Applied Mathematical Sciences, Vol. 1, 2007, no. 45, 2203 - 2219

Encryption-Compression of Images Based on FMT and AES Algorithm

Mohammed Benabdellah, Mohammed Majid Himmi, Noureddine Zahid*, Fakhita Regragui and El Houssine Bouyakhf

Université Mohamed V - Agdal
LIMIARF - Faculté des sciences
* LCS - Faculté des sciences
4 Avenue Ibn Battouta
B.P. 1014 RP, Rabat - Maroc

Abstract

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 AES encryption algorithm of the dominant coefficients, in a mixed-scale representation, of compression by the Faber-schauder Multi-scale Transform (FMT). The comparison of this approach with other methods of encryption-compression, such as Quadtree-AES and DCT-partial-encryption, showed its good performance.

Keywords: Encryption, the multi-scale base of Faber-Schauder, Encryption-compression, Mixed Visualisation, PSNR.

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 [2].

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 ex-pensive 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].

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 [7].

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 [13]. On the other hand, the techniques of encryption aim to remove all the redundancies to avoid the statistical attacks, which is the famous problem [11].

In many methods of compression of images in grey level, the principal idea consists in transforming them so as to concentrate the piece of in-formation (or the energy) the image in a small number of pixels [3]. In general, the linear transformations are preferred because they allow for an analytic study [13]. Among the most used transformations, we can quote that of the cosine which is at the base of the standard of JPEG compression [15].

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 [8]. Laplacienne 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 [9].

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 laplacianne pyramid, but it is most effective [10] [12].

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 con-firmed 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 re-verse 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 ex-plain the encryption algorithms (AES). 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 Quadtree-AES and the DCT-partial encryption.

2 Methods

2.1 Faber-schauder Multi-scale Transform

2.1.1 Construction of the Faber-Schauder multi-scale base

The Faber-Schauder wavelet transform is a simple multiscale transformation with many interesting properties in image processing. In these properties, we advertise multiscale edge detection, preservation of pixels ranges, elimination of the constant and the linear correlation...
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} [4]:

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

The space base W_{j+1} is given by:
$(\psi^{j+1}_{1,k,l} = \phi^j_{2k+1} \times \psi^{j+1}_l, \psi^j_{2,k,l} = \psi^{j+1}_k \times \phi^j_{2l}, \psi^j_{3,k,l} = \psi^{j+1}_k \times \psi^{j+1}_l)_{k,l\in Z}$
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 [4]:
$f(x,y) = \sum_{k,l\in Z} f^1_{k,l}\phi^1_{k,l}(x,y) + \sum_{k,l\in Z}[g^{11}_{k,l}\psi^1_{k,l}(x,y) + g^{21}_{k,l}\psi^2_{k,l}(x,y) + g^{31}_{k,l}\psi^3_{k,l}(x,y)]$.
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 [5].
The continuations f^1 and g^1 can be calculated starting from f^0 in the following way:

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

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

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

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} [17]. 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 [16]. What is more, the operations contain only arithmetic numbers; therefore, the transformation is exact and does not produce any approximation in its numerical implementation [14].

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 [17]. This does not prevent it from having the same properties in image processing as the wavelets bases [18]. 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 [19].

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) [19].

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) [17].

f_{00}^{0}	f_{08}^{0}	g_{00}^{31}	g_{00}^{21}	g_{01}^{21}	g_{00}^{11}	g_{01}^{11}	g_{02}^{11}	g_{03}^{11}
f_{80}^{0}	f_{88}^{0}	g_{10}^{31}	g_{10}^{21}	g_{11}^{21}	g_{10}^{11}	g_{11}^{11}	g_{12}^{11}	g_{13}^{11}
g_{00}^{32}	g_{01}^{32}	g_{00}^{33}	g_{20}^{21}	g_{21}^{21}	g_{20}^{11}	g_{21}^{11}	g_{22}^{11}	g_{23}^{11}
g_{00}^{22}	g_{01}^{22}	g_{02}^{22}	g_{00}^{23}	g_{01}^{23}	g_{30}^{11}	g_{31}^{11}	g_{32}^{11}	g_{33}^{11}
g_{10}^{22}	g_{11}^{22}	g_{12}^{22}	g_{10}^{23}	g_{11}^{23}	g_{40}^{11}	g_{41}^{11}	g_{42}^{11}	g_{43}^{11}
g_{00}^{12}	g_{01}^{12}	g_{02}^{12}	g_{03}^{12}	g_{04}^{12}	g_{00}^{13}	g_{01}^{13}	g_{02}^{13}	g_{03}^{13}
g_{10}^{12}	g_{11}^{12}	g_{12}^{12}	g_{13}^{12}	g_{14}^{12}	g_{10}^{13}	g_{11}^{13}	g_{12}^{13}	g_{13}^{13}
g_{20}^{12}	g_{21}^{12}	g_{22}^{12}	g_{23}^{12}	g_{24}^{12}	g_{20}^{13}	g_{21}^{13}	g_{22}^{13}	g_{23}^{13}
g_{30}^{12}	g_{31}^{12}	g_{32}^{12}	g_{33}^{12}	g_{34}^{12}	g_{30}^{13}	g_{31}^{13}	g_{32}^{13}	g_{33}^{13}

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

f_{00}^{0}	g_{00}^{11}	g_{00}^{21}	g_{01}^{11}	g_{00}^{31}	g_{02}^{11}	g_{01}^{21}	g_{03}^{11}	f_{08}^{0}
g_{00}^{12}	g_{00}^{13}	g_{01}^{12}	g_{01}^{13}	g_{02}^{12}	g_{02}^{13}	g_{03}^{12}	g_{03}^{13}	g_{04}^{12}
g_{00}^{22}	g_{10}^{11}	g_{00}^{23}	g_{11}^{11}	g_{01}^{22}	g_{12}^{11}	g_{01}^{23}	g_{13}^{11}	g_{02}^{22}
g_{10}^{12}	g_{10}^{13}	g_{11}^{12}	g_{11}^{13}	g_{12}^{12}	g_{12}^{13}	g_{13}^{12}	g_{13}^{13}	g_{14}^{12}
g_{00}^{32}	g_{20}^{11}	g_{10}^{21}	g_{21}^{11}	g_{00}^{33}	g_{22}^{11}	g_{11}^{21}	g_{23}^{11}	g_{01}^{32}
g_{20}^{12}	g_{20}^{13}	g_{21}^{12}	g_{21}^{13}	g_{22}^{12}	g_{22}^{13}	g_{23}^{12}	g_{23}^{13}	g_{24}^{12}
g_{10}^{22}	g_{30}^{11}	g_{10}^{23}	g_{31}^{11}	g_{11}^{22}	g_{32}^{11}	g_{11}^{23}	g_{33}^{11}	g_{12}^{22}
g_{30}^{12}	g_{30}^{13}	g_{31}^{12}	g_{31}^{13}	g_{32}^{12}	g_{32}^{13}	g_{33}^{12}	g_{33}^{13}	g_{34}^{12}
f_{80}^{0}	g_{40}^{11}	g_{20}^{21}	g_{41}^{11}	g_{10}^{31}	g_{42}^{11}	g_{21}^{21}	g_{43}^{11}	f_{88}^{0}

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

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 [18], 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

neighboring 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 [11].

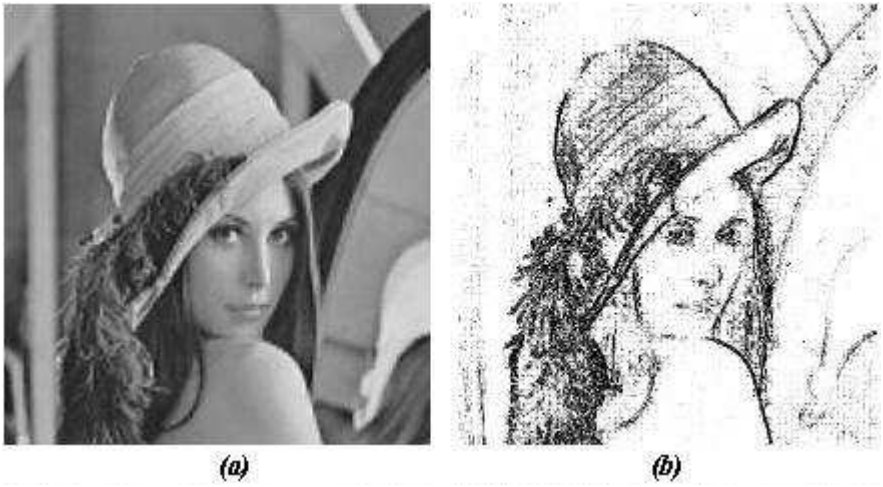

Figure 3: Representation on mixed-scales and on separate scales of the image "Lena". The coefficients are in the canonical base in (a) and in the Faber-Schauder multi-scale base in (b)

2.2 Compression of images by FMT

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)[11]. 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 [14] . Therefore, the cancelation 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 [5]. 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 : $||\delta f||/||f|| \leq Cond(M)||\delta g||/||g||$. 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 [13].

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 [4]. The obtained results (Figure 5) confirm that, in this case too, we

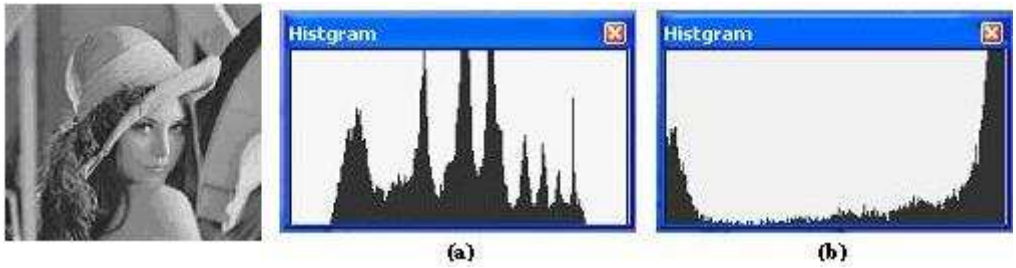

Figure 4: Histograms of image " Lena ": (a) in the canonical base, (b) in the multi-scale base

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)[16]. The results are, obviously preferable, when they are not so textured (Figure 6).

The Mean Square Error (MSE) [17] 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 $M \times N$, while the pixels coordinates are (m,n).

The MSE measures the square of difference in each point, between the original image and the compressed one [12]:
$MSE = 1/M.N \sum_{n=1}^{N} \sum_{m=1}^{M} (I_{original}(m,n) - I_{Compressed}(m,n))^2$

The PSNR measures the signal ratio of noise [14]:
$PNSR = 10Log_{10}(N_g^2/MSE)(dB)$

Here N_g represents the maximal grey level that a pixel can take. For the coded images on 8 bits, for example, $N_g = 255$ [18].

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), what involves the appearance of the blocks of artifacts on the images when the compression ratio is high [6]. This phenomenon of artefact blocks is not common in the FMT transformation (Figure 5).

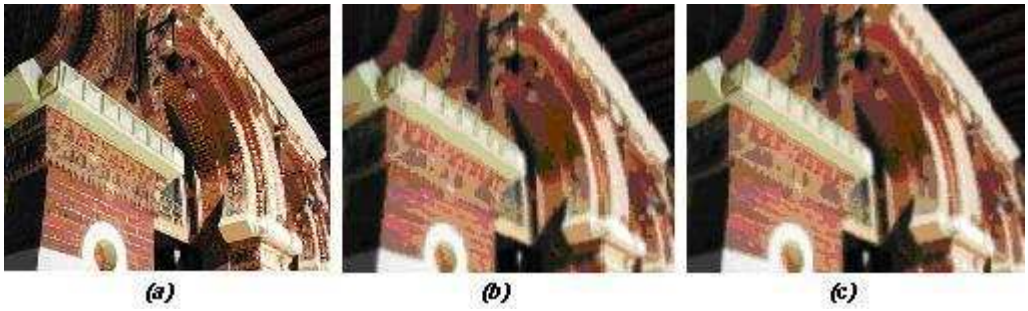

Figure 5: Debasement by FMT. The percentage of eliminated coefficients: (a) Arches's original image, (b) 90%, (c) 93%. Debasement by FMT. The percentage of eliminated coefficients: (a) Arches's original image, (b) 90%, (c) 93%

Images	Eliminated coefficients	PSNR
Arches	86%	54.265
Echographic image	91%	41.478
Lena	90%	34.941
Flower	90%	32.759

Figure 6: The percentage of eliminated coefficients and the PSNR of some images reconstituted

2.3 The encryption algorithm AES

AES is the acronym of Advanced Encryption Standard, creates by Johan Daemen and Vincent Rijmen. It is a technique of encoding to symmetrical key. It is the result of a call to world contribution for the definition of an algorithm of encoding, call resulting from the national institute of the standards and technology of the government American (NIST) in 1997 and finished in 2001. this algorithm provides a strong encoding and was selected by the NIST like normalizes federal for the data processing (Federal Information Processing Standard) in November 2001 (FISP-197), then in June 2003, the American government (NSA) announced that AES was sufficiently protected to protect the information classified up to the level TOP SECRET, which is the most level of safety defined for information which could cause "exceptionally serious damage" in the event of revelations with the public. Algorithm AES uses one the three lengths of key of coding (password) following: 128, 192 or 256. Each

size of key of encoding uses a slightly different algorithm, thus the higher sizes of key offer not only one greater number of bits of jamming of the data but also an increased complexity of the algorithm [1].

This algorithm always preserves the high level of safety proposed by DES; indeed the process is al-ways based on a function of expansion E, boxes of substitutions S, called on the level of the diversification of key K; moreover, the process always preserves the principle of the stages at the moment of the stage of expansion. The innovation brought by the AES is noted on the level of the size of the secret key as well as the size of the data treated in entry; precisely we pass from a key of coding of size 64 bits (8 bytes) for the case of worms a key of size doubles 128 bits (16 bytes) for the AES [7]. The size of the data with crypter is as notably larger as that of since we pass from 64 bits towards 128 bits. Moreover, as for DES, the AES is a cryptographic system with secret key; what makes the operation of Encrypting-decrypting rather light . The size of the data treated by the AES (16 bytes) gives us the possibility well of exploiting the supporting algorithm in applications of the data files of large size [2].

Cryptography with symmetrical algorithms uses the same key for the processes of Encrypting and Decrypting; this key is generally called "secret" (in opposition to "private") because all the safety of the unit is directly related to the fact that this key is known only by the shipper and the recipient [19]. Symmetrical cryptography is very much used and is characterized by a great speed (encrypting with the flight, "one-the-fly"), implementations as well software (Krypto Zone, Firewalls software Firewall-1 type and VPN-1 of Checkpoint) that hardware (dedicated charts, processors crypts 8 to 32 bits, c) what accelerates the flows clearly and authorizes its massive use. This type of cryptography usually functions according to two different processes, encrypting per blocks and the encrypting of "stream" (uninterrupted). Algorithm AES is iterative (Figure 7). It can be cut out in 3 blocks:

- Initial Round. It is the first and the simplest of the stages. It counts only one operation : Add Key Round.

- N Rounds. N is the iteration count. This number varies according to the size of the key used. 128 bits for N=9, 192 bits for N=11, 256 bits for N=13. This second stage consists of N iterations comprising each one the four following operations : Sub Bytes, Rows Shift, Mix Columns, Add Key Round.

- Final Round. This stage is almost identical to the one of the N iterations of the second stage. The only difference is that it does not comprise the operation Mix Columns.

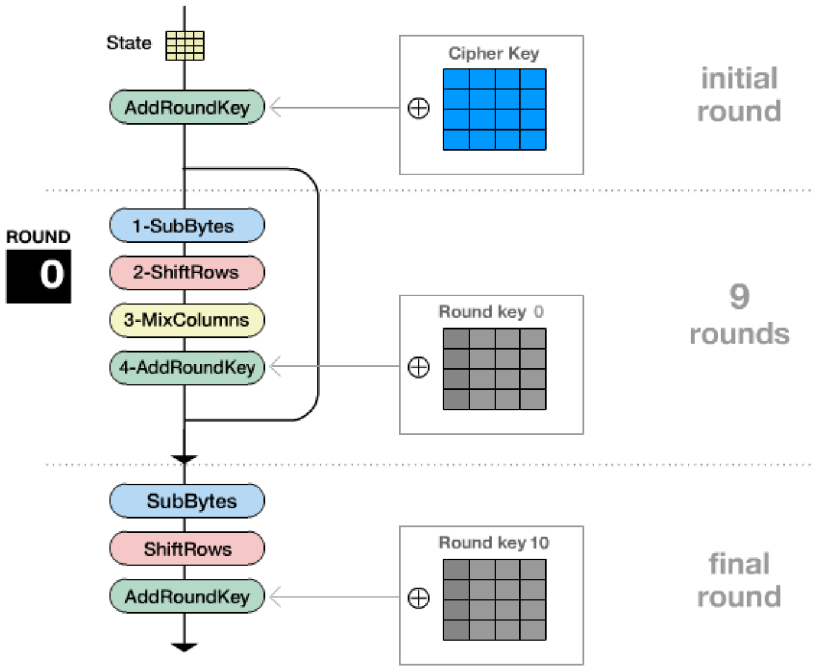

Figure 7: Diagram block of the algorithm AES, version 128 bits

2.4 Principle schema 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 8 as follow:

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 IFMT (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.

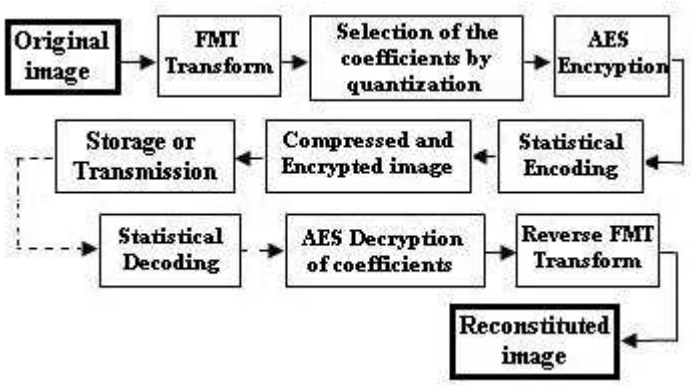

Figure 8: General diagram of the encryption-compression approach

3 Results

3.1 Applications

The results obtained after the application of method FMT-AES on the images (Lena), (echo graphic image), (Flower) and (arches) are given as follows :

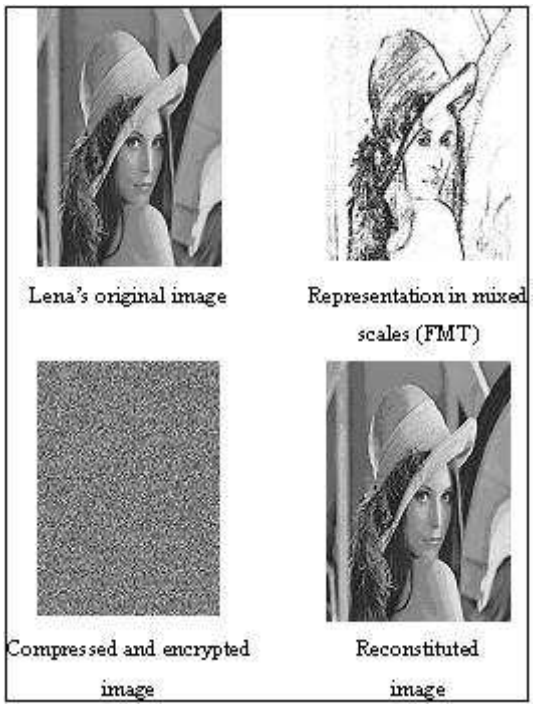

Figure 9: The stages after application of FMT-AES method on Lena's image

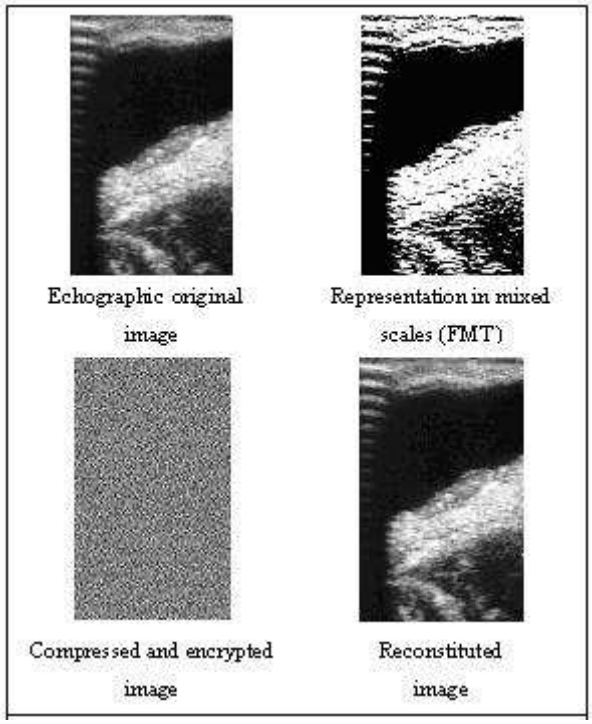

Figure 10: The stages after application of FMT-AES method on Echographic's image

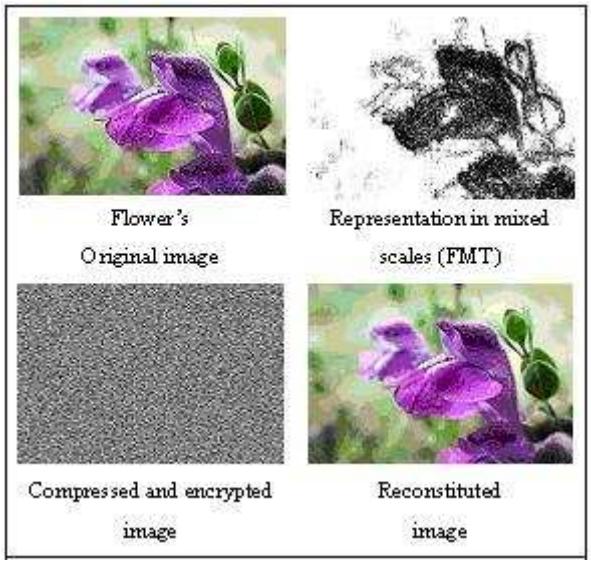

Figure 11: The stages after application of FMT-AES method on Flower's image

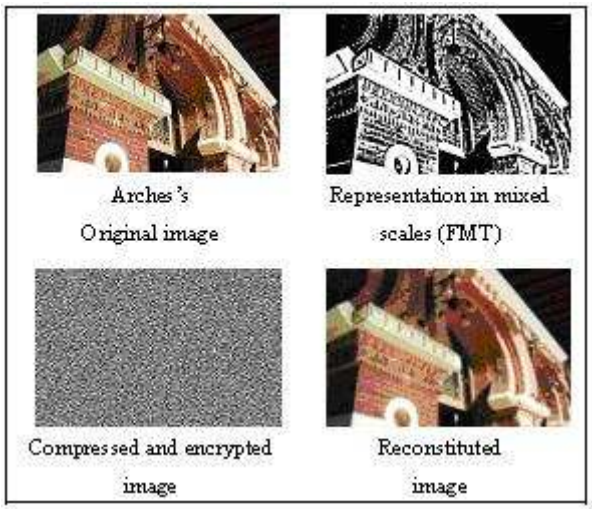

Figure 12: The stages after application of FMT-AES method on Arches's image

3.2 Comparison

The comparison is carried out, after the application of the methods of compression-encryption: Quadtree-AES and DCT-partial encryption and our method FMT-AES, on the image "Lena", "Echographic image", "Arches" 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 3.2Ghz. The results obtained are given on Figure 14 following: The method of partial encryption proposes 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 compression ratio. It should be noted that the Quadtree-AES and the DCT-Partial encryption methods require a very long computing time, while these methods depend on the coefficients selected before the realization of the encryption.

DCT-Partial encryption 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 method, 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-AES.

The principal advantages of our approach are the flexibility and the reduction of the processing time, which is proportional to the number of the

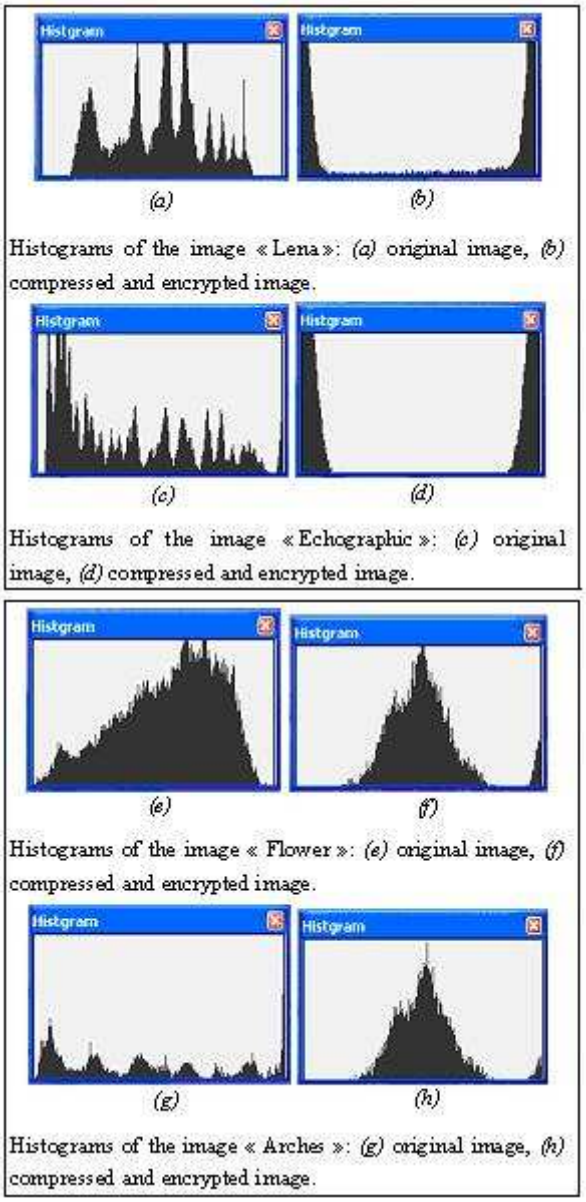

Figure 13: Diagrams of originals images and compressed and encrypted images

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.

	Entropy of original image	Quality of original image	Quadtree-AES				DCT-Partial Encryption				FMT-AES			
			PSNR (dB)	E. of R.I.	R.Q.	C.T. (s)	PSNR (dB)	E. of R.I.	R.Q.	C.T. (s)	PSNR (dB)	E. of R.I.	R.Q.	C.T. (s)
Lena	7.589	0.91	35.083	7.015	0.88	4.32	35.351	7.033	0.89	9.95	34.879	6.981	0.89	3.15
Echo. image	8.351	0.84	41.206	7.797	0.81	4.11	41.478	7.811	0.81	9.72	41.001	7.785	0.82	2.91
Arches	8.782	0.92	53.989	8.213	0.88	4.53	54.265	8.271	0.89	11.15	53.791	8.181	0.89	3.37
Flower	8.988	0.93	32.479	8.405	0.90	4.61	32.759	8.478	0.90	11.23	32.289	8.340	0.91	3.44

Figure 14: Comparison of our method "FMT-AES" with the methods "Quadtree-AES" and "DCT-partial encryption. E.of R.I. : Entropy of Reconstituted Image. R.Q.: Quality of Reconstituted Image. C.T.: Calculated Time

4 Conclusion

We presented an approach of compression- encryption which is based on the Faber-Schauder Multi-scale Transformation, stemming from the expression of the images in the Faber-Schauder base and the AES encryption algorithm. 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 AES encryption algorithm leaves, in the stage of compression, homogeneous zones in the high frequencies. It is approximately twice faster to calculate (in software) and approximately 10^{22} times surer (in theory) that DES. However, even if it is easy to calculate, it is not it enough to be taken into account in the current Wi-Fi charts. The standard 802.11i will thus require a renewal of the material to be able to make safe the networks of transmissions without wire.

The comparison of FMT-AES method with the methods: Quadtree-AES 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] Laurent GARDES, Estimation d'une fonction quantile extrême, *Thèse de Doctorat* Université Montpellier II, 06 Octobre 2003.

[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, A theory 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] Tommi A. Vuorenmaa, A Multiresolution Analysis of stock Market Volatility Using Wavelet Methodology, *Licentiate Thesis*, Department of Economics, University of Helsinki, September 21, 2004.

[11] X.Marsault, Compression et Cryptage des Données Multimédias, *Hermes*, 1997.

[12] Y.Meyer, Ondelettes sur l'intervalle, Cahiers des mathématiques de la décision No 9020, *CEn-tre de REcherche de MAthématiques de la DEcision (CERE-MADE)*, 1992.

[13] 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, 31 March 2006.

[14] M. Benabdellah, N. Zahid, F. Regragui, E. H. Bouyakhf, Encryption-Compression of Echographic images using FMT transform and DES algorithm, *International INFOCOMP Journal of Computer Science*, March 2007, will be published in the following number.

[15] M. Benabdellah, M. Gharbi, F. Regragui, E. H. Bouyakhf, An approach for choosing reference images in video compression, *5émes journées d'optique et de traitement de l'information (OPTIQUE'06)*, INPT-Rabat, Maroc, 19-20 avril 2006.

[16] M. Benabdellah, M. Gharbi, F. Regragui, E. H. Bouyakhf, Méthode hybride de crypto-compression des images par la FMT et l'AES, *Journée d'étude de Recherche et Pédagogie (JRP'06)*, Faculté des sciences benMsik-Casa, Maroc, 12 juillet 2006.

[17] M. Benabdellah, M. Gharbi, N.Zahid, F. Re-gragui, E. H. Bouyakhf, Crypto-compression des images échographiques par la transformation de Faber-Schauder et l'algorithme DES, *Colloque International sur l'Informatique et ses Applications (IA'2006)*, ENSAO- Oujda, 31 octobre, 1 et 2 Novembre 2006.

[18] M. Benabdellah, M. Gharbi, N.Zahid, F. Re-gragui, E. H. Bouyakhf, Crypto-compression des images médicales par la transformation Multi-échelle de Faber-Schauder et l'algorithme AES, *2ème journées d'études Algéro-Francaises en imagerie médicale (JETIM'06)*, USTHB (Alger) et Corne d'or (Tipaza), Algérie, 21-22 Novembre 2006.

[19] M. Benabdellah, M. Gharbi, N.Zahid, F. Regragui, E. H. Bouyakhf, Crypto-compression des images fixes par la FMT et l'AES, *9th Magrebian Conference on Software Engineering and Artificial Intelligence (MCSEAI'06)*, Agadir, Morocco, 7-9 December 2006.

Received: May 18, 2007