IADIS International Journal on Computer Science and Information Systems
Vol. 4, No. 1, pp. 30-41
ISSN: 1646-3692

Encryption-Compression Method of Images

Benabdellah Mohammed[1], Gharbi Mourad[1], Zahid Nourddine[2], Regragui Fakhita[1], Bouyakhf El Houssine[1]
[1]Laboratoire d'Informatique, Mathématiques Appliquées, Intelligence Artificielle et Reconnaissance de Formes, Faculté des sciences de Rabat-Agdal, Maroc.
[2]Laboratoire de Conception et Systèmes, Faculté des sciences de Rabat-Agdal, Maroc.

Abstract

The transmission and the transfer of images, in free spaces and on lines, 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. The standard techniques of encryption are not appropriate for the particular case of the images. For this we have proposed a new hybrid approach of encryption-compression (FMT-AES), 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 Transformation. 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.

I. Introduction

For a protected and reduced transfer of images, the algorithms of encryption images must be able to be combined with the algorithms of compression of images [6]. The techniques of compression seek the redundancies contained in the images in order to reduce the quantity of information[5]. On the other hand, the tech-

niques of encryption aim to remove all the redundancies to avoid the statistical attacks, which is the famous problem [9].

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, 5]. 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[3].

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 [10].

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 AES encryption algorithms. 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.

II. Methods

1. The Faber-Schauder multi-scale transformation

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

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} :

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

The space base W_{j+1} is given by:

$$\left(\psi^{j+1}_{1,k,l} = \phi^{j}_{2k+1} \times \psi^{j+1}_{l},\ \psi^{j}_{2,k,l} = \psi^{j+1}_{k} \times \phi^{j}_{2l},\right.$$
$$\left.\psi^{j}_{3,k,l} = \psi^{j+1}_{k} \times \psi^{j+1}_{l}\right)_{k,l\in Z}$$

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:

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

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

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

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 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].

1.2. Visualization of the transformed images by the FMT

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.

The image obtained is a coherent one which resembles an outline representation of the original image (Figure 1). Indeed, the FMT transformation, like some wavelets transformation, has similarities with the canny outlines detector [8], 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 [7].

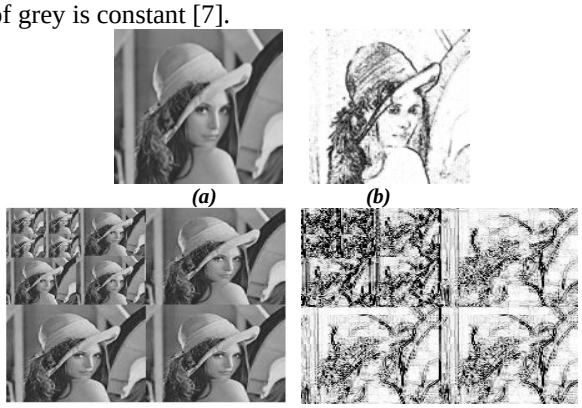


Fig.1. Representation on mixed-scales and on separate scales of the image "Lena". The coefficients are in the canonical base in (a) and (c) and in the Faber-Schauder multi-scale base in (b) and (d).

1.3. 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 (see results of applications). 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 pro-

vokes 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|| ≥ 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 [4].

2. The encryption algorithm AES

AES is the acronym of Advanced Encryption Standard, creates by Johan Daemen and Vincent Rijmen. It is a technique of encryption to symmetrical key. It is the result of a call to world contribution for the definition of an algorithm of encryption, call resulting from the national institute of the standards and technology of the government American (NIST) in 1997 and finished in 2001. 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 [1,2].

The AES Algorithm is iterative (Figure 2). It can be cut out in 3 blocks [12]:

- **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.

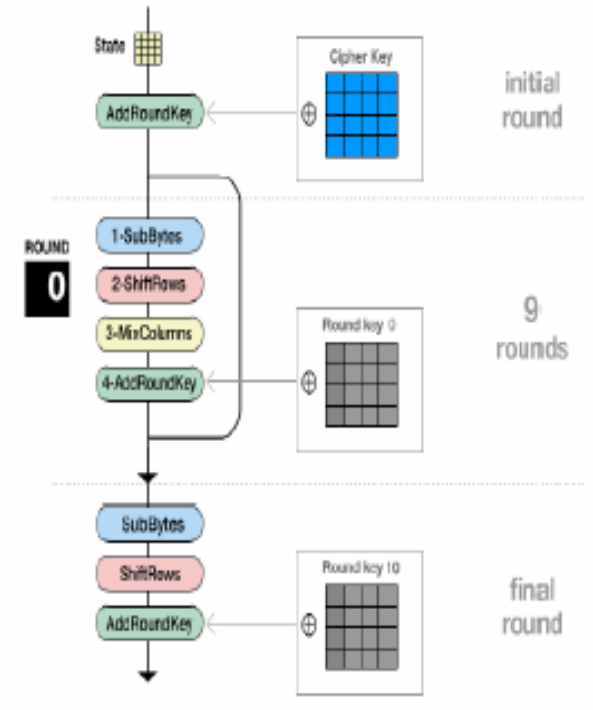


Fig.2. Diagram block of the algorithm AES, version 128 bits.

3. The 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 3 as follow:

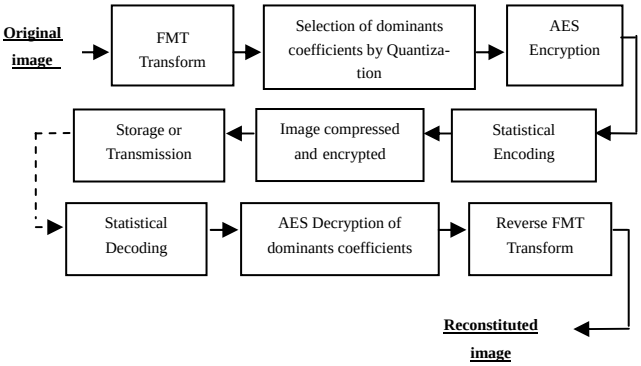


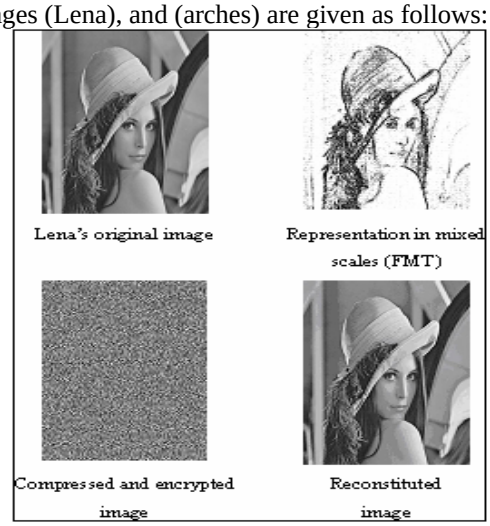
Fig.3. General diagram of the encryption-compression approach.

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 IFMT (reverse FMT) to restore the image.

III. Results

1. Applications

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



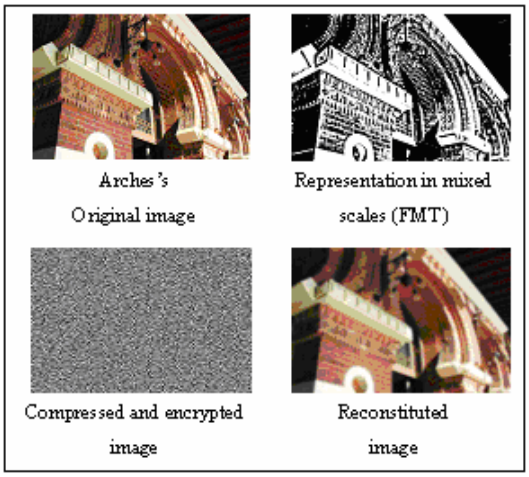


Fig.4. The stages after application of FMT-AES method on Lena's image and Arches's image.

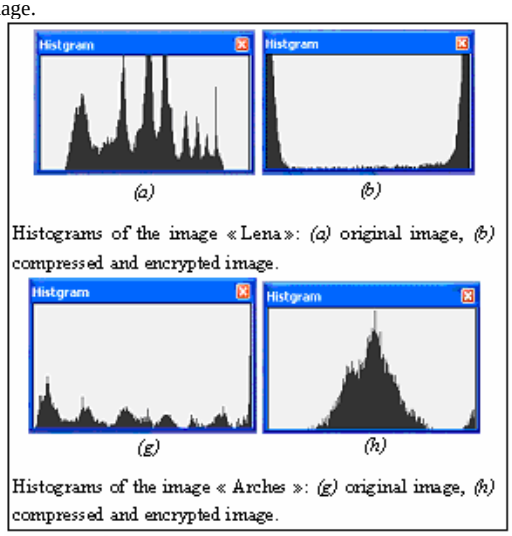


Fig.5. Diagrams of originals images and compressed-encrypted images.

2. Comparison

The comparison is carried out, after the application of the methods of encryption-compression : Quadtree-AES and DCT-partial encryption and our method FMT-AES, on the image

"Lena", "echographic image", "Arches" and "Flower". The results obtained are given on table 1 following :

	Entropy of original image	Quadtree-AES		DCT-Part. Encryt.		FMT-AES	
		PSNR (dB)	Entropy of reconstituted image	PSNR (dB)	Entropy of reconstituted image	PSNR (dB)	Entropy of reconstituted image
Lena	7.589	35.083	7.015	35.351	7.083	34.879	6.981
Arches	8.782	53.989	8.213	54.265	8.271	53.791	8.181

Table 1 : Comparison of our method FMT-AES with the methods Quadtree-AES and DCT- partial encryption.

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 principle 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.

IV. Conclusion

We presented an approach of encryption-compression 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] 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] 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.
[7] 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.
[8] 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.
[9] X.Marsault, *Compression et Cryptage des Données Multimédias*, Hermes, 1997.
[10] 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.