

Images Encrypt-Compression by Wavelets Networks

A. Boukhriss O. Jemai C. Ben Amar

REsearch Group on Intelligent Machines (REGIM)

University of Sfax, National Engineering School of Sfax, B.P. W, 3038, Sfax, Tunisia

aida.boukhriss@yahoo.fr, olfa.jemai@yahoo.fr, chokri.benamar@ieee.org

Abstract

As multimedia applications have become more popular, there is a greater demand for the efficient representation of many different types of data. To accommodate the increasing use of multimedia in network environments, the amount of data transmitted must be minimized and secured.

In this meaning, we propose an efficient scheme of selective encryption, concerning the integration of the RSA encryption in a compression process based on the wavelets networks.

1. Introduction

Computer networks are the means of data transfer in its different forms: text, graphic, video... Optimization and security of transmission and storage are subject of many researches.

In this paper we present a new approach that join a double requirement, first one is to increase security's degree and second one is to decrease transmission time. This approach ensures encryption and compression: encrypt-compression, for a typical data representation which is image.

2. Existent

To improve storage capacity and to reduce transmission time through networks, we must compress data, in particular numerical image. This last one must be encrypted to ensure confidentiality of information during their storage and their transfers on networks. To satisfy these two conditions, classical approach consists on the application of an encryption algorithm independent after the data compression step [1] [2].

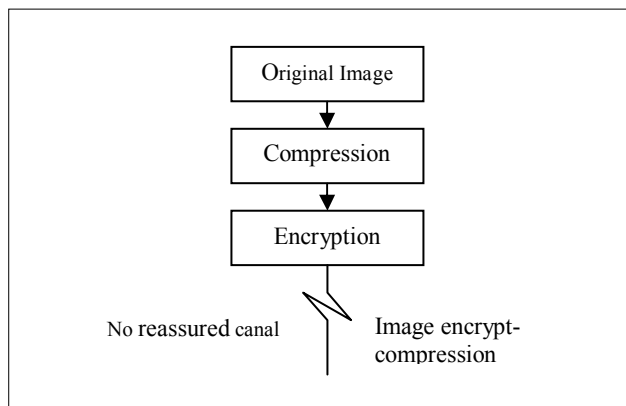


Figure 1. Classical approach of encrypt-compression image

An encryption devoid any type of spatial redundancy. So we always apply compression before encryption to not reduce compression performance. Classical approach demands an important encryption time. In order to reduce this time, a new partial encryption approach appeared [1] [2] [3] [4].

In this paper, we propose an approach that associates wavelet networks compression and partial encryption.

3. Principe schema

Image compression process is a succession of three treatments that are transformation, quantification and encoding. To have a rebuilt picture, image compressed must be decoded, dequantified and finally inversely transformed.

Quantification Step is a treatment of lost data, for this reason, we demand that encryption must be after quantification step and before encoding [5].

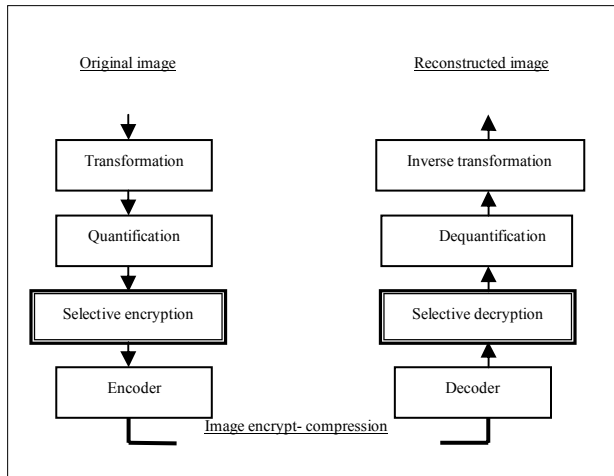


Figure 2. Principle of our approach

4. Principle of our approach

In this part we define at first wavelets as well as wavelet network, and we will finish by a presentation of our approach principle.

4.1. Wavelet transformation

Wavelet transformation is a tool that belongs to the signal treatment domain. Fourier transformation is his ancestor. Wavelet transformation is a tool that cuts data, functions or operators while composing following frequencies a resolution to adapt in the frame. This analysis consists of the use of functions family $\psi_{a,b}$ built from function ψ of $L^2(\mathbb{R})$ which has a complex values and called wavelet mother, or analyzing wavelet:

$$\psi_{ab}(t) = \frac{1}{\sqrt{a}} \psi\left(\frac{t-b}{a}\right) \quad (1)$$

More important wavelets properties are:

- ✓ Admissibility: Be a function ψ belonging in $L^2(\mathbb{R})$ and $TF(\psi)$ its Fourier transformation ψ satisfying admissibility condition if:

$$\int_{-\infty}^{+\infty} \frac{|TF(\psi(\omega))|^2}{|\omega|} d\omega < +\infty \quad (2)$$

- ✓ Localization: Wavelet is a function $\psi(x)$ of $L^2(\mathbb{R})$ having the location property if she is in quick decrease on the two edges of his definition domain. Location means that energy wavelet is contained in a finished interval.

Ideally, wavelet is a null function outside the finished interval, which means that this function has a compact support.

- ✓ Oscillation: Wavelet is a function $\psi(x)$, integrals and sufficiently oscillating to becoming a null integral:

$$\int \psi(t) dt = 0 \Leftrightarrow TF(\psi(0)) = 0 \quad (3)$$

Therefore $\psi(x)$ must have a wavelet character that changes sign at least once.

- ✓ Translation and Dilation: Wavelets analysis associates an itself translated and expanded family of copies:

$$\psi_{ab}(t) = \frac{1}{\sqrt{a}} \psi\left(\frac{t-b}{a}\right) \text{ with } a, b \in \mathbb{R}, a > 0. \quad (4)$$

4.2. Wavelets networks

Architecture of the wavelets networks that we propose, for encrypt-compression of images, contains a layer of entry cells, a layer of hidden cells, and a layer of exit cells. Cells of a layer are connected to all cells of following layer and only to these. Values propagate themselves from entry cells towards exit cells.

To specify that we mean by parameter, we can refer ourselves to figure3. We designate by parameter, the architecture coefficients, intervening in calculation of gone out furnished by the network.

$$y(t) = \sum_{k=1}^K W_k \psi_k\left(\frac{t-b_k}{a_k}\right) \quad (5)$$

These parameters are therefore:

w_{ij} : Connection weights between the cell i and exit cell j.

a_i : Dilation coefficients of cell i.

b_i : Translation Coefficients of cell i.

Transfer function ψ of hidden cells is a wavelet function. Architecture of our wavelets network will be as show.

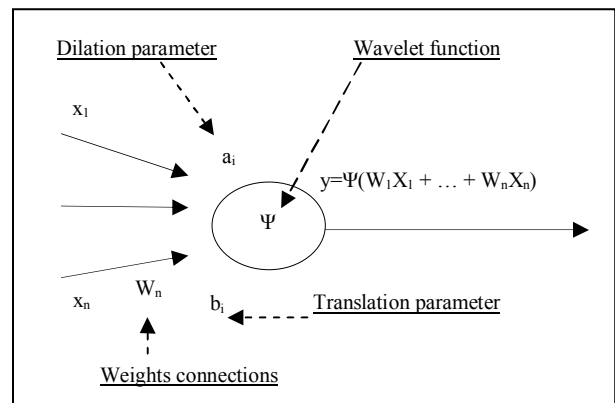


Figure 3. Graphic representation of our wavelets network

4.3. Principal of our approach

Technique of encrypt-compression in our work is based on the wavelets networks with retro-propagation algorithm for apprenticeship phase.

Compression operation starts with segmentation of picture choose by the user before starting the encrypt-compression process. Our network apprenticeship, is done while applying retro-propagation algorithm.

Our departure basis contains vectors and each one represents a pad of picture. Entry network values represent intensities values of pixels in a same pad, exits values desired must be equal to one of entries. Network parameters initialization is the first step of the encrypt-compression. Values are taken with a random manner. In apprenticeship phase, we will successively present apprenticeship vectors and we will adjust to every time values of parameters network, to know weights connection of different cells, expansion coefficients and translation coefficients of wavelets family used, so that values of gone out and entries one will be identical for every pad. We will repeat traverses of apprenticeship basis to verification of a stop criterion that we choose, a maximum number of loops (a loop is a traverses basis).

Network gone out is according to w_{ij} (connection weights). As for encrypting we chose encrypted w_{ij} values and this in order to minimize encrypted information and to diminish encrypting time. Practically we will apply partial encrypting, but theoretically this is a total encrypting on the whole of picture that is applied since network gone out calculates itself according to balanced sum of connections weights with network entries.

Encrypting process is realized by applying an asymmetrical encrypting algorithm that is one of RSA.

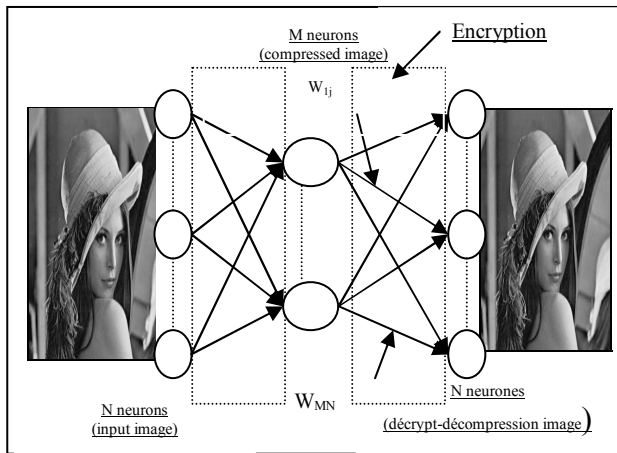


Figure 4. Principle schema of our approach

5. Implementation and results

Figure 5 illustrates the flowchart of encrypt-compression crosses technique.

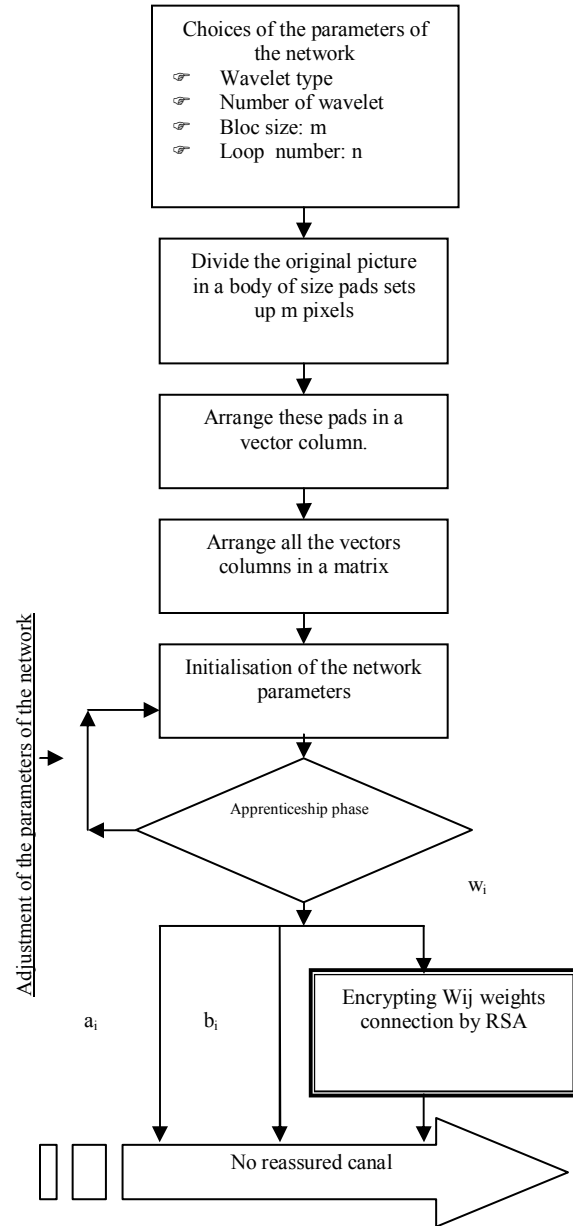


Figure 5. Flowchart of our approach

Variation of parameter wavelets number selected by the user defines picture compression rate. This factor is defined by:

$$\text{ratio} = \left(1 - \frac{NO * (2 + NB + TB) + TC}{NB * TB}\right) \times 100 \quad (6)$$

With NO, NB, TB respectively represent number of neurons in hidden layer, number of pads in picture to compress and pad size and TC represents encrypted key size .

Rebuilt picture is not same to original picture, therefore necessarily there is loss of information. We will try to vary some parameters of our architecture for well to identify location of network picture quantification.

Table 1. Quality of rebuilt picture according to architecture parameters

Type of wavelet	PSNR	EQM	loops Number
Mexican Hat	14.486	2314.257	3
	17.752	1091.081	5
	19.894	666.262	10
	21.255	487.019	15
	38.382	9.437	20
Rasp3	27.095	126.926	3
	31.925	41.738	5
	38.856	8.460	10
	41.774	4.321	15
	43.206	3.107	20

We can notice that for any wavelet function used, picture quality becomes more and more good as a PSNR and MSE when we increase loops numbers. Therefore if we find a mean to calculate the connections weights, expansions parameters and translations parameters, wavelets network can be a mean of compression without loss with a higher compression rate, which is impossible with other methods.

For encrypt-compression crosses technique, compression rate depends on encrypted key size, in order to not diminish compression performances especially rates we must encrypt with a small size key. Pictures encrypted methods that use a key of a size that surpasses information itself cannot be integrated in a compression algorithm.

To test performance of our encrypt-compression approach we will try to increase security level and therefore encrypted key size and see the compressed rates variation.

Table 2. Rates variation of compression according to encrypted key size

Pad number	Pad size	Wavelet number	Encrypted size key	Ratio
1024	64	7	8 bits	89.0396
1024	64	7	32 bits	89.0350
1024	64	7	64 bits	89.0289
1024	64	7	128 bits	89.0167
1024	64	7	512 bits	88.9435

Table 2 watches shows that compressed rate remains almost the same even if we increase encrypted key size; therefore we have thus encrypted picture with a negligible size key in comparison with sent information to the destination.

Encrypted percentage part in comparison with original picture is a very interesting factor to verify validity of such approaches or encrypted algorithm since this percentage influences on encrypting speed [1].

First compression method on which one is applied the encrypt-compression crosses technique is compression by DCT transformation. Encoding is applied here on bases frequencies. Studies showed that this technique is not very interesting especially of any saw encrypted times since almost 50% of entirety of picture must be encrypted.

Adopted methods today for encrypt- compression are two encrypted methods by selection that one of Quadtree and one of SPIHT.

Encrypted by selection choice allows us to diminish encrypted time. In figure 3 we will classify four used methods of picture encrypt-compression according to percentage on encrypted part compared to original picture.

Percentage of encrypted part in our approach is the quotient cuts weights of connections with size of network entered pads.

$$\text{Percentage (\%)} = \frac{\text{NO}}{\text{TB}} * 100 \quad (7)$$

Table 3. Classification of encrypt-compression schema according to percentage of encrypted part

Encrypt-compression	Image size (bytes)	Percentage of
---------------------	--------------------	---------------

schema		encrypted part (%)
DCT [1] [6]	256x256	50
	512x512	50
Quadtree [1] [5] [6]	256x256	27
	512x512	13
SPIHT [1] [5]	256x256	7
	512x512	2
Wavelets network	256x256	6.25
	512x512	6.25

6. Conclusion

In this work we presented an effective schema of encrypt-compression in which one we developed a new approach concerning integration of encrypting inside compression algorithm by wavelet networks.

This schema can be adapted to transmission sector of all picture type. For that, we tried to reduce encrypted time and of interpreting to improve the management and transmission speed and the storage capacity. Our approach is flexible, in fact we can, according to compressed rates and of treatment speed tolerated, choose pad size to segment picture.

Our schema is secured since we use a RSA sacred encrypt-system, in fact the first algorithm RSA advantage is that it is asymmetrical so it does not necessitate transmission of the key between sender and destination of a secured manner. Encrypted integration in the picture compressed process does not allow the decrease of wavelets network performance for compression picture since quality of rebuilt picture after encrypt-compression remains same as picture quality rebuilt after compression. To improve security level, and as extension of our work we can apply a symmetrical encrypted algorithm, we can also develop a crosses technique that combines compression, encrypting and tattoo and that allows increasing the security level.

7. References

- [1] H. Cheng, X. Li, "Partial encryption of compressed images and videos". *IEEE Transactions on Signal Processing*, 48(8), 2000, pp.2439-2451.
- [2] M.V. Droogenbroeck, R. Benedett, , "Techniques for a selective encryption of uncompressed and compressed images". *Proceedings of ACIVS 2002 (Advanced Concepts for Intelligent Vision Systems)*, Ghent, Belgium, September 2002, pp.9-11.
- [3] M. VanDroogenbroeck,, "Partial encryption of images for real-time applications". In *Fourth IEEE Benelux Signal Processing*, Hilvarenbeek, The Netherlands, April 2004, pp.11-15.
- [4] X. Liu, A.M. Eskicioglu, "Selective Encryption of Multimedia Content in Distribution Networks: Challenges and new Directions". *Proceedings of the 2nd IASTED International Conference on Communications, Internet, and Information Technology (CIIT 2003)*, Scottsdale, AZ, 17-19 November 2003, pp.527-533.
- [5] Y. Seo, D. Kim, J. yoo, S. Dey, A. Agrawal, "Wavelet domain image encryption by subband selection and data bit selection", *Dept. Of electronic Materials Eng*, Kwangoon University.
- [6] X. Li, J. Knipe, H. Cheng, , "Image compression and encryption using tree structures", *Pattern Recognition Letters* 18, November 1997, pp.1253 – 1259.
- [7] C. Ben Amor, J. Knipe, H. Cheng, "Image compression and encryption using tree structures", *Pattern Recognition Letters* 18, November 1997, pp.1253 – 1259.