Crypto-Compression Using TEA's Algorithm and a RLC Compression

Jean-Claude Borie, William Puech, Michel Dumas

Crypto-compression using TEA's algorithm and a RLC compression .

Jean-Claude Borie[1], **William Puech**[2] **and Michel Dumas**[1]

[1] *CEM2 Laboratory , STINIM , UMR 5507 CNRS, University of Montpellier II, Pl. Gabriel Péri, 30021 Nîmes Cedex 1, France*
[2] *LIRMM,UMR CNRS-UM2 5506, University de Montpellier II,161 street Ada, 34392 Montpellier Cedex 05, France.*
borie@univ-montp2.fr, william.puech@lirmm.fr, dumas@univ-montp2.fr

ABSTRACT. *In this paper, we discuss the secure of transfering of medical images. We propose two cryptosystems, the first one is a very fast algorithm by block, the TEA (Tiny Encryption Algorithm) and the second is a stream cipher based on Vigenere's ciphering. We show differences existing between them, especially concerning the combination of the image encryption and the compression. Results applied to medical images are given to illustrate the two methods.*

RÉSUMÉ. *Dans cet article, nous discutons du transfert sécurisé d'images médicales. Nous proposons deux cryptosystèmes, le premier d'entre eux est un algorithm très rapide de chiffrement par blocs, le TEA (Tiny Encryption Algorithm) et le second est un chiffrement par flots constituant une variante du chiffrement de Vigenère. Nous indiquons les différences qui exitent entre ces deux systèmes, en particulier en ce qui concerne la combinaison du cryptage d'images et de la compression. Des résultats appliqués à des images médicales illustrent les deux méthodes.*

KEYWORDS: *Secure transfer, medical, images, block cipher, stream cipher, crypto-compression.*

MOTS-CLÉS : *Transfert sécurisé, médical, images, chiffrement par blocs, chiffrement par flots, crypto-compression.*

1. Introduction.

Ciphering of medical images is actually an important issue. One essential difference between text data and image data is that the size of image data is much larger than the text data.The time is a factor very important for the image encryption.We find it at two levels, one is the time to encrypt, the other is the time to transfer images. To minimize it, the first step is to choose a robust, rapid and easy method to implement cryptosystem. An other important criteria concerns the method of compression, it will decrease the size of images without loss of image quality. In our study we have found some articles on crypto-compression: one of them talk about image coding for mobile using tree structures [Xia 97], the second on compression and encryption of binary and gray-scale images using schemes based on SCAN [Mani 01]. Other articles dealing with medical imagery in particulary in [Cao 03] and in [Nor 03] a partial encryption technique based on AES the new standard is proposed.

This paper is organized as follows. In Section 2, we briefly present TEA and stream cipher cryptosystems. In Section 3, we propose a crypto-compression process in two cases : echography image and a 3D reconstruction image. Finally some conclusions are given in Section 4.

2. Encryption algorithms.

In previous papers [Bor1 02,Bor2 02], we have studied a public key cryptosystem to encrypt image pixel by pixel, with the RSA algorithm. But, if we take blocks of several pixels, the time of ciphering is too long. We have considered other systems with a secret key. The algorithm DES and RSA require much time to encrypt images and it is not also very interesting. Among several systems, we have retained two of them: the TEA and the stream cipher method.

2.1. *Tiny Encryption Algorithm.*

TEA is a short algoritm [Tea 94] which uses Feistel block cipher with a 128-bit key K and 64-bit message blocks. It uses arithmetic and XOR operations rather than substitution (S-Box) and permutation. The number of rounds is variable, for a good security 32 rounds are necessary, but authors advise that 64 rounds are better. A cycle of TEA applied to the block y_i, z_i consists of:

$$\begin{array}{rcl} y_{i+1} & = & y_i + f(z_i, s, k[0,1]), \\ z_{i+1} & = & z_i + f(y_{i+1}, s, k[2,3]), \end{array} \quad [1]$$

where $k[0], k[1], k[2] and k[3]$ are $32 - bit$ subkeys obtained from K.
Initially $s = 0$ and in each round it is incremented by a fixed constant $\delta = [(\sqrt{5} - 1)2^{31}]$.

2.2. *A stream cipher method.*

We present a stream cipher algorithm which was proposed by W. Puech and al. A stream cipher is a symmetric encryption algorithm. It operates on smaller units of image, here one pixel, while a block cipher as TEA operates on eight pixels of the image. This idea constitutes a variant of the Vigenere's cipher. Our technique of encryption consists in add to a pixel of the image the k preceding pixels, each of them multiply by a coefficient generated with the keystream. Generally the key can be as long as the size of the image. Figure 1 illustrates this stream cipher.

If *p(n)* is a pixel of the original image, *p'(n)* the ciphered pixel is according to the

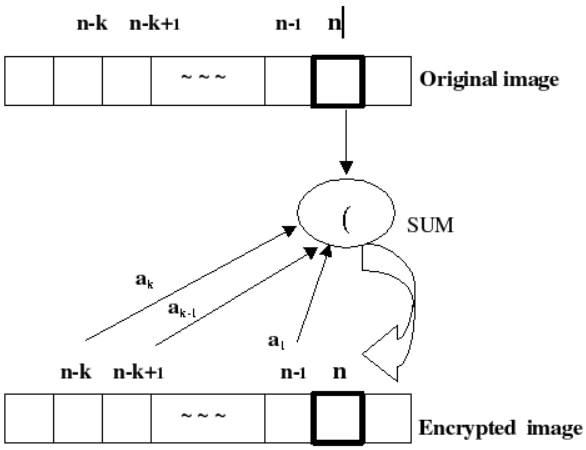


Figure 1. *Stream cipher method.*

next equation:

$$p'(n) = p(n) + \alpha(1)p'(n-1) + \ldots + \alpha(k)p'(n-k), \qquad [2]$$

where $n \in [k, N]$ with $k \in [1, n]$ and N the number of pixels.
The equation (2) can be written:

$$p'(n) = p(n) + \sum_{i=0}^{i=k} \alpha(i).p'(n-i), \qquad [3]$$

where *k* is the order of recurrence corresponding to the length of the chosen key.

2.2.1. *Virtual's pixels construction.*

As we can see on Figure 1, our encryption system requires the introduction of pixels $p(-1), p(-2, \ldots, p(-k)$. We have called " virtuals pixels " these k pixels, that

initially don't exist in the image. These pixels are necessary to begin the encryption of the k first pixels. Virtuals pixels are generated by the secret key.

2.2.2. $\alpha(i)$ *coefficients.*

The coefficients $\alpha(i)$ are also generated with the keystream. These coefficients are been coded on two bits. In this case, the effective length of the key to use is $2.k$ bits. If we note b_{2i-1} and b_{2i} these two bits , we define $\beta(i) = 2.b_{2i-1} + b_{2i}$, and $\alpha(i)$ coefficients are obtained from the next equation :

$$\left\{ \begin{array}{ll} \alpha(i) = \beta(i) - 1 & si\ \beta(i) \in [0, 1, 2], \\ \alpha(ß) = \pm 2 & si\ \beta(i) = 3. \end{array} \right\} \quad [4]$$

During the binary lecture of the keystream, to the binary value 11 is associated alternately the number $+2$ or -2. The Table 1, recapitulates the various possibilities. The

$two\ bits\ value$	00	01	10	11
$\alpha(i)$	0	$+1$	-1	$+/-2$

Table 1. $\alpha(i)$ *coefficients*

average coefficients $\alpha(i)$ value is close or equal to zero and expresses by :

$$\frac{1}{k} \sum_{i=1}^{k} \alpha(i) \approx 0. \quad [5]$$

The particularity of the method resides in the fact that the encryption of each pixel depends on three elements :

– the pixel in clear p(n),
– the he length of the keystream,
– and the *k* precedent pixels in the image.

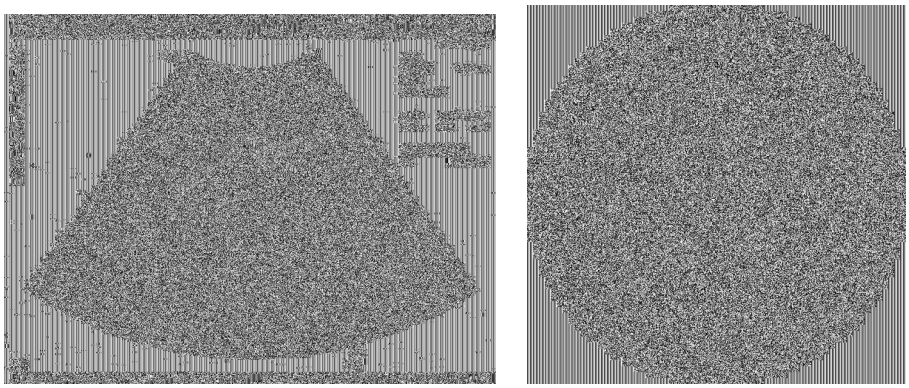
2.3. *Application on medical images.*

To illustrate the proposed methods, we have chosen two images, one echography (432 KB-Figure 2.a) and the other obtained by scanner (256 KB- Figure 2.b).

TEA encryption : The Tiny Encryption Algorithm is fast to encrypt and decrypt medical images, around one second for echography using a pentium III. But the nature of encryption clearly shows blocks encryption. Besides, Figures 3.a and b allow to guess the nature of images. We have observed that with a 3D reconstruction of the aorta image (256KB) from 2D image sections obtained by scanner, the encryption

a) Size : 768 × 576 (432 KB) b) Size : 512 × 512 (256 KB)

Figure 2. *Original image a) echography b) scanner.*



a) Size : 768 × 576 (432 KB) b) Size : 512 × 512 (256 KB)

Figure 3. *TEA ciphering a) echography b) scanner.*

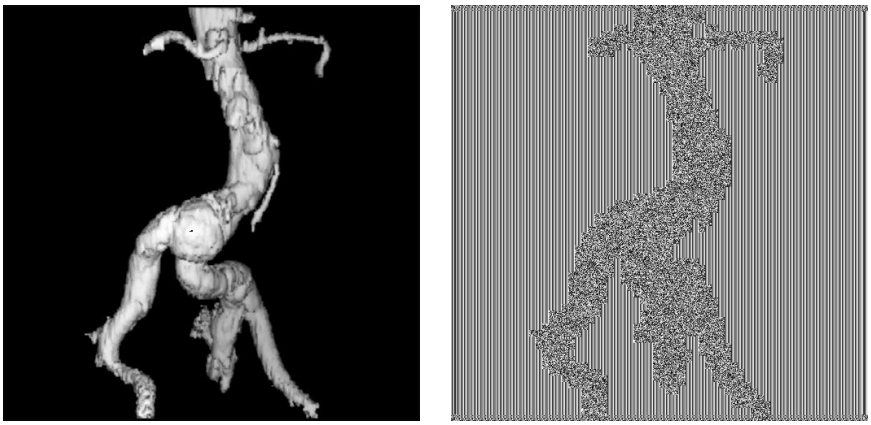
is also not very good (Figures 4.a and 4.b). We also observe an alternation of clear and darker vertical bands. The number of vertical bands amounts easily, it depends primarily on the length of the studied image. This repetitive structure is explained by the fact that encrytion is carried out per blocks in mode Encoding Cipher Block (ECB). Each block is encrypted with the same secret key thus any group having the same group of pixels placed in the same order will be encrypted in the same way. For example the identical blocks :

$$p(i,j), p(i,j+1), p(i,j+2), p(i,j+3), p(i,j+4), p(i,j+5), p(i,j+6), p(i,j+7)$$

of the line *i*, and the block

$p(i+1,j), p(i+1,j+1), p(i+2,j+2), p(i+3,j+3), p(i+4,j+4), p(i+5,j+5), p(i+6,j+6), p(i+7,j+7)$

of the line *i+1* are encrypted strictly in an identical way and lead to stucture in bands observed. In the article [**?**] a similar observation to our is made. The authors assimilate the alternation of lines to a "code bars ". The encryption with TEA's algo-



a) Size : 512 × 512 (256 KB) b) Size : 512 × 512 (256 KB)

Figure 4. *TEA ciphering a) aorta 3D b) encrypted image.*

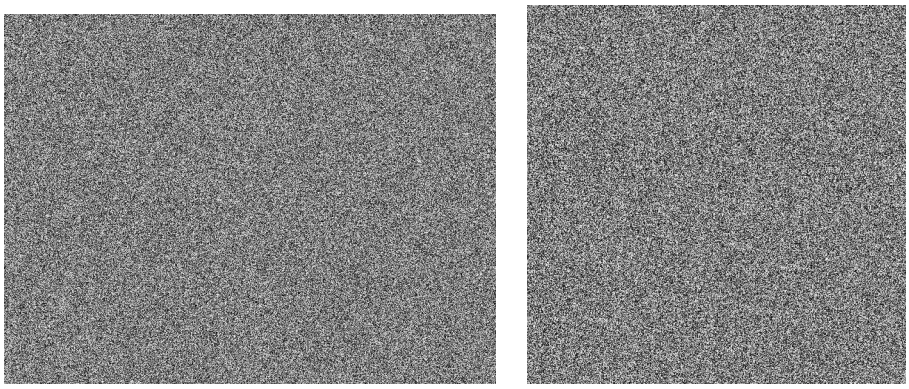
rithm shows regular structures, which can be exploited by an attacker.

Stream cipher. We have chosen a 128-bit keystream which generates 64 virtual pixels and 64 α_i coefficients with $-2 \leq \alpha_i \leq +2$. On these images (Figures 5.a and 5.b), the advantage of stream cipher appears clearly, one has no indication on used cryptosystem as well as on the nature of the image, even for the 3D image of the aorta.

3. Compression

3.1. *Problem on image compression.*

The transmission of numerical images often needs an important number of bits. This number is again more consequent when it concerns medical images. If we want to transmit these images by network, reducing the image size is important. The goal of the compression is to decrease this initial weight. This reduction strongly depends of



a) Size : 768 × 576 (432 KB) b) Size : 512 × 512 (256 KB)

Figure 5. *Stream cipher a) Echography b) scanner.*

the used compression method, as well as of the intrinsec nature of the image. Therefore the problem is the following:

1) To compress without lossy, but with low factor compression. If you want to transmit only one image, it is satisfactory. But in the medical area, these are often sequences that the doctor waits to emit a diagnostic.

2) To compress with losses with the risk to lose information .
The question that puts then is what are the relevant informations to preserve and those that can be neglected without altering the quality of the diagnosis or the analysis. The human visual system is one of the means of appreciation, although subjective and being able to vary from an individual to an other. However, this system is still important to judge the possible causes of degradation and the quality of the compression.

3.2. *Our method.*

We are going to see that encryption and compression constitute a pair that is difficultly reconcilable, one has tendency to increase the weight of the file, the other to decrease the image quality. The solution that we have proposed is to join these two methods in one: the crypto-compression. This compromise appears to be enough satisfactory, on one hand the compression is without loss with a rate oscillating between 1.5 and 4 according to cases, on the other hand an unique program suffices to undertake two operations. These values are close to those obtained by others methods. For example, LZ77 or LZ78 are the names for the two lossless data compression algorithms published by A.Lempel and J.Jacob [LZ 77,LZ 78]. They are both dictionary coders. Later in 1984, LZ77(LZ78) was improved by T. Welch, resultant in LZW

[WEL 84]. We have used also the new lossless format JPEG2000 which has replaced the old JPEG [JPEG2000].

The proposed method is analogous to Run Length Coding, and it is usable for images comprising homogeneous areas as medical images, especially in the 3D image of the aorta where great black zones appear. These images possess often very numerous redundancies that are the basis of the proposed method of compression. We consider a block of *n* consecutive pixels having the same level of gray. If the block is heterogeneous it is encrypted without special treatment. If the block of *n* pixels is homogeneous, we read the next series and so on until the next heterogeneous block. All identical blocks are coded in the same manner.

To signal the redundancy of this serie we use an eight block bytes The distribution

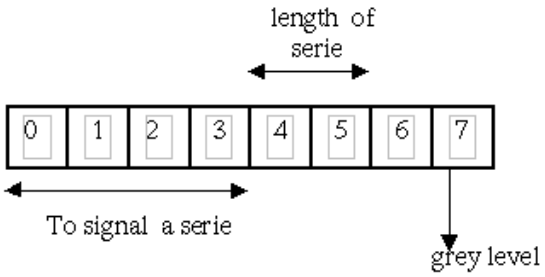


Figure 6. *Crypto-compression method.*

of the eight bytes is the following (Figure.6):
- the four bytes of strong weight serve to signal that there is a serie of *n* identical pixels;
- the two next bytes indicate the length of the continuation;
- the seventh byte serves to define the serie;
- finally the weak weight byte indicates the value of grey level.

Results

To estimate the quality of the process of crypto-compression we have studied the evolution of the entropy:

$$H = -\sum_{i=0}^{2^R-1} n_i.log_2 p(n_i), \qquad [6]$$

where n_i is the value of grey level, $p(n_i)$ the probability to find this grey level and R the number of bits per pixel.
Entropy allows to have an idea of the redistribution of pixels and the number necessary

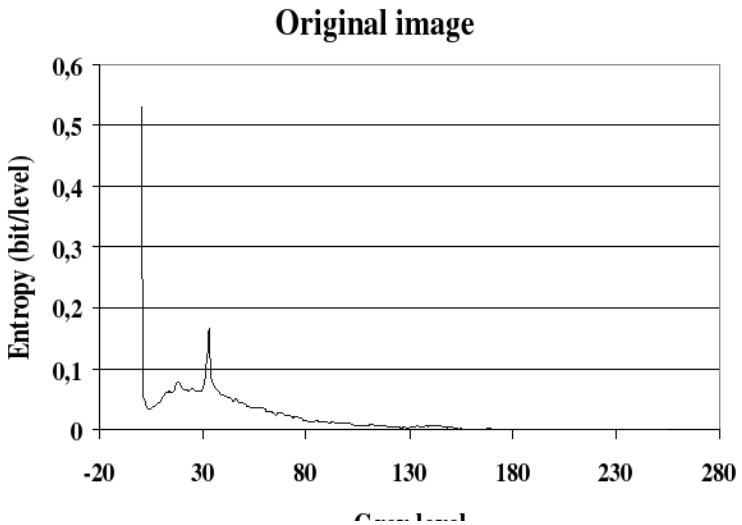


Figure 7. *Echography: entropy of original image-Figure 2.a.*

for transmission by network. The entropy of the echography (Figure 7) shows a peak which corresponds about 38.3% of pixels having an initial grey level of 0. The Figure 8 shows the effect of encryption by blocks of 64 bits with eight modes dominants. These eight peaks corresponding to levels of gray where the entropy is more important than elsewhere. In fact the entropy of these levels indicates the importance of the redundancies in the image. The Figure 9 shows that pixels are redistributed in almost homogeneous way with an average of $0.031bit/pixel$.

$Images$	$a)\ Echography$	$b)\ 3D\ \ reconstruction$
	$Entropy\ (bits/pixel)$	$Entropy\ (bits/pixel)$
$Original\ image$	5.9	2.4
$Encrypted\ image$	7.5	7.89
$Crypto-compressed\ image$	7.92	7.92

Table 2. *Entropy variations .*

The entropy of the echography (Figure 7) shows a peak which corresponds about 38.3% of the pixels having an initial grey level of 0 and an other peak with a grey level of 32 for 3% of the pixels . The Figure 8 shows the effect of encryption by blocks of 64 bits with eight modes dominants. Figure 9 indicates that pixels are redistributed in almost homogeneous way with an average about $0.031bit/pixel$.

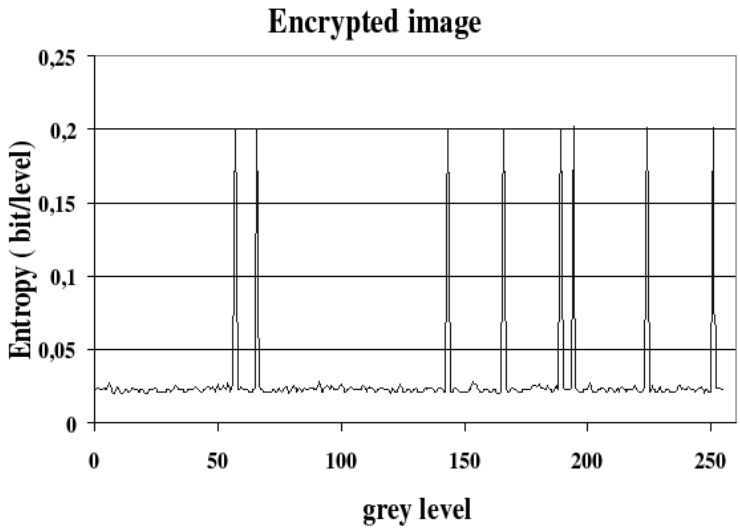


Figure 8. *Echography: entropy of the encrypted-image.*

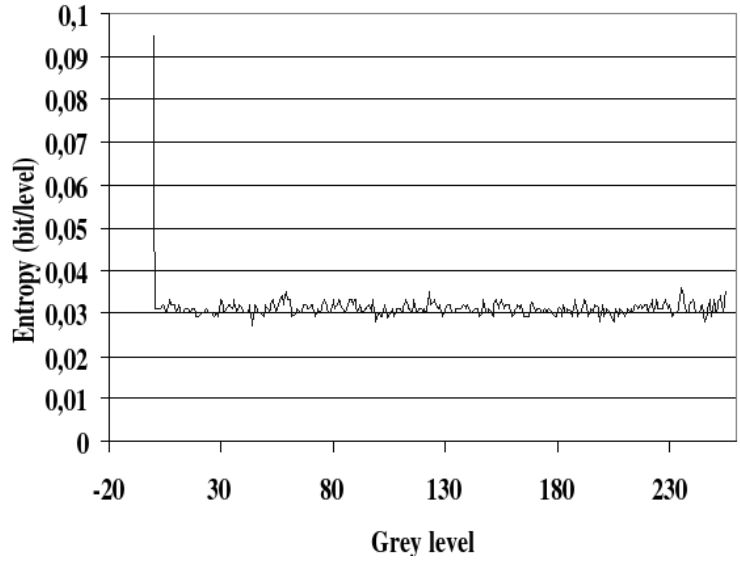
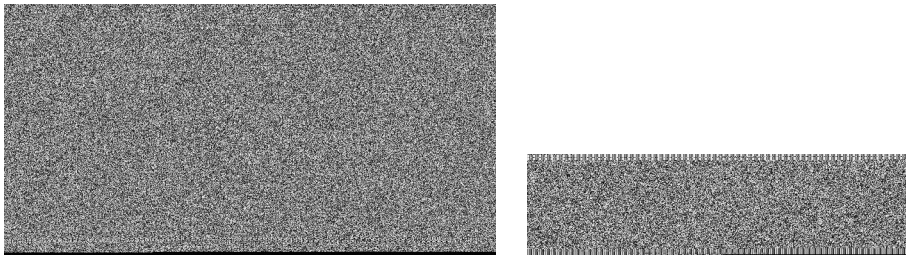


Figure 9. *echography : entropy crypto-compressed image.*

We observe (Table 2) that the entropy of encrypted image is very high and the entropy of crypto-compressed one is better (near eight bits/pixel). But our method

allows to realize two operations in the same time and to reduce the size of the file.The Figure 10.a represents the image of echography after crypto-compression, its size is $294KB$ with a rate of compression of 1.5. The image of aorta Figure 10.b having homogeneous blocks more numerous, the size is reduced from $256KB$ to $68KB$ for a rate of compression of 3.76.



a) Size : 768 × 392 (294 KB) b) Size : 512 × 136 (68 KB).

Figure 10. *a) echography b) 3D image aorta.*

4. Conclusion.

In this paper, we have presented methods to encrypt images for a secure transfer purpose. We have shown that the quality of the encryption depends on the chosen crypto-system.
Encryption increases the entropy of the image and thus the number of bits necessary by pixel. To transfer medical images without losses we think that crypto-compression seems to be an interesting solution with a rate varying between 1.3 and 3.8. The crypto-compression is adapted to the encryption by blocks as TEA but it is not possible with stream-ciphers.

5. References

[Bor1 02] J.C.Borie, W.Puech, M.Dumas, *Encrypted Medical Images for Secure Tranfer*,International Conference on Diagnostic Imaging and Analysis ICDIA 2002, Shanghai, P.R China August 18-20 pages 250-255.

[Bor2 02] J.C.Borie, W.Puech, M.Dumas, *Encrypted images for Secure transfer with RSA algorithm* , International Conference, COMMUNICATIONS 2002 proceedings ,"Politecnica" University of Bucharest and IEEE romanian section, Romania, 5-7 december 2002 .

[Cao 03] F.Cao, H.K.Huang, X.Q.Zhou, *Medical image security in a HIPAA mandated PACS environment*, Computerized Medical Imaging and Graphics 27 (2003) pages 185-196.

[JPEG2000] http://www.jpeg.org/jpeg2000.

[LZ 77] J.Ziv, A.Lempel,*A Universal Algorithm for Sequential Data Compression*, *IEEE trans.Inform.Rheory*, 1977 vol.23, no.3, pp 337-343.

[LZ 78] J.Ziv, A.Lempel,*Compression of Individual Sequences via Variable-rate Coding,IEEE trans.Inform.Rheory*, 1978 vol.24, no.5, pp 530-536.

[Mani 01] S.S.Maniccam,N.G.Bourbakis,*Lossless image compression and encryption using SCAN*,Pattern Recognition 34 (2001) pages 1229-1245.

[Nor 03] R.Norcen, M.Podesser, A.Pommer, H.P.Schmidt, A.Uhl,
Confidential storage and transmission of medical image data,Computers in Biology and Medicine 33 (2003) pages 277-292.

[Puech 01] W.Puech, JJ.Charre and M.Dumas. Transfert sécurisé d'images par chiffrement de Vigenère. In NîmesTic 2001 .La relation Homme-Système: Complexe, Nîmes, France ,pages 167-171, dec 2001.

[TEA 94] http://www.ftp.cl.cam.ac.uk/ftp/papers/djw-rmn/djw-rmn-tea.html
TEA, a Tiny Encryption Algorithm,D.Wheeler, R.Needham, Computer Laboratory Cambridge University UK November 1994.

[WEL 84] T.A.Welch,*A technique for High-Performance Data Compression*, *Computer*,1984,vol.17,no.6, pp 8-19.

[Xia 97] Xiaobo Li,Jason Knipe,Howaed Cheng,*Image compression and encryption using tree structures*,Pattern Recognition Letters (1997) pages 1253-1259.