Simultaneous fusion, compression, and encryption of multiple images

Ayman Alfalou, C. Brosseau, Nadine Abdallah, Maher Jridi

Simultaneous fusion, compression, and encryption of multiple images

A. Alfalou,[1,*] C. Brosseau,[2] N. Abdallah,[1] and M. Jridi[1]

[1]*ISEN Brest, Département Optoélectronique, L@bISEN, 20 rue Cuirassé Bretagne, CS 42807, 29228 Brest Cedex 2, France*

[2]*Université Européenne de Bretagne, Université de Brest, Lab-STICC, CS 93837, 6 avenue Le Gorgeu, 29238 Brest Cedex 3, France*

**ayman.al-falou@isen.fr*

Abstract: We report a new spectral multiple image fusion analysis based on the discrete cosine transform (DCT) and a specific spectral filtering method. In order to decrease the size of the multiplexed file, we suggest a procedure of compression which is based on an adapted spectral quantization. Each frequency is encoded with an optimized number of bits according its importance and its position in the DC domain. This fusion and compression scheme constitutes a first level of encryption. A supplementary level of encryption is realized by making use of biometric information. We consider several implementations of this analysis by experimenting with sequences of gray scale images. To quantify the performance of our method we calculate the MSE (mean squared error) and the PSNR (peak signal to noise ratio). Our results consistently improve performances compared to the well-known JPEG image compression standard and provide a viable solution for simultaneous compression and encryption of multiple images.

OCIS codes: (070.0070) Fourier optics and signal processing; (100.0100) Image processing; (200.4560) Optical data processing.

References and links

1. A. Alfalou and C. Brosseau, "Optical image compression and encryption methods," Adv. Opt. Photon. **1**(3), 589–636 (2009).
2. M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process. **52**(10), 2992–3006 (2004).
3. A. Alfalou, A. Loussert, A. Alkholidi, and R. El Sawda, "System for image compression and encryption by spectrum fusion in order to optimise image transmission," FGCN 2007, IEEE Proceeding, ISBN: 0–7695–3048–6, Vol. 2, 2007, pp. 593–596.
4. A. Alfalou and C. Brosseau, "Exploiting root-mean-square time-frequency structure for multiple-image optical compression and encryption," Opt. Lett. **35**(11), 1914–1916 (2010).
5. T. J. Naughton, J. B. McDonald, and B. Javidi, "Efficient compression of fresnel fields for Internet transmission of three-dimensional images," Appl. Opt. **42**(23), 4758–4764 (2003).
6. P. Refrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).
7. B. Javidi, C. M. Do, S.-H. Hong, and T. Nomura, "Multi-spectral holographic three-dimensional image fusion using discrete wavelet transform," J. Disp. Technol. **2**(4), 411–417 (2006).
8. See, e.g. K. R. Rao and P. Yip, *Discrete Cosine Transform: Algorithms, Advantages, Applications,* (Academic Press, 1990), and *http://www.jpeg.org/*.
9. B. Javidi, ed., *Optical and Digital Techniques for Information Security*, (Springer Verlag, New York, 2005).
10. Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express **15**(16), 10253–10265 (2007).

1. Introduction

At present, efforts are underway to develop compression and encryption techniques which are relevant for a broad range of applications from communication systems to secure local-storage and network-transmission of images to medical image security [1–7]. In parallel with experimental progress, the theory and simulation has advanced greatly, allowing, for example, for modelling of the trade-off between image compression and security [2]. While these

#153431 - $15.00 USD Received 25 Aug 2011; accepted 19 Oct 2011; published 10 Nov 2011

techniques were generally elaborated independently, their complexity increases with the system's size. Likewise, they can induce a number of serious restrictions and performance limitations for communication systems of digital products when both techniques are used simultaneously, e.g. traditional encryption techniques degrade the compression rate. Here, what we have in mind is to devise a scheme to circumvent these issues and improve the compression and encryption performances. For this purpose, we adapt the DCT spectral fusion (DCT-SF) method which has been successfully applied for grouping 4 images in the DCT spectral plane [3] with the fusion method of multiple Fourier planes based on a specific shifting [4]. We give strong numerical evidence that this methodology provides a secure means for image compression. The recently described SF-based models using discrete cosine transform (DCT) preclude direct file compression since the rapidly varying spectra necessitate a large number of encoding bits [3]. Here, we show that a more general model allowing us to increase significantly the number of input target images can be used to compress spectrally multiplexed information. The proposed model adopts the approach developed by Naughton *et al*. [5] for encoding the multiplexed files. A main focus of this work is to demonstrate that incorporation of an optimized encryption procedure based on double random phase encryption (DRP) [6] leads to a technique potentially secure against chosen-plaintext attacks.

The rest of this article is organized as follows: in Sec. 2 we will briefly describe the procedure to optimize the DCT spectral fusion of multiple images procedure. The compression of this spectrum is described in Sec. 3. Next, Sec. 4 presents comprehensive numerical tests and a comparative analysis of these results to those obtained by using the well-known JPEG image compression standard. Our last task is to describe our method for reinforcing the encryption. We summarize and conclude in Sec. 6.

2. Spectrally multiplexing multiple images

The fusion method in the spectral domain developed here consists in merging the information contained in different target images. The general problem of interest is illustrated in Fig. 1. We begin by DC transforming each image. On the one hand, DCT is expected to be a valuable tool for all-optical processing of images by using converging lens [1]. On the other hand, the use of DCT (used in the JPEG compression technique [8]) is motivated by the observation that, grouping the information for reconstructing the image, in the upper left corner of its spectral plane. Next, each spectral plane is multiplied by a low-pass filter, which in turn, implies that the spectral information should decrease according the type of the filter considered. The size of the filter (in pixels) $\left(Fs_x, Fs_y\right)$ along x and y can now be expressed as a properly scaled function of the target image size (in pixels) $\left(Is_x, Is_y\right)$ and the number of target images at the input of the system

$$\left(Fs_x, Fs_y\right) = \left(\frac{Is_x}{n}, \frac{Is_y}{n}\right). \tag{1}$$

As a result, the size of the spectral plane is decreased by a factor of n^2, where n denotes the number of target images. Next, well defined rotation and shift operations are applied to each filtered part for grouping 4 DCTs as shown in Fig. 1. Such a grouping of the DCTs results in a first level of encryption. Special attention is called to the fact that the result of this grouping is similar to a Fourier transform. In addition, the reconstructed images overlap each other after these transformations.

The problem to encode the output plane multiplexing the different DCTs, has been outstanding in image processing because it requires a large number of bits which can significantly increase the size of the file containing the images to store and/or transmit. The accuracy and robustness of the procedure are challenging issues, including the difficulty with the required computations. In order to be able to decrease the multiplexed file, an optimized encoding of the different frequencies with a reduced number of bits is needed. For this purpose, we relied on the procedure proposed in [5] as described in the next section.

#153431 - $15.00 USD Received 25 Aug 2011; accepted 19 Oct 2011; published 10 Nov 2011

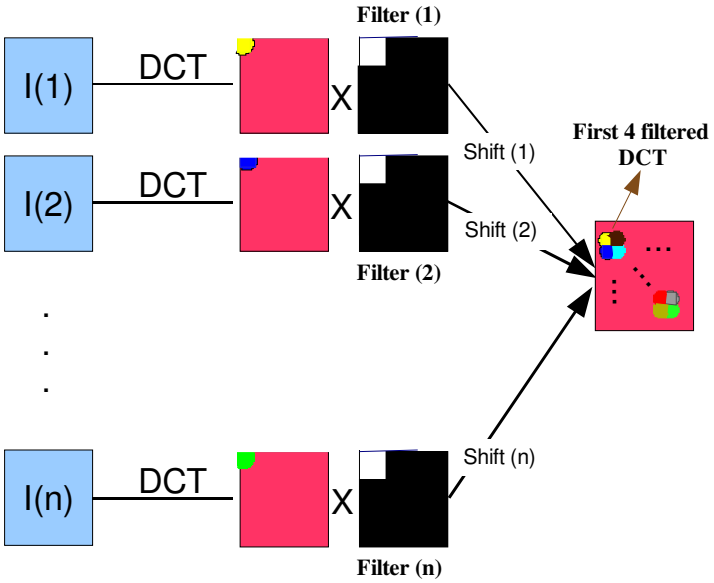


Fig. 1. Synoptic diagram illustrating the fusion method of multiple images, *n* is the number of target images. Rotation, shift, and 4 by 4 grouping constitute a first level of encryption.

3. Compressing images

Now let us consider the spectral compression technique which follows a three-step procedure. We first want to decrease the size of each filtered DCT. For this purpose, we need to increase the number of target images to be multiplexed (see Fig. 2(a)). This arises because the size of the low-pass filter decreases (Fig. 2(b)), and hence the size of each filtered DCT is decreased as shown in Fig. 2(c). In the second step, we divided the filtered part of each DCT in separate areas, starting from the upper left corner (Fig. 2(d)). For illustrative purpose, 2-pixel areas were chosen as shown in Fig. 2(d) along the diagonal, where each color denotes a specific area.

In the third step, a quantization of the different areas is realized through the relation

$$V'_{zone_l}(i,j) = round\left(\frac{\left(2^{m-1}-1\right)V_{zone_l}(i,j)}{Max\left(V_{zone_l}\right)}\right). \tag{2}$$

Here, $V_{zone_l}(i,j)$ and $V'_{zone_l}(i,j)$ correspond respectively to the DCT before and after the quantization of the area ℓ of coordinates (i,j), $Max\left(V_{zone_l}\right)$ denotes the maximum value of the DCT frequencies in the area ℓ, m is the number of bits used for encoding these real-valued frequencies, and *round*(…) is the integer part function. An example of a filtered and quantized DCT is shown in Fig. 2(e) illustrating the changes in the frequencies values for a given $\left(N',N'\right)$ pixel DCT filtered image. The compression rate can be expressed as

$$T_c = \left(1-\frac{nb_{out}}{nb_{in}}\right)100, \tag{3}$$

where nb_{in} is the size (in bits) of the multiple images at the input of the system, with n target 8-bit encoded gray-level images of size (N,N) pixels, i.e. $nb_{in} = 8\times n\times N^2$, nb_{out} denotes the

#153431 - $15.00 USD Received 25 Aug 2011; accepted 19 Oct 2011; published 10 Nov 2011

size of the multiplexed file, i.e. $nb_{out} = n \times m \times \left(N^{'}\right)^2$, and $N^{'}$ corresponds to the size (in pixels) of the filtered DCT. Optimizing T_c can be done by choosing a number of bits relevant to each area (Fig. 2(e)) as $m_l = \log_2\left(Max_l - Min_l\right)$, where $\left(Max_l, \mathrm{Min}_1\right)$ defines the maximum and minimum values for the area ℓ. This rule of quantization constitutes a second level of encryption.

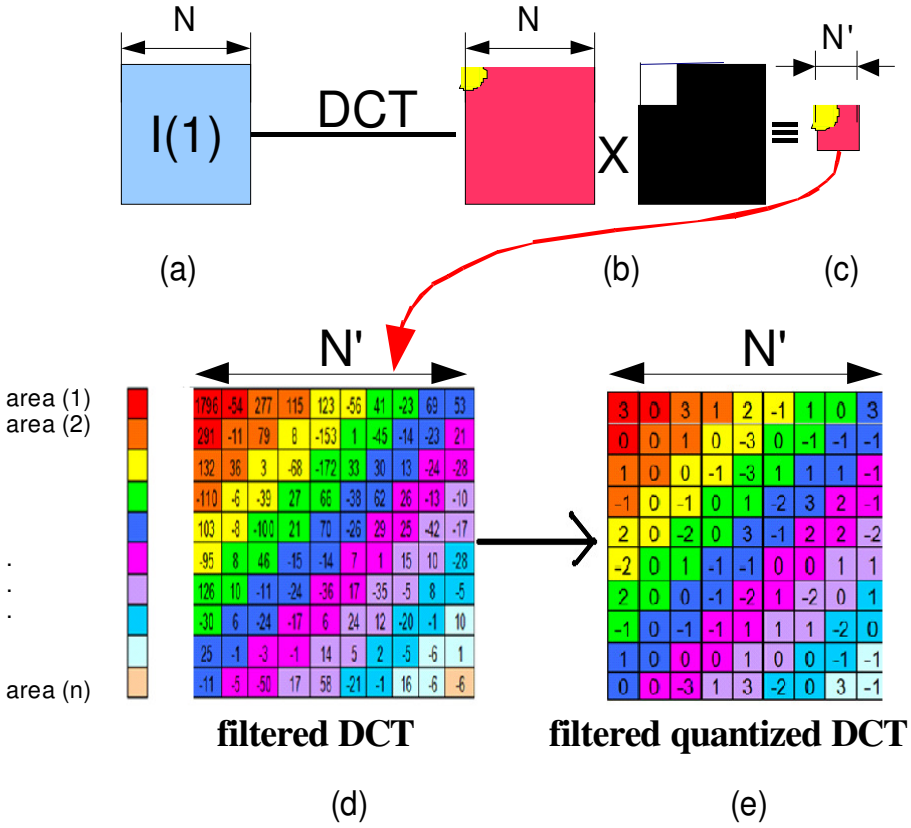


Fig. 2. Principle of the compression technique used in this work: (a) the target image, (b) the DCT and the low-pass filter, (c)-(d) example of a filtered DCT divided in separate areas, (d) the filtered and quantized DCT.

An example from our numerical simulations shown in Table 1 illustrates the good performances of the compression technique. The specific example we consider is a sequence of 16 gray scale and 8-bit encoded images of a subject moving in the scene.

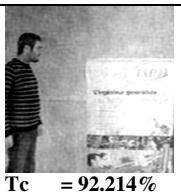
The performance of our method can be quantized by the normalized MSE and the PSNR. These parameters have been numerically evaluated and are summarized in Table 1 which shows also the compression rate T_c and reconstruction results. The integer in the first row considers the number of target images at the input of the system. The second row shows the reconstructed images at the output of the system by encoding the filtered and multiplexed DCTs with m = 15 bits (Fig. 2(e)). The third, fourth, and fifth rows show the results for m = 8, 5, and 3 bits, respectively. For each n and m values we show the reconstructed image at the output of the system.

As can be seen, a compression rate of 98.5% can be obtained for reconstructing the target images, i.e. only 1.5% of the initial size of the target image has been kept. A unique feature of this simulation is that the smaller is m the lesser is the quality of the reconstructed image and

#153431 - $15.00 USD Received 25 Aug 2011; accepted 19 Oct 2011; published 10 Nov 2011

the larger is the compression rate. As also seen in Table 1, good results can be achieved when $m = 5$, while maintaining a significant compression rate.

Table 1. Compression and reconstruction results obtained by increasing the number of target images and decreasing the number of bits for encoding the different areas of the filtered and quantized DCTs.

Bit Number				
Image Number	*m*=15	*m*=8	*m*=5	*m*=3
n=2	 **Tc = 7.844%** MSE = 0.0005 PSNR= 33.0419	 **Tc = 51.66%** MSE = 0.0051 PSNR= 36.9653	 **Tc = 70.92%** MSE = 0.0088 PSNR= 30.5461	 **Tc = 85.416%** MSE = 0.001 PSNR= 18.3696
n=6	 **Tc = 69.46%** MSE = 0.001 PSNR= 30.0369	 **Tc = 84.01%** MSE = 0.0013 PSNR= 28.7088	 **Tc = 90.04%** MSE = 0.0017 PSNR= 27.6306	 **Tc = 92.214%** MSE = 0.0117 PSNR= 19.3921
n=9	 **Tc = 79.69%** MSE = 0.0019 PSNR= 27.158	 **Tc = 89.35%** MSE 0.0019 PSNR= 27.1446	 **Tc = 93.60%** MSE = 0.0023 PSNR= 26.4226	 **Tc = 96.79%** MSE = 0.0116 PSNR= 19.4091
n=16	 **Tc = 88.85%** MSE = 0.0046 PSNR= 23.3774	 **Tc = 94.33%** MSE = 0.0046 PSNR= 23.3725	 **Tc = 96.74%** MSE = 0.0049 PSNR= 23.1258	 **Tc = 98.55%** MSE = 0.0149 PSNR= 18.2952

4. Comparing with the JPEG image compression encoder

We now compare our results with the results obtained by the JPEG image compression standard [8]. We consider the well-known benchmark Lena's picture which does not have a uniform background like the images considered in Sec. 3. The compression rate was kept constant close to 98%. The reconstructed image obtained with our method and that obtained by using the JPEG compression are shown in Fig. 3. Figure 3(a) shows that the contours and the perceptual details of the reconstructed image are degraded. JPEG is the most detrimental for reconstruction since it is sensitive to the different blocks. As we can see in Fig. 3(b), our results demonstrate that a much accurate reconstruction of Lena's picture can be achieved with our methodology. This observation is also consistent with the higher values of the PSNR even if the compression ratio is slightly greater compared to that used for the JPEG method.

#153431 - $15.00 USD Received 25 Aug 2011; accepted 19 Oct 2011; published 10 Nov 2011

We also investigated whether better performances may be achieved with increasing T_c and found that our scheme renders higher PSNR than its JPEG compressed counterpart.

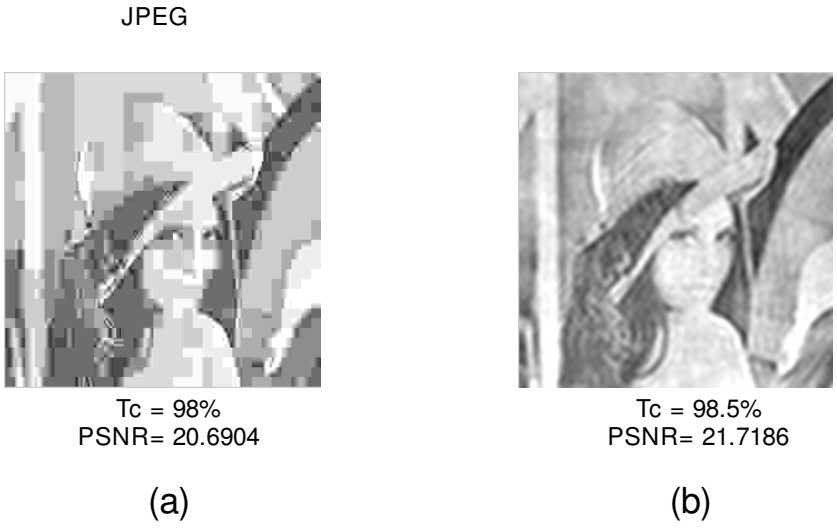


Fig. 3. Comparison of the reconstructed Lena's picture with: (a) the JPEG compression and (b) the present algorithm.

5. Encrypting images

As mentioned previously, two levels of encryption are used in our procedure. The first one is due to the grouping of the DCTs in the spectral domain (see Fig. 1). As we have already mentioned above multiplexing the different images allows the images to overlap each other, and after a second transformation, i.e. to hide the target images, one of the input images is used as encryption key. The second level of encryption originates from the division in separate areas and the quantization of the filtered DCTs. This quantization has for effect to modify the spectral information. Now for increasing the encryption level of our scheme a third level biometric-based encryption is added. The latter consists in multiplying the multiplexed and quantized file with the doubly encrypted spectrum of a fingerprint using the DRP method. Figure 4 shows an illustrative example obtained with the three levels of encryption.

5.1. Optimized encryption level

In a bid to improve the security level of the system, we modified the positioning of the fingerprint image as compared to the standard for the video sequence. As an illustrative example for the second block of 16 images of this video sequence, we show in Fig. 4(c) how the fingerprint used for the encryption is obtained. This change of the fingerprint has for effect to modify the third encryption key for each block of images. Of course, alternative choices can be made for adding a key to the system.

5.2. Resistance of the encryption scheme against attack

Several plaintext-chosen attacks against our encryption scheme, such as those proposed in [9,10], were considered. Here we present the most dangerous attack for our system. Figure 4(d) shows the simulation result when the cipher knows the principle of our method and when the access to the system is granted to him or her. The qualitative differences shown above highlight clearly the robustness of our algorithm against this type of attacks.

#153431 - $15.00 USD Received 25 Aug 2011; accepted 19 Oct 2011; published 10 Nov 2011

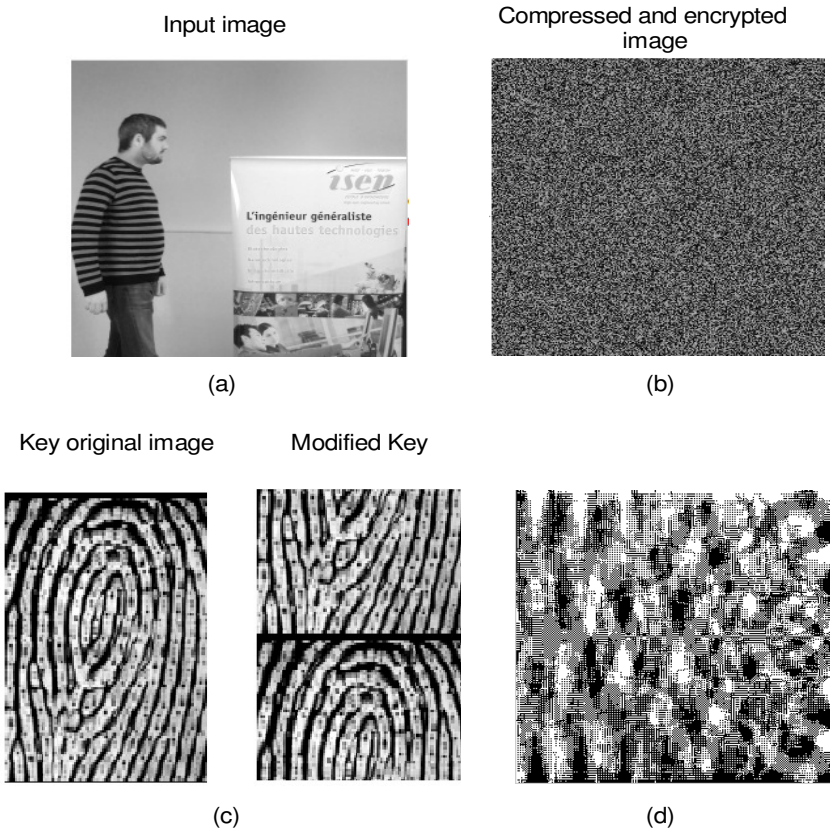


Fig. 4. Illustrating the three levels of encryption in our method: (a) the original target image, (b) the encrypted image with three levels of encryption (one of them is a fingerprint), (c) the modified fingerprint used for encryption of the second block of target images, and (d) simulation result when the cipher knows the principle of our method and when the access to the system is granted to him or her.

6. Concluding section

In summary, we have attacked the problem of finding an optimal way to multiplex spectrally multiple images as well as its implementation for simultaneous compression and encryption. This procedure uses DCT. Each DCT is filtered with low-pass filter whose size is related to the number of target images. Our idea is to compress the multiplexed file with a new encryption scheme consisting in a quantization of the filtered DCTs in different areas and then to encode them with an optimized number of bits. According to the above considerations, our results go beyond the well-known JPEG image compression standard. Our methodology offers tow levels of encryption. The increase of the level of encryption was realized by multiplying the multiplexed and quantized file with a doubly encrypted fingerprint. The merit of our approach is then that, due to the change of the fingerprint, by considering specifically the numbering of the block of target images, it enables us to resist a chosen-plaintext attack when the cipher knows the principle of our method and when the access to the system is granted to him or her. Owing to the qualitative nature of the above test, the end results confirming the effectiveness of our scheme appear conclusive. The concrete optical implementation of this procedure is, however, beyond the scope of this study.

Acknowledgment

Lab-STICC is Unité Mixte de Recherche CNRS 3192.

#153431 - $15.00 USD Received 25 Aug 2011; accepted 19 Oct 2011; published 10 Nov 2011