Encryption-Compression of still images using the FMT transformation and the DES algorithm

Mohammed Benabdellah, Mourad Gharbi, Nourddine Zahid, Fakhita Regragui, Elhossine Bouyakhf.

Laboratoire d'Informatique, Mathématiques Appliquées, Intelligence Artificielle et Reconnaissance de Formes, Faculté des sciences de Rabat-Agdal.

Med_benabdellah@yahoo.fr, gharbi@fsr.ac.ma, zahid@fsr.ac.ma, regragui@fsr.ac.ma, bouyakhf@fsr.ac.ma.

Abstract

The development of the applications related to several fields of image processing requires the use of telecommunication and information technologies which evolved very quickly these last years. The compression and the encoding of data are two techniques whose importance believes in an exponential way in a myriad of applications.

The use of the data-processing networks, for the transmission and the transfer of the data, must satisfy two objectives which are: the reduction of the volume of information to free, the maximum possible, the public networks of communication, and the protection in order to guarantee a level of optimum safety.

For this we have proposed a new hybrid approach of encryption-compression, which is based on the DES encryption algorithm of the dominant coefficients, in a mixed-scale representation, of compression by the multi-scale transformation of Faber-Schauder. The comparison of this approach with other methods of encryption-compression, such as DCT-RSA and DCT-Partial-encryption, showed its good performance.

Keywords: *Compression of images, Encryption, Multi-scale Base of Faber-Schauder, Encryption- Compression, Mixed Visualisation, PSNR, Entropy.*

1. Introduction

The transmission and the transfer of images, in free spaces and on lines, are actually still not well protected. The standard techniques of encoding are not appropriate for the particular case of the images.

The best would be to be able to apply asymmetrical systems of encoding so as not to have a key to transfer. Because of the knowledge of the public key, the asymmetrical systems are very expensive in calculation, and thus a protected transfer of images cannot be envisaged. The symmetrical algorithms impose the transfer of the secrete key. The traditional methods of encoding images impose the transfer of the secret key by another channel or another means of communication [1,2].

The encryption algorithms per blocks applied to the images present two disadvantages: on the one hand, when the image contains homogeneous zones, all the identical blocks remain identical after the coding. For this, the encrypted image contains textured zones and the entropy of the image is not maximal. In addition, the techniques of encryption per blocks are not resistant to the noise. In fact, an error on a coded bit will propagate important errors on the running blocks entirely. The traditional methods encryption-compression have all tendencies to carry out techniques of encoding and compression in a disjoined way; this causes a problem during the decoding and the decompression stages, especially in the case of some application domains of real time type like the emission of images by satellites or the telemedicine where time is a paramount factor.

For a protected and reduced transfer of images, the algorithms of encoding images must be able to be combined with the algorithms of compression of images. The techniques of compression seek the redundancies contained in the images in order to reduce the quantity of information. On the other hand, the techniques of encryption aim to remove all the redundancies to avoid the statistical attacks, which is the famous problem.

In many methods of compression of images in grey level, the principal idea consists in transforming them so as to concentrate the piece of information (or the energy) the image in a small number of pixels. In general, the linear transformations are preferred because they allow for an analytic study. Among the most used transformations, we can quote that of the cosine which is at the base of the standard of JPEG compression [10].

The multi-scales transformations make it possible to take into account, at the same time, the great structures and the small details contained in an image; and from this point of view, they have similarities with the human visual system [11]. Laplacian pyramid algorithm of Burt-Adelson was the first example known, but it suffers in particular from the redundancy of the representation of data after transformation.

Mallat used the analysis of the wavelets to develop a fast algorithm of multi-scales transformation of images which has same philosophy as the diagram of the laplacian pyramid, but it is most effective

In this paper, we present the Faber-schauder Multi-scales Transformation (FMT), which carries out a change of the canonical base towards that of Faber-Schauder. We use an algorithm of transformation (and reverse transformation), which is fast and exact. Then, we present a method of visualization at mixed scales which makes it possible to observe, on only one image, the effect of the transformation. We notice a concentration of coefficients around the outline areas, and this is confirmed by the particular aspect of the histogram. If we encrypt only his significant coefficients we will only have a small disruption of the multi-scale image and, with a good conditioning, we will be able to decipher and rebuild the initial image without a big debasement.

In what follows, we describe the basic multi-scale construction of Faber-Schauder and we focus on the algorithm of transformation and reverse transformation. Then, we introduce the mixed-scale visualization of the transformed images and its properties. Then, we speak about the compression of images by the FMT, and we explain the encryption algorithms (DES). Lastly, we finish by the general diagram of the hybrid method of the introduced encryption-compression and the results found, after the application and comparison with the methods DCT-RSA and the DCT-Partial encryption.

2. Methods

2.1. The Faber-schauder multi-scale transformation

2.1.1. Construction of the Faber-Schauder multi-scale base

The multi-resolution analysis (11) of $L^2(R)$ is composed of vector spaces (V_j) of the linear continuous functions per pieces on the intervals $\left(\left[k2^j,(k+1)2^j\right]_{k\in Z}\right)$ such as:

$$.....V_2 \subset V_1 \subset V_0 \subset V_{-1} \subset V_{-2}.....$$

An unconditional base of each space V_j, called a canonical base, and is given by the family of functions:

$$\left|\phi_n^j(x) = 2^{-j}\phi\left(2^{-j}x - n\right)\right|_{n\in Z}$$

$$\phi(x) = \begin{cases} 1+ x \text{ si } -1 \le x \le 0 \\ 1- x \text{ si } 0 \le x \le 1 \\ 0 \quad \text{sinon} \end{cases}$$

Où

For a $2D$ signal, a multi-resolution analysis of $L^2(R)$ can be built from the tensorial products of spaces V_j : $V_j = V_j \times V_j$, and the canonical base of V_j are given by: $\left|\phi_{k,l}^j(x,y) = 2^{-j}\phi(2^{-j}x-k, 2^{-j}y-1)\right|_{k,l\in Z}$ With $\phi(x,y) = \phi(x)\times\phi(y)$.

The images are also sequences of numbers $f^0 = (f_{k,l})_{k,l\in Z}$ in $L^2(Z^2)$ representing the values of pixels. An image can be then associated with function f of V_0 given by:

$$f(x,y) = \sum_{k,l\in Z} f_{k,l}\phi^0_{k,l}(x,y)$$

.

For the construction of the Faber-Schauder base, we suppose the family of under spaces $(W_j)_{j\in Z}$ of $L^2(R^2)$ such as V_j is the direct sum of: V_{j+1} and W_{j+1} :

$$\begin{cases} V_j = V_{j+1} + W_{j+1} \\ W_{j+1} = V_{j+1} \times W_{j+1} + W_{j+1} \times V_{j+1} + W_{j+1} \times W_{j+1} \end{cases}$$

The space base W_{j+1} is given by: $\left(\psi^{j+1}_{1,k,l} = \phi^{j}_{2k+1} \times \psi^{j+1}_{l}, \psi^{j}_{2,k,1} = \psi^{j+1}_{k} \times \phi^{j}_{2l}, \psi^{j}_{3,k,1} = \psi^{j+1}_{k} \times \psi^{j+1}_{l}\right)_{k,l\in Z}$

And the unconditional base and Faber-Schauder multi-scale of $L^2(R^2)$ is given by: $(\psi^{m}_{1,k,l}, \psi^{m}_{2,k,l}, \psi^{m}_{3,k,l})_{k,l,m\in Z}$

A function of V_0 : $f(x,y) = \sum_{k,l\in Z} f^0_{k,l}\phi^0_{k,l}(x,y)$ Can be broken up in a single way according to V_1 and W_1 :

$$f(x,y) = \sum_{k,l\in Z} f^1_{k,l}\phi^1_{k,l}(x,y) + \sum_{k,l\in Z} \left[g^{11}_{k,l}\psi^{1}_{k,l}(x,y) + g^{21}_{k,l}\psi^{2}_{k,l}(x,y) + g^{31}_{k,l}\psi^{3}_{k,l}(x,y)\right]$$

The continuation f^1 is a coarse version of the original image f^0 (a polygonal approximation of f^0), while $g^1 = (g^{11}, g^{21}, g^{31})$ represents the difference in information between f^0 and f^1. g^{11} (respectively g^{21}) represents the difference for the first (respectively the second) variable and g^{31} the diagonal represents difference for the two variables.

The continuations f^1, g^1 can be calculated starting from f^0 in the following way:

$$\begin{cases} f^1_{k,l} = f^0_{2k,2l} \\ g^{11}_{k,l} = f^0_{2k+1,2l} - \frac{1}{2}(f^0_{2k,2l} + f^0_{2k+2,2l}) \\ g^{21}_{k,l} = f^0_{2k,2l+1} - \frac{1}{2}(f^0_{2k,2l} + f^0_{2k,2l+2}) \\ g^{31}_{k,l} = f^0_{2k+1,2l+1} - \frac{1}{4}(f^0_{2k,2l} + f^0_{2k,2l+2} + f^0_{2k+2,2l} + f^0_{2k+2,2l+2}) \end{cases}$$

Reciprocally one can rebuild the continuation f^0 from f^1 and g^1 by :

$$\begin{cases} f^0_{2k,2l} = f^1_{k,l} \\ f^0_{2k+1,2l} = g^{11}_{k,l} + \frac{1}{2}(f^1_{k,l} + f^1_{k+1,l}) \\ f^0_{2k,2l+1} = g^{21}_{k,l} + \frac{1}{2}(f^1_{k,l} + f^1_{k,l+1}) \\ f^0_{2k+1,2l+1} = g^{31}_{k,l} + \frac{1}{4}(f^1_{k,l} + f^1_{k,l+1} + f^1_{k+1,l} + f^1_{k+1,l+1}) \end{cases}$$

We thus obtain a pyramidal algorithm which, on each scale j, decompose (respectively reconstructed) the continuation f^j in (respectively from) f^{j+1} and g^{j+1}. The number of operations used in the algorithm is proportional to the number N of data, which is not invalid in the signal $(O(N))$ what makes of it a very fast algorithm. What is more, the operations contain only arithmetic numbers; therefore, the transformation is exact and does not produce any approximation in its numerical implementation [4].

The FMT Transformation has exactly the same principle of construction as that of Mallat except that the canonical base of the multi-resolution analysis is not an orthogonal base. This does

not prevent it from having the same properties in image processing as the wavelets bases. In addition, the FMT algorithm is closer to that of the laplacian pyramid, because it is very simple and completely discrete, what makes it possible to observe directly on the pixels the effects of the transformation. In short, the FMT transformation is a good compromise between the wavelets bases and the diagram of the laplacian pyramid [4].

2.1.2. Visualization of the transformed images by the FMT

The result of the wavelets transformation of an image is represented by a pyramidal sequence of images, which includes the differences in information between the successive scales (figure 1). However, we can consider the FMT multi-scale transformation as a linear application, from the canonical base to the multi-scale base, which distributes the information contained in the initial image in a different way. It is thus more natural to visualize this redistribution, in the multi-scale base, in only one image, as it is the case in the canonical base. The principle of the visualization of images in the canonical base consists in placing each coefficient at the place where its basic function reaches its maximum. The same principle is naturally essential for the multi-scale base (Figure 2) [4].

The image obtained is a coherent one which resembles an outline representation of the original image (Figure 3). Indeed, the FMT transformation, like some wavelets transformation, has similarities with the canny outlines detector [9], where the outlines correspond to the local maximum in the module of transformation. In fact, in the case of the FMT transformation, on each scale, the value of each pixel is given by the calculation of the difference with its neighbouring of the preceding scale. Thus the areas which present a local peak for these differences correspond to a strong luminous transition for the values of grey, while the areas, where those differences are invalid, are associated with an area, where the level of grey is constant [8].

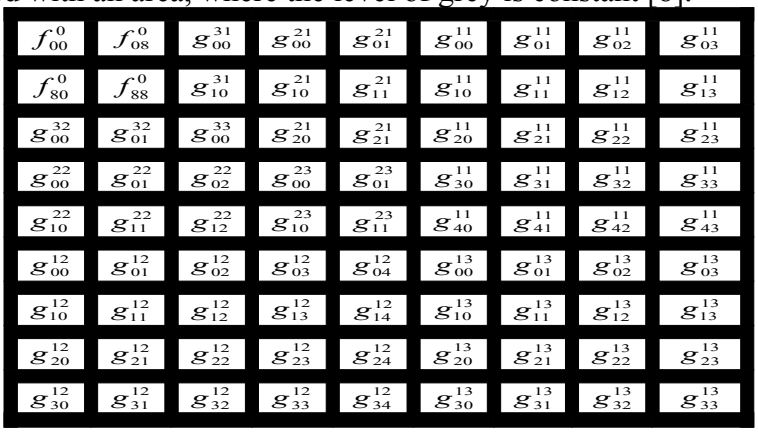


Figure 1: Representation on separated scales for 9×9 transformed image in the multi-scale base.

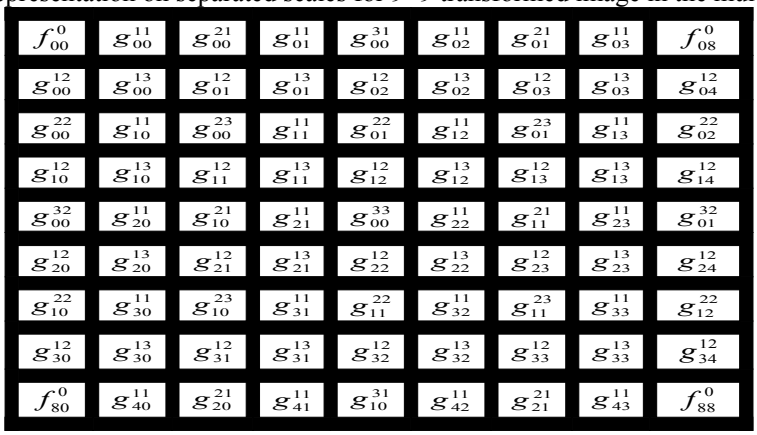
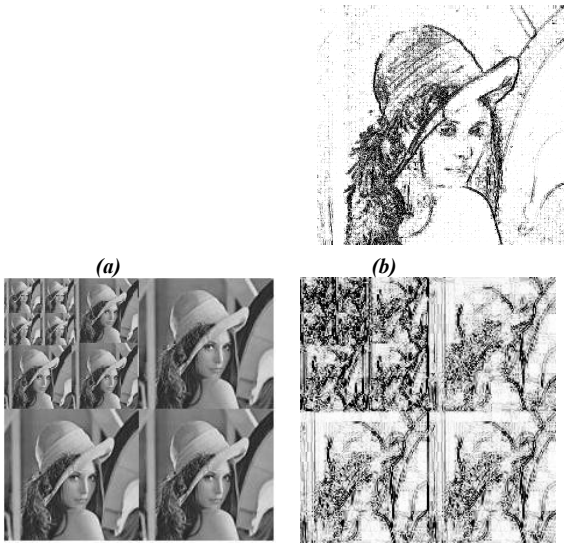


Figure 2: Representation on mixed scales, the coefficients are placed at the place where their basic functions are maximal.



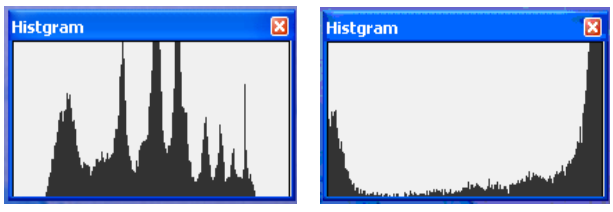
(a) *(b)* *(c)* *(d)*

Figure 3: Representation on mixed-scales (at the bottom) and on separate scales (at the top) of the image "Lena". Thecoefficients are in the canonical base in (a) and (c) and in the Faber-Schauder multi-scale base in (b) and (d).

2.1.3. Compression of images by FMT

We noted that the FMT transformation of the images gives, by the means of visualization on mixed scales, a good description of the outlines of the image. In fact, the result is more than only one image of the outlines because it contains exactly same information as that of the initial image and we can even find the original image by the reverse transformation. This leads us to raise the question to know if these multi-scale coefficients of the outline areas characterize the image completely. Theoretically, the answer is negative. Indeed, there are, in the case of the continuous wavelets transformations, some counter-examples of different functions which have the same outline points in their wavelet transformation [9]. Hence, we can only wish that the introduced debasement, if we do not hold account of the outline regions, remain unperceivable in the rebuilt image.

A worthwhile priority over the FMT transformation, which is also valid for the wavelets transformations, is the characteristic aspect observed in the histograms of transformed images: the number of coefficients for a given level of grey decreases very quickly, to practically fade away, when we move away from any central value very close to zero (figure 4). This implies that the information (or the energy) of the transformed image is concentrated in a small number of significant coefficients, confined in the outline region of the initial image. Therefore, the cancellation of other coefficients (almost faded away) only provokes a small disruption of the transformed image. In order to know the effect of such disruption in the reconstruction of the initial image one should calculate the matrix conditioning of the FMT transformation. In fact, if we have f = Mg where f is the initial image and g is the multi-scale image, then the conditioning of M (Cond(M) = $||M||.||M^{-1}|| \geq 1$) who checks : $||df||/||f|| \leq Cond(M)\ ||dg||/||g||$. This means that the relative variation of the restored image cannot be very important, with reference to the multi-scale image, if the conditioning is closer to 1 [4].



(a) *(b)*

Figure 4: Histograms of image « Lena »: (a) in the canonical base, (b) in the multi-scale base.

For the orthonormal transformations, the conditioning is always equal to 1; thus it is optimum. However, we can always improve the conditioning if we are able to multiply each column (or each line) by a well chosen scalar; in the case of a base changing, this pushes a change in the normalization of the base elements.

The obtained results (Figure 4) confirm that, in this case too, we get a good conditioning. Most generally, we have verified that we can practically eliminate between 90% and 99% of the multi-scale coefficients, without any remarkable debasement of the reconstructed image, and with a good ratio of noise signal (PSNR). The results are, obviously preferable, when they are not so textured.

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are mathematical measures which need the original image, before the compression, in order to measure the distortion [3]. The size of the images is MxN, while the pixels coordinates are (m,n).

If we compare the performances of the FMT transformation with the standards method of compression, (JPEG), we will verify that we can reach good results of compression, without debasing the image. What is more, those results are obtained when applying the multi-scale transformation to the whole image, while the DCT transformation, which is the basis of the JPEG method, is not effective when applied to reduced blocks pixels (generally applied to blocks of size 8×8 pixels) [6], what involves the appearance of the blocks of artifacts on the images when the compression ratio is high [5]. This phenomenon of artefacts blocks is not common in the FMT transformation (see applications).

2.2. The encryption algorithm DES

The D.E.S algorithm **(**Data Encryption Standard) is born in 1975 following a request from I.B.M. in 1960 for its program from research on data-processing coding [13]. At the beginning, the specialists in the N.S.A. (National Security Agency) break teeth thus I.B.M. above is constrained to use it in a form simpler than envisaged. The use of the D.E.S. spreads then little by little in the American administrations [1]. Since, the D.E.S. is given on level every approximately 5 years to face the increasing power of the computers which put it in danger [12].

The message, above all, converted into binary, is cut out in blocks B_i of 64 bits. The key K, it, comprises 56 bits. For each block B_i, one applies the following algorithm [7]:

1) One carries out an initial permutation of the bits of the block B_i. One calls G_0 and D_0 then the parts of 32 bits right-hand side and left of the block obtained.
2) One repeats 16 times the following procedure :
    a. $G_i = D_{i-1}$
    b. $D_i = G_{i-1}$ XOR $f(D_{i-1}, K_i)$ (XOR is represented by + on the diagram below) where K_i is a block of 48 bits of the key K, and F a function successively made up of an expansion of bits, a XOR, a reduction of bits, and a permutation of bits.
3) One recomposes a B'16 block in “resticking” D16 and G16 in this order.
4) One carries out the opposite permutation of the initial permutation 1).

Here a diagram summarizing the various parts of the algorithm (Figure 5)[2]:

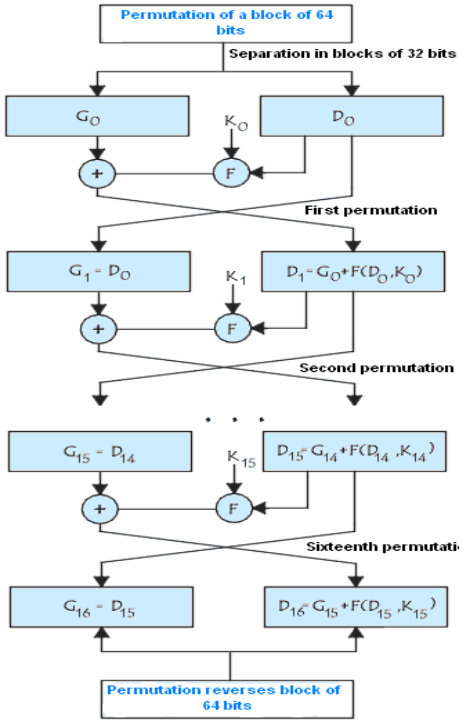


Figure 5: Diagram of Encryption DES.

2.3. The schema of principle of the encryption-compression suggested approach

The essential idea is to combine the compression and the encryption during the procedure. It is thus a question of immediately applying the encryption to the coefficients of the preserved compression, after the application of transformed FMT to visualization in mixed scales. Our general diagram is given on figure 6 as follow:

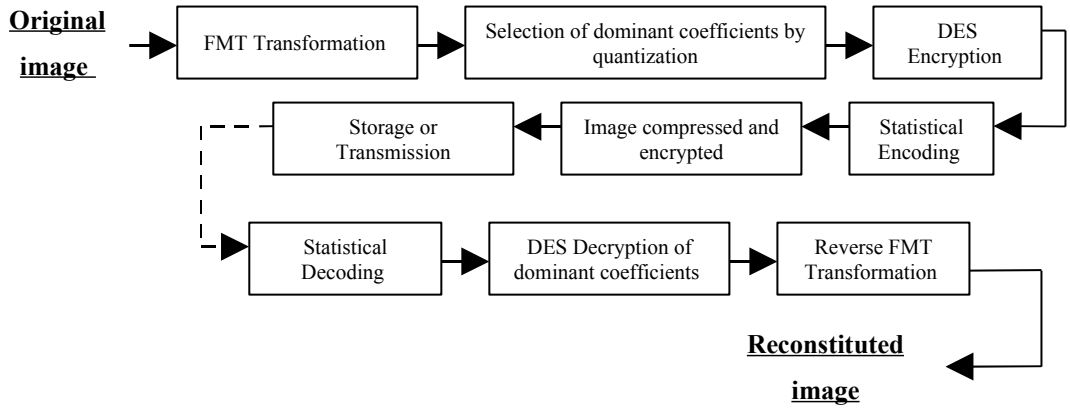


Figure 6: General diagram of the encryption – compression approach.

It consists in carrying out an encryption after the stage of quantization and right before the stage of entropic coding. To restore the starting information, one decodes initially the quantified coefficients of the FMT matrix by the entropic decoder. Then, one deciphers them before the stage of quantization. Lastly, one applies the RFMT (Reverse FMT) to restore the image.

The principal advantages of our approach are the flexibility and the reduction of the processing time during the coding and decoding operations. Indeed, by our method, one can vary the processing time according to the desired degree of safety.

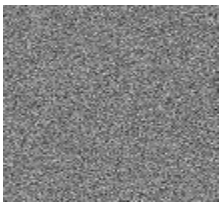
3. Results

3.1. Applications

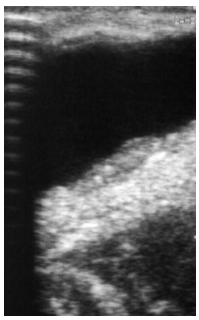
The results obtained after the application of our method on the images (Lena), (echo graphic image), (Flower) are given as follows:

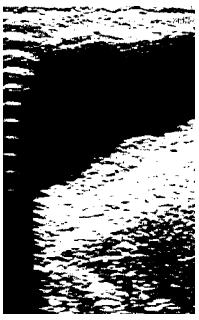

Lena's original image

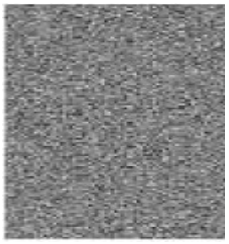

Representation in mixed scales (FMT)


Compressed and encrypted image


Reconstituted image


Echographic's original image

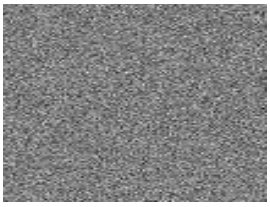

Representation in mixed scales (FMT)


Compressed and encrypted image


Reconstituted image


Flower's Original image


Representation in mixed scales (FMT)


Compressed and encrypted image


Reconstituted image

3.2. Comparison

The comparison is carried out, after the application of the methods of compression-encryption: DCT-RSA, DCT-partial encryption and our method FMT-DES on the image "Lena", "echographic images" and "Flower". It should be noted that the resolution of the images is 256×256 dpi, and the processor used is Intel Pentium4 for a rate equalizes 3.2 GHz. The results obtained are given on table 2 following:

	Entropy of original image	DCT-RSA		DCT- Part. Encryt..		FMT-DES	
		PSNR (dB)	Entropy of reconstituted image	PSNR (dB)	Entropy of reconstituted image	PSNR (dB)	Entropy of reconstituted image
Lena	7.589	35.023	7.033	35.351	7.083	34.807	6.996
Echo. image	8.351	41.146	7.814	41.478	7.811	40.928	7.799
Flower	8.988	32.414	8.423	32.759	8.478	32.205	8.357

Table 2: Comprarison of FMT-DES with DCT-RSA and DCT-Partial Encryption.

For applied the encryption methods RSA and Partial encryption, we propose to quantify only the quantified frequential coefficients relating to the low frequencies. By quantifying all the coefficients of the first column and the first line of the blocks 8×8, the size of the crypto-compressed image is closer to the size of the original image. In this case we lose in ompression ratio. It should be noted that the DCT-RSA and DCT-Partial encryption require a long computing time, while these methods depend on the coefficients selected before the realization of the encryption. It leads to the appearance of the artefact blocks on the reconstituted images when the compression ratio is high. This Phenomenon of artefact blocks is not known any more in the FMT

transformation. For the DCT-Partial encryption and DCT-RSA methods, we kept the coefficients of the first line and the first column, after the application of the DCT transformation on each block of 8×8 pixels. In general, the two methods give a less visual quality compared to the method FMT-DES.

The principal advantages of our approach are the flexibility and the reduction of the processing time, which is proportional to the number of the dominant coefficients, at the time of the operations of encryption and decryption. Indeed, by our method, one can vary the processing time according to the desired degree of safety.

4. Conclusion

We presented an approach of encryption-compression which is based on the (FMT) multi-scale transformation, stemming from the expression of the images in the Faber-Schauder base and the encryption algorithm (DES). The FMT transformation is distinguished by its simplicity and its performances of seclusion of the information in the outline regions of the image. The mixed-scale visualization of the transformed images allows putting in evidence its properties, particularly, the possibilities of compression of the images and the improvement of the performances of the other standard methods of compression as JPEG and GIF. The encryption algorithm (DES) leaves, in the stage of compression, homogeneous zones in the high frequencies.

The algorithm of encoding D.E.S. is strongly threatened by the computing powers of the computers. It is indeed not impossible to sweep the majority of the keys to break the code. A new system, the A.E.S. (Advanced Encryption Standard) is designed to replace it.

The comparison of our method with the methods: DCT-RSA and DCT-Partial encryption showed well its good performance.

Finally, we think of using hybrid methods in compression and encryption by mixture of data and setting up a encrypt analysis of the proposed approach.

References

[1] A.Sinha and K.Singh, *A technique for image encryption using digital signature*, Optics Communications, 218 : 229-234, 2003.
[2] C.C.Chang, M.S.Hwang and T-S Chen, *A new encryption algorithm for image cryptosystems*, Journal of Systems and Software, 58 : 83-91, 2001.
[3] G.Granland, M.Kocher and C.Horne, *Traitement numérique des images*, sous la direction de Murat Kunt, Press Polytechniques Universitaires Romande, Paris, CENT-ENST, 1993.
[4] H.Douzi, D.Mammass and F.Nouboud, *Amélioration de la Compression des Images par la Transformation Multi-Echelle de Faber-Schauder*, Vision Interface '99, Trois-Rivières, Canada, May 19-21, 1999.
[5] M.Benabdellah, M.Gharbi, N.Lamouri, F.Regragui, E. H. Bouyakhf, *Adaptive compression of images based on Wavelets*, International Georgian Journal of Computer Sciences and Telecommunications, No.1(8), pp.32-41, http://gesj.internet-academy.org.ge/gesj_articles/ 1172.pdf, 31 March 2006.
[6] N.Ahmed, T.Natarjan and K.R.Rao, *Discrete Cosine Transform*, IEEE Trans. On Computers, Vol. C-23, pp. 90-93. January 1974.
[7] R.Norcen, M.Podesser, A.pommer, H.P.schmidt and A.Uhl, *Confidential storage and transmission of medical image data*, Computers in Biology and Medicine, 33 : 277-292, 2003.
[8] S.G.Mallat, *Atheory for multiresolution signal decomposition: the wavelet representation*, IEEE Trans, on Pattern Analysis and Machine Intelligence, Vol 11, No 7, July 1989.
[9] S.G.Mallat and S.Zhong, *Characterization of Signals from Multiscale Edges*, IEEE Trans. On Pattern Analysis and Machine Intelligence, Vol 14, No 7, July 1992.
[10] X.Marsault, *Compression et Cryptage des Données Multimédias*, Hermes, 1997.
[11] Y.Meyer, *Ondelettes sur l'intervalle*, Cahiers des mathématiques de la décision No 9020, CEntre de REcherche de MAthématiques de la DEcision (CERE-MADE), 1992.
[12] O. Frider, *Cryptographie : Advanced Encryption System-AES*, ETR6, Ecole d'ingénieurs de Canoon de Vaud, tcom, Mai 2004.
[13] Alberdi Ion, Delaplac Mathieu, Gabes Jean, *La sécurité du 802.11 (Wifi), Et son implication dans l'infrastructure des sociétés*, 20 janvier 2005.

Article received: 2006-08-18