Enhanced System for image's compression and encryption by addition of biometric characteristics

A. Loussert, A. Alfalou, R. El Sawda, A. Alkholidi
ISEN-BREST Laboratory L@BISEN 20 rue cuirasse Bretagne C.S. 42807, 29228
Brest cedex 2, France
ayman.al-falou@isen.fr, alain.loussert@isen.fr

Abstract

In case of transmission of fast and protected information, it is important to carry out two operations distinctly. The first, is an operation of encryption, which aims to modify the compressed information to make them unreadable to whoever does not have the necessary authorization to see them (in this paper, we propose give this authorization by using a fingerprint image). The second is an operation of compression which consists in reducing the size of information to be transmitted, by removing redundant information of them. However, these two operations are often carried out separately, although they are strongly bound and one influences on the other. We propose, in this article, to carry out these two operations (compression and encryption) together with a new system able to amalgamate spectral information. This nondestructive spectral fusion, allowing at the same time the compression and the encryption of this information. This system is based on one hand on the rarity of similitude in two different fingerprints and on the second hand on the Discrete Cosine Transformation "DCT", a transformation used for a long time in JPEG compression.

Keyword: Signal and Image Processing, Image Compression/Decompression, Biometrics characteristics, Image Encryption/Decryption, Transmission, DCT, FFT.

1. Introduction

Since fifteen years, the scientific community have been more and more interested in methods of compression and encryption containing optical treatment. Indeed optics is very well adapted to process the two-dimensional and very big size data such as for example: images. That is essentially motivated by three points:
- speed of the optical treatment compared with the digital processing.
- the image to treat, is optical at the source.
- the fact that optics makes it possible to treat the whole image without resorting to an image division in zones. What makes it possible to avoid the very outstanding mosaic effect in the digital processing.

In this article, we were interested in the techniques of optical compression based on the Fourier transformation [1][2] and more particularly in the two techniques presented by the authors of the articles [3][4]. In the first one [3], the authors presented and validated a technique of optical compression based on bringing together of spectral images to compress. While, in the second one [4], the authors showed the possibility of implementing JPEG compression optically by realizing DCT transformation optically. These two articles show the possibility of amalgamating spectral information and realizing the DCT optically, two properties which we can also use to change the spectral distribution of an image and by consequence encrypt it. Indeed, one of the techniques of optical encryption of the images is based on the change of the spectral
distribution of the spectrum of the image to crypt by multiplying it with a mask of
random phase [5].

As previously shown, the optical compression and encryption of the images are often
separately realized and do not take into account the similarities which exist between the
two processes. However, in [6][7], the authors presented a method of optical encryption
based on a spectral change of the image to crypt with an optically compressed mask of
phase. The latter is realized by spectral amalgamating of several encryption keys using
the method of compression presented by [3]. These articles show that it is possible to
associate and to amalgamate the two processes of encryption and compression.

2- DCT transform and compression

Before detailing the principle of our system of compression and encryption of the
images, we will start by reminding, in this paragraph, the principle of the DCT
transformation [8][9].

DCT, largely used in image processing, is mathematically defined by the equation
(1). One of the properties of this transformation (which particularly interests us in this
article) is its capacity to regroup necessary relevant information for the rebuilding of an
image in the high-left corner of its spectrum. Indeed, this property has been used for a
long time as the core of the JPEG compression method [8][9]. The general diagram
allowing this selectivity based on DCT is presented figure (1).

\[
DCT_{pq} = \alpha_{p,q} \sum_{m,n=0}^{N-1} f(m,n) \cos \left( \frac{\pi(2m+1)p}{2N} \right) \cos \left( \frac{\pi(2n+1)q}{2N} \right)
\]

with:

\[
\alpha_{p} = \begin{cases} 
\frac{1}{\sqrt{N}} & p = 0 \\
\frac{1}{\sqrt{2N}} & 1 \leq p \leq M-1 
\end{cases}
\]

\[
\alpha_{q} = \begin{cases} 
\frac{1}{\sqrt{N}} & q = 0 \\
\frac{1}{\sqrt{2N}} & 1 \leq q \leq N-1 
\end{cases}
\]

\( f(x, y) \) is the input image.

\((m, n)\) and \((p, q)\) are respectively, the spatial and frequential coordinates.

This figure (1) shows in (a) the capacity of the DCT to regroup information in the
spectral field. Then, we proceed to the elimination of the information considered as
redundant (in the non necessary sense) by using a low-pass filter (figure 1-c),
elimination of information = compression). Thus, the compression ratio is strongly
related to the size of this filter and consequently on the quantity of kept information.
This step was optically realized by an assembly proposed by [4] and which made it
possible to obtain the DCT optically by using a simple convergent lens.
Figure 1. Bringing together and selection of information with a DCT: (a) an image with several levels of gray (256,256) pixels, (b) its transformation into "DCT", (c) low-pass filter, (d) the filtered spectrum containing desired information

3. Compression and Encryption system

In the previous paragraph, we showed that it was possible to compress an image optically by using the DCT, thereafter we will use and adapt this technique to realize a system able to compress an image while encrypting it.

Synoptic diagram

The compression of an image can be defined, as being the selection of relevant necessary information for a given application. However, to have a good compression ratio and a good quality of the image after compression, it is necessary to be careful to well select this relevant information. It is this principle which is used in JPEG compression. As in the latter, we will base ourselves on the DCT for regroup relevant information in order to propose an optical system of compression and encryption. Indeed, as it is explained in the article [4] the step of optical compression requires an operation of filtering after obtaining the spectrum of the image to compress, by the DCT figure (2-b).

After this filtering, we obtain a spectrum of size \( c \times c \) pixels with \( c \ll N \), \( N \) being original size of the image in pixels (figure 2-a). This results in releasing a big
part the spectral plan. Thus, we will use this property in order to insert other compressed spectra (for images taken from same or different sequences). While regrouping, in a nondestructive way, these various spectra in only one plane, we obtained the compression and the multiplexing of these various images. The number of images which can be multiplexed together depends on the size of the spectra to keep for each of them (knowing that it is necessary to find a compromise between the desired quality and size of spectrum to be filtered: because if one increases, the other will automatically decreases). This nondestructive regrouping has another consequence: it changes in a very marked way the distribution of the frequencies in the spectral plan which results in the encryption of the images together.

4. Enforced security level
In order to ensure a good level of encryption against any hacking attempt, we propose to change the rotation of the frequencies of the various images figure (2-c) before gathering them (here, we added the various spectra). This is to ensure that whoever does not have the necessary information on the number of spectra and their distributions in the spectral plane, will not be able to decrypt this information figure(2-d) quickly.

In fact, without the rotation of the image spectrum, the shape of the spectra obtained with the DCT is very characteristic and easily detectable thanks to the amplitude which
drops gradually while moving away from the high-left corner towards the low-right corner of the spectrum figure(3).

Figure 3. Characteristic representation of the DCT transformation: on horizontal axis, we have the number of pixels, on the vertical axis we have the DCT amplitude.

Figure 4. Synoptic diagram describing the system of compression and encryption using two security levels.
To solve this problem, we propose to multiply the spectrum, figure (4-d), thus obtained with a random mask or better with the spectrum of the corresponding fingerprint person figure(4). This multiplication aims to change the characteristic spectral distribution of the DCT figure(4-e).

Figure 5. Synoptic diagram describing the system of decompression and decryption using two security levels

After applying our method and transmitting compressed and encrypted information, the extraction of the images after reception is done by respecting the various steps of transmission method, but in the opposite direction. Thus, we will multiply the received image by the inverse of random mask or by the inverse fingerprint spectrum of the authorized corresponding person (figure 5), then we apply various rotations in the opposed direction, and finally we proceed to the inverse DCT to obtain our original images (figure 5).

5. Results

As an example, we have chosen a video sequence composed of two images figure(6-a). After applying our compression (and) encryption method, we obtained the result presented in ( figure 6-b). This compressed and encrypted image shows that we succeed in carrying out the two operations simultaneously (compression and encryption). In
(figure 6-c), we have the two output images using our compression and encryption system enforced using a random encryption Key.

**Figure 6.** (a) Input video sequence, (b) Compressed and encrypted image, (c) Estimated Output video sequence decrypted and decompressed

### 6. Conclusion
In this article, we proposed and showed, by the previous articles, that it was possible to use the DCT to jointly realize a compression and an encryption of the data by spectral fusion. These results use an all optical assembly making it possible to construct almost instantaneously all these operations allowing a very important gain in transmission time and an enhanced system by using biometric characteristics.
7. References


