affect the correlation's decision at the receiver, see Figure (3).

Let us consider two non-compressed "Bitmap" images (**I(1)** and **I(2)**), Figure (4-a). Using these two images, we generate one compressed and encrypted image (**Icc**) shown in figure (4-b). At the receiver, the decryption and the decompression of image "**Icc**" is realized which generates two other images (decrypted and decompressed) designated by (**O(1)** and **O(2)**), see Figure (4-c). Very good quality images with very weak values of the Mean Square error have been shown. Thanks to the good performance of our approach, the correlator's decision does not show any deterioration in our approach on the contrary of a JPEG compression. To obtain such good performance, original images I(1) and I(2) should be correlated by using a segmented filter, see figure (4-d). The correlation results are shown in Figure (4-e). We should mention that the same previous filter should be used at the receiver's side to correlate O(1) and O(2)), see Figure (4-f). By comparing the correlation planes and PCEs (Figures ((4-e) and (4-f)), we can notice that there is no significant drop in PCEs as well as the peaks of correlation are always very sharp and well centred.

That enables us to validate our approach and to show that the proposed technique of compression and simultaneous encryption does not deteriorate the performances of the decisions of the correlator using a multi-correlation segmented filter.

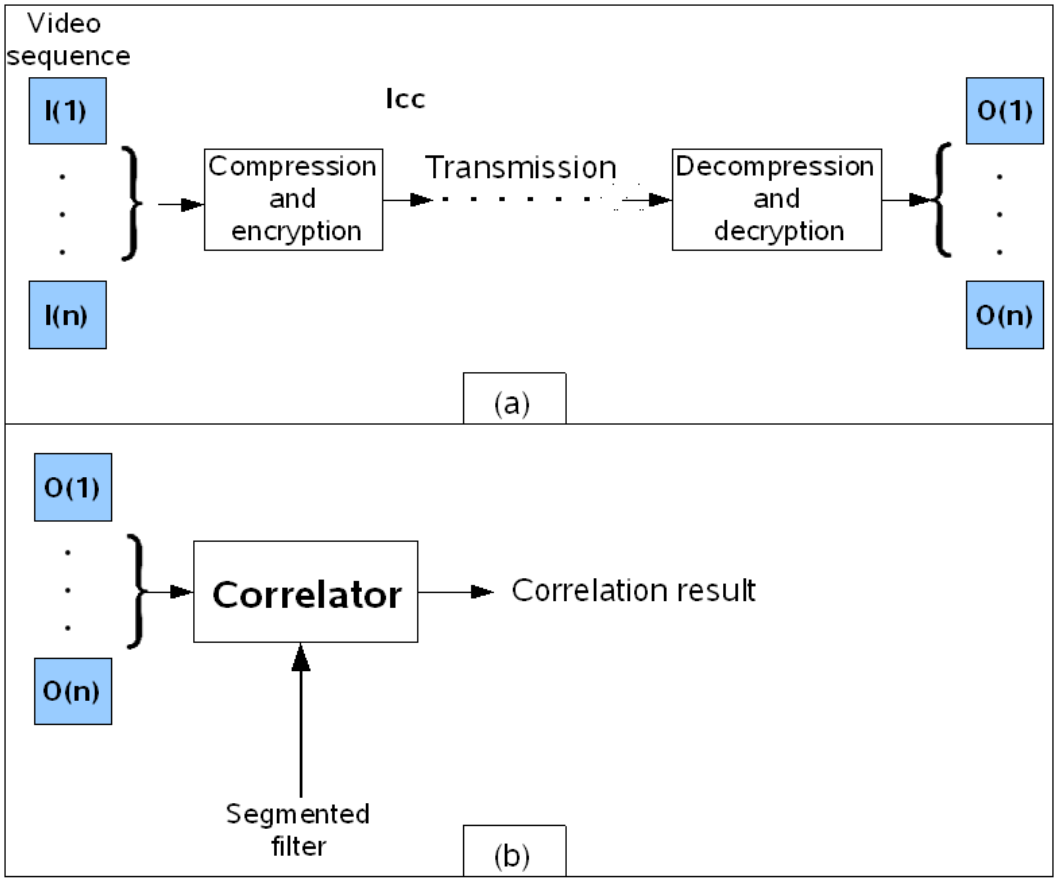

Figure 3. Synoptic diagram: (a) Video sequence Compression/Decompression and Encryption/Decryption (b) Identification and Recognition using a segmented filter carried out with non compressed and non encrypted references.

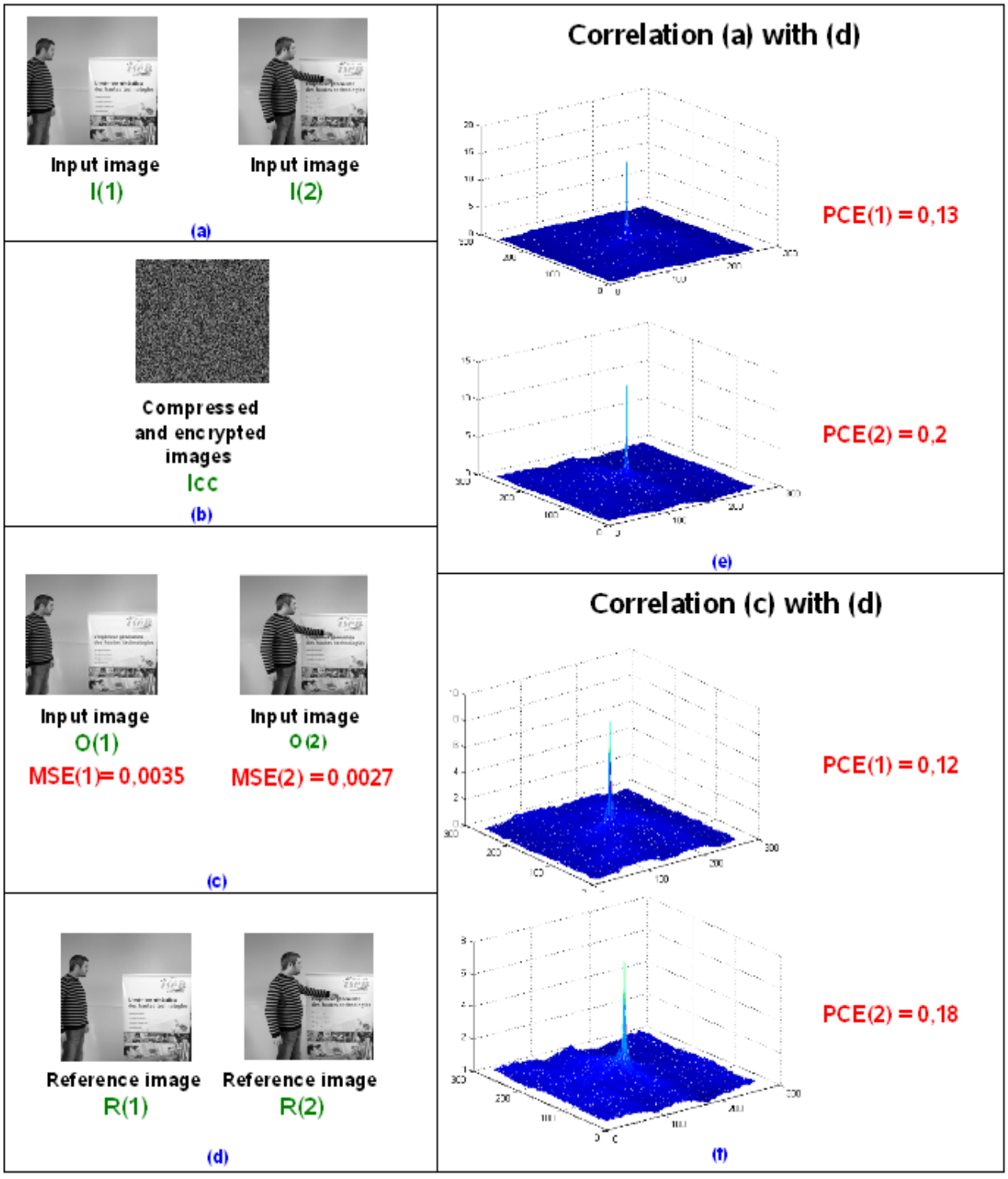

Figure 4. Simulation results.

5. CONCLUSION AND PERSPECTIVES

In this manuscript, various compression techniques have been discussed. A new method of simultaneous compression and encryption based on a filtering and a "DCT" transformation is proposed. By applying our technique, PCE values and various correlation peaks do not show any significant loss. It is well known that this loss can produce deterioration in the correlation's decision. Further experimental results will be conducted to test the robustness of our approach with an increased number of images, i.e. against the increase of the compression ratio.

We should mention that a constant number of bits have been used to decode all DCT pixels. However, in a DCT all the pixels do not have the same importance (the ratio between an upper left corner pixel and the one in the right bottom corner can be 10^6, for images considered in our simulations). Using this property, we propose to normalize the values of the DCT by zones and to code them on a different number of bits according to the zone and the importance of this zone.

At this stage, reconstructed images of poor quality have been obtained if the proposed scheme is completely implemented on optical devices. In addition, the equivalent all-optical system is complex and expensive. To cope with this inconvenient, we propose to digitally implement the method and to take profit from digital circuit evolution. For that, we suggest to use Field Programmable Gate Array (FPGA) as implementation target and VHDL as material description language. It is important to notice that the proposed method presents parallel structure as shown in Fig.2 and this allows a rapid FPGA implementation. Indeed, in the proposed method two important blocks have to be implemented: FT and DCT. For FT function, we can use the well known Fast Fourier Transform algorithm developed in [18] and for DCT, pipelined representation based on the Loeffler algorithm [19] is the most suitable for our method. Finally, digital implementation will require elementary delay elements or registers to synchronize the compression method and the second security level.

REFERENCES

[1] A. Alfalou, C. Brosseau "The nuts and bolts of optical image compression and encryption methods," **submitted.**

[2] E. Darakis and J. J. Soraghan, "Compression of interference patterns with application to phase-shifting digital holography," Applied Optics **45**, 2437-2443 (2006).

[3] E. Darakis and J. J. Soraghan, "Reconstruction domain compression of phase-shifting digital holograms," Applied Optics **46**, 351-356 (2007).

[4] M. Burrows and D. J. Wheeler, [A block-sorting lossless data compression algorithm], Digital Systems Research Center, (1994).

[5] S. L. Wijaya, M. Savvides, and B. V. K. Vijaya Kumar, "Illumination-tolerant face verification of low-bit-rate JPEG2000 wavelet images with advanced correlation filters for handheld devices," Applied Optics **44**, 655-665 (2005).

[6] S. Soualmi, A. Al. Falou, and H. Hamam, "Optical image compression based on segmentation of the Fourier plane: new approaches and critical analysis," J. Opt. A: Pure Applied Optics **9**, 73-80 (2007).

[7] A. Cottour, A. Alfalou, and H. Hamam, "Optical video image compression: a multiplexing method based on the spectral fusion of information**,**" *in IEEE-Conference on Information and Communication Technologies: From Theory to Applications,* IEEE, 1-6 (2008).

[8] A. Alfalou and A. Alkholidi, "Implementation of an all-optical image compression architecture based on Fourier transform which will be the core principle in the realisation of DCT," Proc. SPIE **5823**, 183-190 (2005).

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

[10] G. Keryer, J. L. de Bougrenet de la Tocnaye, and A. Al Falou, "Performance comparison of ferroelectric liquid-crystal-technology-based coherent optical multichannel correlators," Appl. Opt. **36**, 3043-3055 (1997).

[11] A. Al Falou, G. Keryer, and J. L. de Bougrenet de la Tocnaye, "Optical implementation of segmented composite filtering," Applied Optics **38**, 6129-6136 (1999).

[12] A. Alfalou, M. Elbouz and H. Hamam, "Segmented phase-only filter binarized with a new error diffusion approach," J. Opt. A: Pure Applied Optics **7**, 183-191 (2005).

[13] J.L. Horner, B. Javidi, J. Wang, "Analysis of the binary phase-only filter," Optics Communications 91, 189-192 (1992).

[14] J. L. Horner, "Metrics for assessing pattern-recognition performance," Applied Optics. **31**, 165-166 (1992).

[15] T. J. Naughton, Y. Frauel, B. Javidi, and E. Tajahuerce, "Compression of digital holograms for three-dimensional object reconstruction and recognition," Applied Optics **41**, 4124-4131 (2002).
[16] A. Alfalou, A. Loussert, A. Alkholidi, and R. El Sawda, "System for image compression and encryption by spectrum fusion in order to optimize image transmission," in IEEE *Proceeding Future Generation Communication and Networking*, 590-593 (2007).
[17] A. Loussert, A. Alfalou, R. El Sawda, and A. Alkholidi, "Enhanced System for image's compression and encryption by addition of biometric characteristics", Int. J. Software Eng. and Appl. **2**, 111-118 (2008).
[18] I.S. Uzun, A. Amira and A. Bouridane, "FPGA implementations of fast Fourier transforms for real-time signal and image processing," IEE Proc.-Vis. Image Signal Process. **152**, 283-296 (2005).
[19] C.-Y. Pai, W.E. Lynch and A.J. Al-Khalili, "Low-power data-dependent 8x8 DCT/IDCT for video Compression", IEE Proc.-Vis. Image Signal Process **150**, 245-255 (2003).