International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

Protection of Images by Combination of Vernam Stream Cipher and S.V.D Watermarking

Ralaivao Harinaivo Hajasoa
Telecommunication- Automatic – Signal – Image- Research Laboratory/Doctoral School in Science and Technology of Engineering and Innovation/University of Antananarivo
Antananarivo, Madagascar

Raminoson Tsiriniaina
Telecommunication- Automatic – Signal – Image- Research Laboratory/Doctoral School in Science and Technology of Engineering and Innovation/University of Antananarivo
Antananarivo, Madagascar

Randriamitantsoa Paul Auguste
Telecommunication- Automatic – Signal – Image- Research Laboratory/Doctoral School in Science and Technology of Engineering and Innovation/University of Antananarivo
Antananarivo, Madagascar

***Abstract*— In this article, we propose a hybrid scheme for encryption and watermarking. It reflects to the study of a new method to make sure and safe the transfer of digital images. It combines two methods namely, Vernam stream cipher method and Singular Value Decomposition (S.V.D)-watermarking. Encryption and watermarking are complementary lines of defense in protecting multimedia content. Before transmission, the original image is encrypted with the mask obtained after applying the generator pseudo-random number to the secret user key. The watermark which represents the secret key in image format is then embedded into the multimedia content. During the insertion process, a public key and a private key are used within the asymmetric cipher method in order to protect the watermarking key. In order to strengthen the protection, RSA is called for securing the watermarking key. Then, the watermarked encrypted image can be conveyed within the public channel which is not secured. Each receiver can decrypt the stream after reconstructing the same key, and extract the watermark from the image.**

Keywords—Encryption, watermarking, S.V.D (Singular Value Decomposition).

I. INTRODUCTION

For a long time, the confidentiality and the security of information are very important and primordial that we cannot ignore in several domains.

Recent research has used two different approaches resulting in encryption techniques that are independent from watermarking techniques :

- Encryption makes the content unintelligible through a reversible mathematical transformation based on a secret key. Among several techniques, we have used Vernam method applied to images
- Digital watermarking consists on inserting a mark into an image to protect it against copies. In this case, our method is based on S.V.D decomposition.

This present article presents therefore an approach which establishes a relation between the data encryption key and the watermark. The both methods are chosen for their respective improvement.

II. VERNAM ENCRYPTION AND DECRYPTION

A. Principle and methodology

The Vernam Cipher is named after Gilbert Sandford Vernam (1890-1960) who, in 1917, invented the stream cipher and later co-invented the OTP (One-Time-Pad).

This method has been applied on a text.

The Vernam Cipher is based on the principle that each **plain text** character from a message is 'mixed' with one character from a **key stream**. If a truly **random** key stream is used, the result will be a truly 'random' **cipher text** which bears no relation to the original plaintext. In that case the cipher is similar to the unbreakable OTP.

For one bit named x_i of the text ***x*** mixed with a bit z_i of the key ***z***, a bit y_i is obtained by the equation:

$$y_i = x_i \oplus z_i \quad (1)$$

Where $\oplus$ is the bitwise exclusive OR

The reverse process is defined by the equation :

$$x_i = y_i \oplus z_i \quad (2)$$

Finally, the original text ***x*** named **plaintext** can be reconstructed with the bits x_i [7].

The advantage of using the XOR operation is that it can be undone by carrying out the same operation again. In other words:

Plaintext + key = ciphertext ⇒ ciphertext + key = plaintext

B. Illustration

For example, we want to transmit the word **HELLO** which is stored on the **plaintext**.

We also have a pre-recorded **key**, with a series of random characters; in this case the sequence **AXHJB**.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

The text encryption can be illustrated:

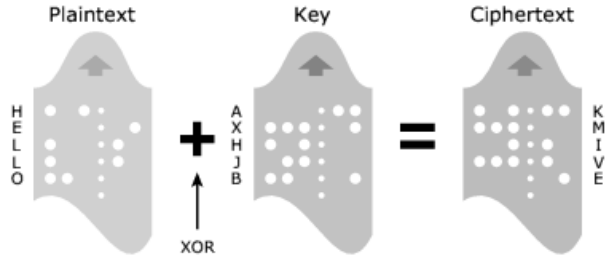


Fig. 1. Mixing of the plaintext and the Key

It is very simple to find again the plaintext because plaintext and ciphertext are permuted on the same equation for the reverse process. This operation is illustrated as follow:

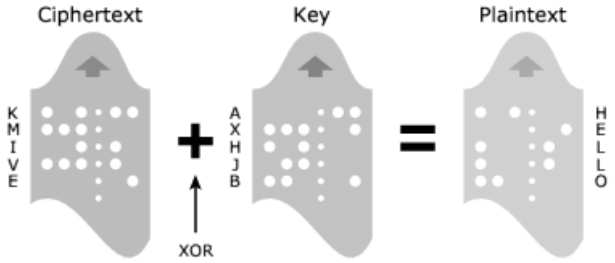


Fig. 2. Mixing of the Ciphertext and the Key

The same principle can be used on an image.

C. Vernam encryption of an image

The encryption method is based on the following formula:

$$I^c = I \text{ xor } K \qquad (3)$$

where I, IC, K are respectively the original image, the encrypted image and the mask.
This operation can be subsequently represented as follow:

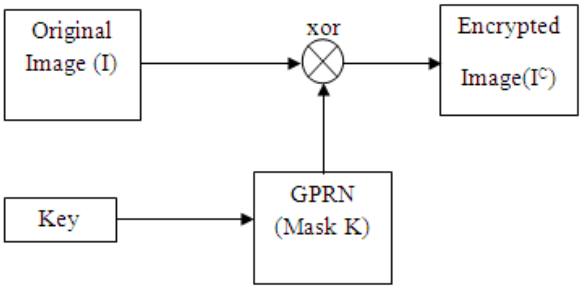


Fig. 3. Encryption scheme of an image by Vernam method

G.P.R.N: Generator of Pseudo Random Number
Key: user key
I^C: Encrypted Image
I: Original Image
K: mask

D. Vernam decryption of an image

The decryption algorithm follows the reverse process of the different steps of encryption that have been implemented.
The decryption method is based on the following formula:

$$I = I^c \text{ xor } K \qquad (4)$$

This operation can be represented as follow:

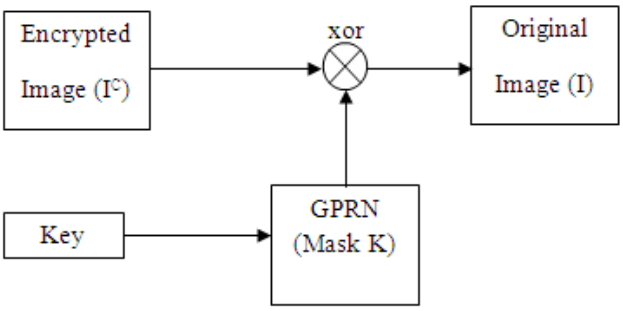


Fig. 4. Decryption scheme of an image by Vernam method

The same key is used during the encryption and the decryption.

E. Cipher Security

The above procedure is 100% safe if, and only if, the following conditions are all met [8] [9]:

1. There are only two copies of the key-tape,
2. Both sides of the communications link have the same key-tape,
3. The key-tape is used only once,
4. The key-tape is destroyed immediately after use,
5. The key-tape contains truly random characters,
6. The equipment is TEMPEST proof,
7. The key tape was not compromised during transport.

III. R.S.A ENCRYPTION AND DECRYPTION

A. Principle and algorithm

The RSA cryptosystem, named after its inventors R. Rivest, A. Shamir, and L. Adleman, is the most widely used public-key cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization problem [10].

Algorithm RSA public-key encryption [11]:
B encrypts a message m for A, which A decrypts.
1. Encryption. B should do the following:
(a) Obtain A's authentic public key (n; e).
(b) Represent the message as an integer m in the interval [0; n−1].
(c) Compute $c = m^e \bmod n$.
(d) Send the ciphertext c to A.
2. Decryption. To recover plaintext m from c, A should do the following:
(a) Use the private key d to recover $m = c^d \bmod n$.

B. Watermarking key

In our systems, images are first encrypted using one key, and then embedded using different keys. To keep the two types of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

keys distinct, we use the terms cipher key (or crypto key) and watermark key, respectively.
RSA method is used for the watermark key.
In another word, the system employs cipher key to control Vernam encryption and watermark key to control embedding and detection.
So, it should not be possible to detect the presence of a watermark in a Work without knowledge of the key, even if the watermarking algorithm is known. Further, by restricting knowledge of the key to only a trusted group (i.e., by preventing an adversary from learning the key), it should become extremely difficult, if not impossible, for an adversary to remove a watermark without causing significant degradation in the fidelity of the cover Work [1] [2] [3].

IV. S.V.D WATERMARKING

A. *Singular value and SVD decomposition of matrix*

Although any other watermark embedding and extraction algorithm can be used, we implemented an SVD-based watermarking scheme.
Every real matrix A (dimension is equal to n) can be decomposed into a product of 3 matrices:

$$A = U.S.V \quad (5)$$

where U and V are orthogonal square matrices :

$$U^T.U = U.U^T = I$$

$$V^T.V = V.V^T = I$$

And

$$S = diag(\lambda_1, \lambda_2, \dots, \lambda_r) \quad (6)$$

where r is the rank of matrix A.
The diagonal entries of S are called the singular values (SVs) of A. The columns of U are called the left singular vectors of A or known as hanger and the columns of V are called the right singular vectors of A or known as aligner.
The matrix S contains the sorted singular values on its main diagonal [5] [6].

$$S = \begin{pmatrix} \lambda_i & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{pmatrix}$$

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$$

$$\lambda_{r+1} = \lambda_{r+2} = \cdots = \lambda_n = 0$$

This decomposition is known as the Singular Value Decomposition of A, and can be written as

$$A = \sum_{i=1}^{r} \lambda_i U_i V_i^T \quad (7)$$

Note that each SV specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image.

The SVD is one of the most useful tools of linear algebra with several applications to multimedia including image compression, signal processing, and watermarking.

B. *Application of SVD: image watermarking*

The watermark is embedded by using the key of watermarking to choose the bloc in where the bit value will be inserted.
According to this bit value, the third singular value of the bloc is changed [4].
So it modifies the corresponding SVs of the bloc image.
The process is as shown in figure 5.

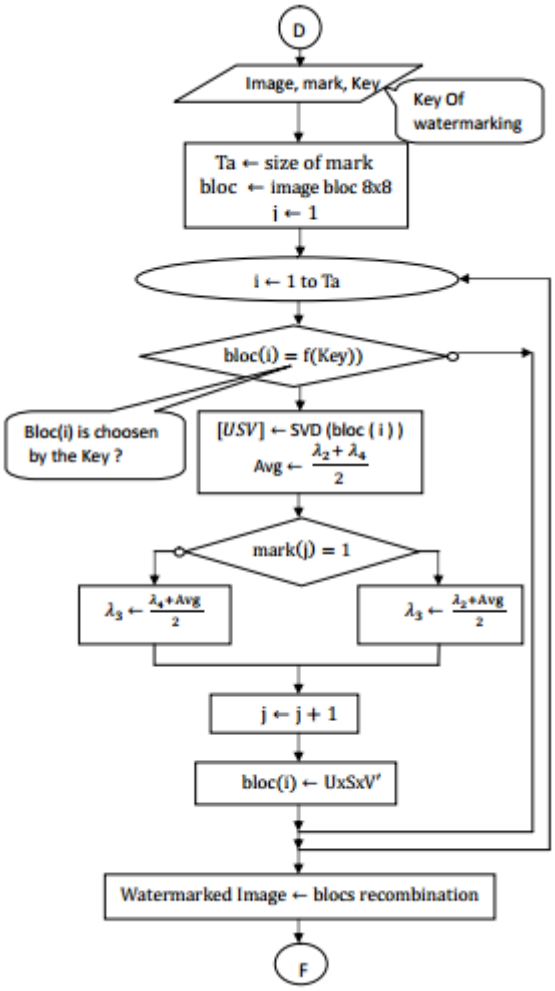


Fig. 5. Watermark Embedding algorithm

The watermark extraction is the inverse of the embedding process.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

The process is as shown in figure 6.

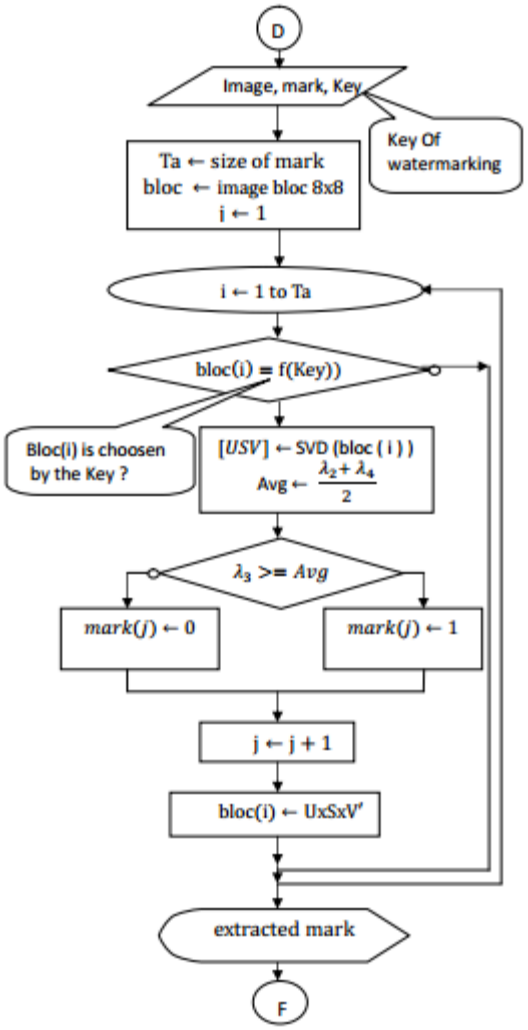


Fig. 6. Watermark extraction algorithm

V. COMBINATION OF ENCRYPTION AND WATERMARKING

In the proposed scheme, the basic tasks performed by the sender and receiver are shown as follows:

A. *Sender side*

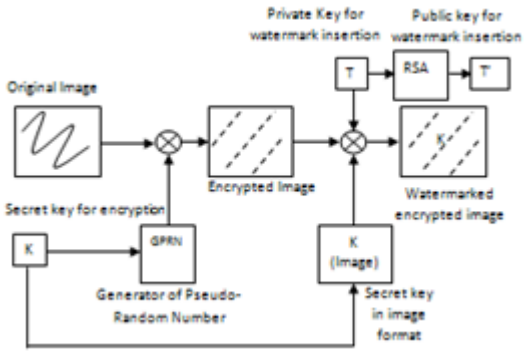


Fig. 7. Encryption and watermark embedding before emission

B. *Receiver side*

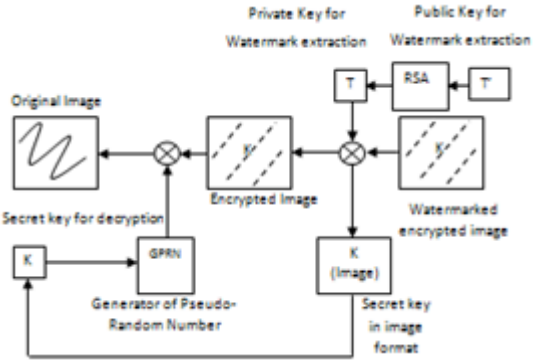


Fig. 8. Decryption and watermark extraction

C. *Transmission over a public channel*

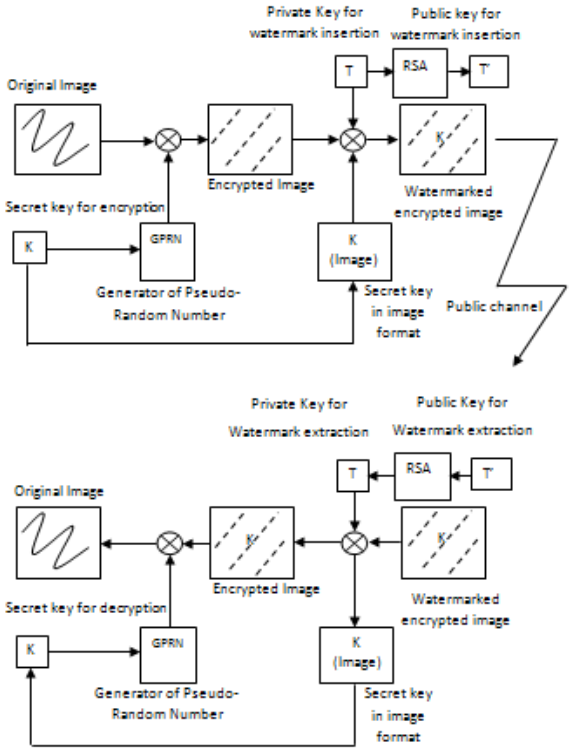


Fig. 9. Combination scheme

VI. SIMULATION WITH MATLAB

A. *Generator of the Pseudo Random Number*

We have used *randint* function of Matlab who generate matrix of uniformly distributed random integers [12] [13].

randint(*M*, *N*, *IRANGE*, *STATE*) Generates an M-by-N matrix of random integer.

IRANGE can be either a scalar or a two-element vector:

Scalar: If IRANGE is a positive integer, then the output integer range is [0, IRANGE-1]. If IRANGE is a negative integer, then the output integer range is [IRANGE+1, 0].

Vector: If IRANGE is a two-element vector, then the output integer range is [IRANGE (1), IRANGE (2)].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

B. Illustration

```
>> randint(10,10,[0,9],5)

ans =

     8     2     5     9     7     2     8     2     3     2
     9     1     5     2     7     2     9     7     7     1
     2     8     9     4     3     7     6     2     3     9
     8     8     8     5     4     7     3     4     0     8
     7     7     4     9     9     8     3     0     9     3
     3     9     3     3     5     5     5     6     8     5
     7     1     2     0     0     7     6     5     7     9
     5     6     7     1     7     6     0     4     9     9
     4     9     3     5     8     8     1     7     2     7
     3     8     5     8     7     3     2     5     6     2
```

Fig. 10. Generation of random matrix 10x10

In our simulation, with the cipher key equal to **127** and $randint(256,256,[0,255],\mathbf{127})$, we obtain the encryption mask:

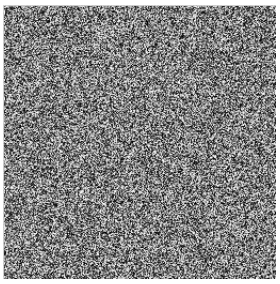


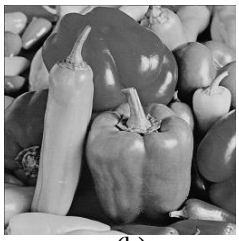
Fig. 11. Vernam encryption mask

The watermark is constructed from with the cipher key and we obtain a binary image format illustrated as shown in figure 12.

Fig. 12. Watermark image in binary format 10x10

In our simulation, we have used the following images:

(a)



(b)

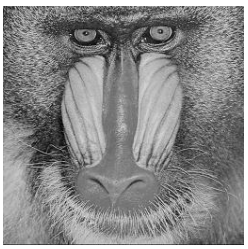


Fig. 13. Images tests: (a) Lena (b) agrumes (c) mandrill

VII. EXPERIMENTAL RESULTS

A. Result of the combination encryption and watermarking with Lena

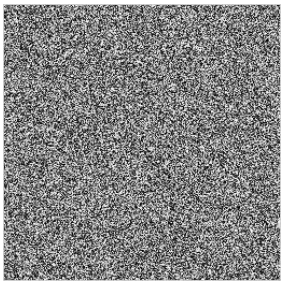


Fig. 14. Watermarked encrypted image (Lena)

B. Comparison of histograms

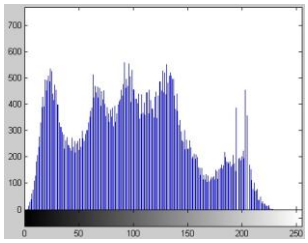


Fig. 15. Histogram of the original image (Lena)

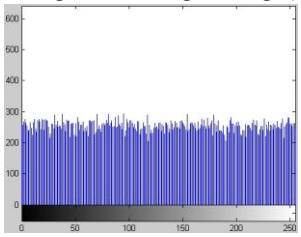


Fig. 16. Histogram of the watermarked encrypted image (Lena)

C. recovered image and watermark

(a)

(b)

Fig. 17. Recovered image of: (a) Lena (b) watermark

D. Difference between original image and watermarked encrypted image

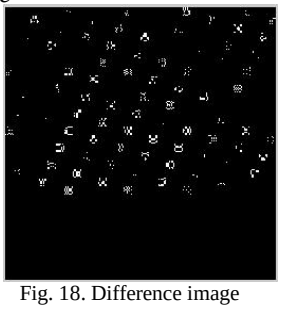


Fig. 18. Difference image

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 06, June - 2017

E. P.S.N.R variation as a function of S.V.D and its energy

For this experience, we have used the three images (Lena, agrumes and mandrill) in order to see the efficiency of the S.V.D method.

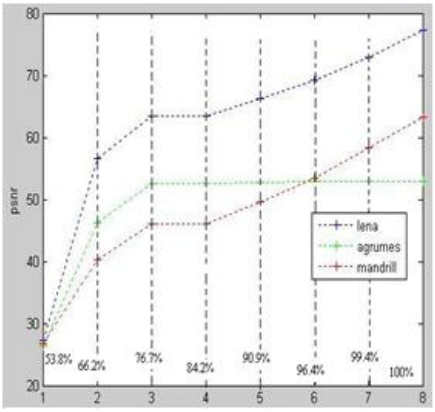


Fig. 19. P.S.N.R variation as a function of the number of S.V.D coefficients.

VIII. CONCLUSION

Applied to images, the encryption method using Vernam stream cipher is very fast and performs the processing within a linear complexity.

The heaviness of the extraction procedure with the old methods urged us to apply the S.V.D watermarking method which would be blind and robust. It does not require the original image to extract the mark. The SVD-based watermarking scheme was been already tested using several attacks, and was resistant to these attacks.

Finally, the Combination of encryption and watermarking algorithms yields effective results for protecting images.

REFERENCES

[1] A. H. Tewfik and M.D. Swanson. "Data Hiding for Multimedia Personalization, Interaction And Protection". IEEE Signal Processing Magazine, p. 41–44, 1997.

[2] A. Meerward, "Digital Image Watermarking in the wavelet transform domain", Diploma thesis, Salwburg University, 2001.

[3] AES. Announcing the Advanced Encryption Standard. Federal Information Processing Standards Publication, 2001.

[4] B. Tao and B. Dickinson. Adaptive Watermarking In The DCT Domain. In Proc. Int. Conf. Image Processing (ICIP), Lausanne, Switzerland, 1996.

[5] C. S. Lu, «Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual-Property", IDEA GROUP PUBLISHING, 2005.

[6] C.C. Chang, M.S. Hwang, et T-S Chen. A new encryption algorithm for image cryptosystems. The Journal of Systems and Software, p. 83–91, 2001

[7] Douglas R. Stinson. Cryptography: Theory and Practice, (Discrete Mathematics and Its Applications). Chapman & Hall/CRC Press, New York, Novembre 2005.

[8] G. Lo-varco, W. Puech, et M. Dumas. Dct-based watermarking method using error correction codes. Dans ICAPR'03, International Conference on Advances in Pattern Recognition, Calcutta, India, p. 347–350, 2003.

[9] J. F. Delaigle, C. De Vleeschouwer, F. Goffin, and B. Macq. Low Cost watermarking based on a Human Visual Model. Lecture Notes in Computer Science, 1997.

[10] R.AGARWAL,M.SANTHANAM, "Digital watermarking in the singular vector domain", 2006.

[11] R. Norcen, M. Podesser, A. Pommer, H.P. Schmidt, et A. Uhl. Confidential storage and transmission of medical image data. Computers in Biology and Medicine, p. 277–292, 2003.

[12] W. Puech, J.J. Charre, et M. Dumas. Transfert sécurisé d'images par chiffrement de Vigenère. Dans NimesTic 2001, La relation Homme - Système : Complexe, Nîmes, France, p. 167–171, 2001.

[13] P. BAS, J. M. CHASSERY, B. MACQ, "Méthode de tatouage fondée sur le contenu», Traitement du Signal, Vol. 19, p. 11-17, 2002.