An Efficient Hybrid Method for Safe Transfer of Medical Images

William Puech

To cite this version:

William Puech. An Efficient Hybrid Method for Safe Transfer of Medical Images. E-MEDISYS'08: E-Medical Systems, Sfax, Tunisia. lirmm-00371816

HAL Id: lirmm-00371816
https://hal-lirmm.ccsd.cnrs.fr/lirmm-00371816

Submitted on 30 Mar 2009

An Efficient Hybrid Method for Safe Transfer of Medical Images

William PUECH[a,b]

[a]*LIRMM, UMR 5506 CNRS, University of Montpellier II*

161 rue Ada, 34392 Montpellier, France

[b]*University of NIMES, Place G. Péri, 30021 NIMES CEDEX 1, France*

william.puech@lirmm.fr

Abstract: The works presented in this paper show how encryption algorithms provide security to medical imagery. The main objective is to guarantee the protection of medical images during transmission, and also once this digital data is archived. The subsequent challenge is to ensure that such coding withstands severe treatment such as compression. For ethical reasons, medical imagery cannot be sent when such a risk is present, and has to be better protected. Encryption is the best form of protection in cases such as this. Many different techniques for the encryption of text already exist. In this paper we show how essential it is to ensure the security of medical imagery and data.

Key words: Image encryption, Data Hiding, Safe transfer.

INTRODUCTION

Nowadays, more and more digital images are being sent over computer networks. The works presented in this paper show how encryption algorithms give security in medical imagery. In order to do this, the images can be encrypted in their source codes in order to apply this functionality at the application level. In this way, the functionalities of encryption are inserted at the software level. We can therefore guarantee the protection of a medical image during transmission, and also once this digital data is archived. In the case of certain types of medical imagery, large homogenous zones appear. These zones affect the effectiveness of the coding algorithms. Nevertheless, these homogenous zones, useless for any diagnosis, can be safely used for the watermarking of medical images.

For ethical reasons, medical imagery cannot be sent when such a risk is present, and has to be better protected. Encryption is the best form of protection in cases such as this. Many different techniques for the encryption of text already exist. Since Ancient times, humanity has always attempted to encode secret messages in order to elude wandering indiscreet eyes and ears. The most basic forays into this field relied upon algorithms which allowed coding and decoding. Over time, the notion of a key arose. Today, encryption systems rely upon algorithms which are available to the world at large, and it is the key, a code which remains confidential, which allows for the encryption and decryption of the message [KER 83].

In Section 1 we will present the standard encryption algorithms and will show how these can be suited to medical imagery. In Section 2, we will show how it is possible to combine encryption and data hiding in these images, while retaining a high quality of image. Finally we will conclude in Section 3.

1. Medical image encryption

In this section, we will show how it is possible to apply the above algorithms to medical images in grey level. Because of the bidimensional characteristic of images, and their size, these standard algorithms must be modified in order to be used effectively on medical images. The aim of image encryption is to obtain an image in the same format and without a size bigger than the original image. Because of this, if a user does not possess the key, he does at least have access to an image in a known format. By carrying the encryption step up to the application level, it is possible to proceed, for example, towards a region of interest of the image. In the case of large images, it therefore becomes unnecessary to decrypt the whole image if we only want to view one particular area of it.

1.1. Image encryption by block

In the case of encryption by block, the length of the blocks is fixed, and varies from 64 bits (8 pixels) to 248 bits (32 pixels). From the bidimensional information of an image, several pixel grouping solutions are possible. In the aim of withstanding a downstream compression as well as possible, or compressing at the same time as the coding, it is useful to group the pixels with their nearest neighbours (in rows, columns, or blocks). Each block of pixels is encrypted separately. The encrypted block obtained will then come to replace the original block in the image. In this paper, the route taken for scanning the blocks is carried out only in a linear manner (scan line). Manniccam and Bourbakis show that it is often more useful to use other types of scanning (spirals, zigzags etc.) in order to combine encryption with lossless compression [MAN 01], [MAN 04].

1.2. Coding images by asynchronous stream cipher

In this section, we present an asynchronous stream cipher algorithm which is applied to images. Let K be a key of length k bits b_i, $K = b_1b_2...b_k$. The unit of encryption is the pixel (1 byte). The method lies in the fact that for each pixel of the image, the encryption depends upon the original pixel, the value of the key K, and the k/2pixels previously encrypted. For each pixel p_i of the original image, we calculate the value of the pixel p'_i of the encrypted image using the following equation:

$$\begin{cases} z_i = \left(\sum_{j=1}^{k/2} \alpha_j \, p'_{i-j} \right) \bmod (256) \\ p'_i = (z_i + p_i) \bmod (256) \end{cases} \quad (1)$$

with i ε [0,…,N−1] where N is the number of pixels in the image, k is the length of the key with k ε [1,N], and α_j is a sequence of k/2 coefficients generated from the secret key K.

The equations (1) have a recurrence of the order k/2, corresponding to half of the length of the key. The coefficients α_j are integer values included between -2 and +2 such as:

$$\begin{cases} \alpha_j = \beta_j - 1 & \text{if } \beta_j \in \{0,1,2\} \\ \alpha_j = \pm 2 & \text{if } \beta_j = 3 \end{cases} \quad (2)$$

with βj = $2b_{2j-1}$+$b2_j$, where b_{2j-1} and b_{2j} are two consecutive bits of the secret key K. In addition, the probability density of the α_j must be uniform in order to reduce the transmission errors during the decryption stage. The sign in front of the coefficients equals to 2 depends on the coefficients α_j in order to have:

$$\frac{1}{k/2} \sum_{j=1}^{k/2} \alpha_j \approx 0 \quad (3)$$

Considering that the encryption of a pixel is based on the k/2 pixels previously encrypted, we cannot encrypt the k/2 first pixels of the image. It is necessary to associate the α_j coefficients with a sequence of k/2 virtual encrypted pixels p'_{-i}, for i ε [1,…,k/2]. This pixel sequence corresponds to an initialisation vector (IV). In consequence, an IV is coded in the key: k/2 values of virtual pixels which allow us to encrypt the k/2 first pixels of the image as though they had predecessors. The length k of the key K must be big enough to guarantee maximum security. Equation (4) presents the decryption procedure. In the decryption procedure, we must apply the process in reverse. We can notice that the function which generates the dynamic key is the same as equation (1):

$$\begin{cases} z_i = \left(\sum_{j=1}^{k/2} \alpha_j \, p'_{i-j} \right) \bmod (256) \\ p_i = (p'_i - z_i) \bmod (256) \end{cases} \quad (4)$$

1.3. Applying encryption to medical images

Starting out with the image in Figure 1.a, we have applied the DES algorithm by blocks of 8 pixels in a row, with a 64-bit key to obtain the image in Figure 1.c. We can observe the appearance of textures (Figures 1.c-e). The reason for this phenomenon lies in the appearance of large homogeneous zones (black in this case) on the medical images. At the level of the histograms (Figures 1.d-f), we observe the strong presence of grey levels corresponding to the encryption of the grey levels of the homogeneous zones. The encryption is therefore very poor for two reasons: firstly because it is easy to guess the nature of the medical image (an ultrasound), but mainly because the availability of the value of the plaintext block (the pixels were all black), and after encryption (the grey levels dominating in the encrypted image) is a precious clue for cryptanalysts. Block encryption algorithms therefore present us with serious problems when images contain homogeneous zones.

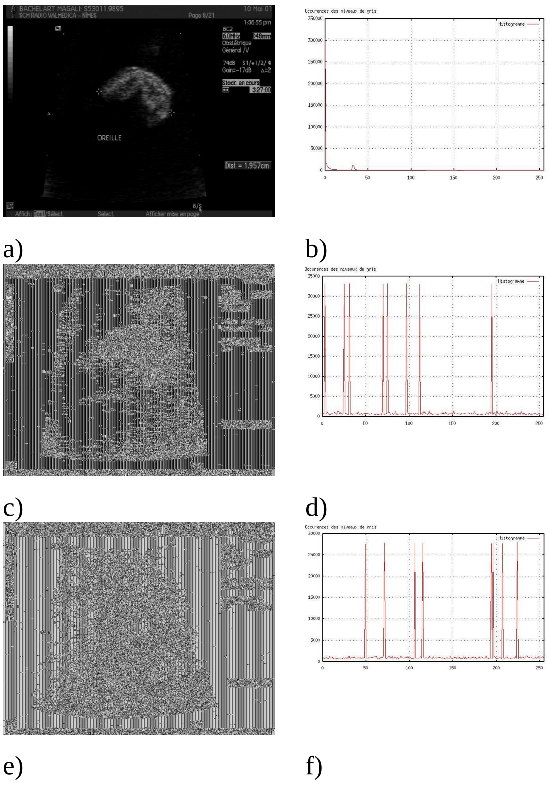

Figure 1. *a) medical ultrasound image (442KB), with large homogeneous zones,*
Encrypted image c) encrypted by DES algorithm (block of 8 pixels with a 64-bit key),
e) by AES algorithm (block of 8 pixels with a 128-bit key)
b), d), and f) histograms

From the original image, Figure 2.a (396x400 pixels), we have applied a stream cipher algorithm with a 128-bit key. Figure 2.c illustrates the values obtained for the dynamic key z_i generated by the equation (1). We can note that (Figure 2.d) the probability of the appearance of each value is practically equal. And so, the function generating the dynamic key g() produces a sequence with a large period and good statistical properties. From the equations (1), we obtain an encrypted image (Figure 2.e), and we can see that the initial image is no longer visible at all. By comparing the histogram of the initial image (Figure 2.b), with the histogram of the encrypted image (Figure 2.f), we can see that the density of probability of the grey levels is more or less identical. As a result, the entropies of the encrypted images are very high (around 8 bits/pixel).

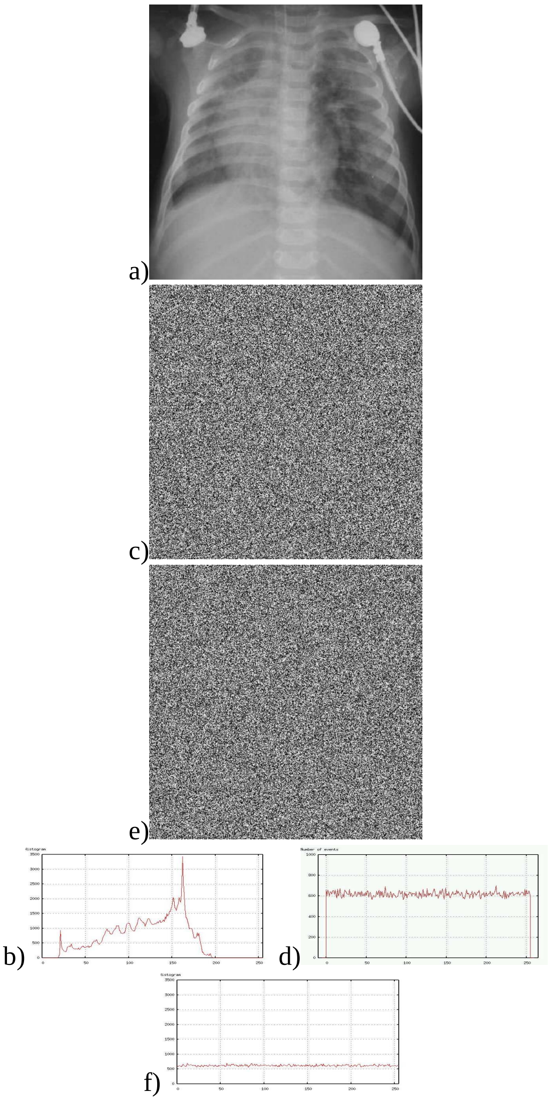

Figure 2. *a) original image, b) histogram of original image, c) image of the dynamic key z_i, d) histogram of the values of the dynamic key z_i, e) final encrypted image with the coding algorithm by asynchronous stream cipher, with a 128-bit key, f) histogram of the encrypted image*

Stream cipher has one major advantage over other encryption systems used in medical imagery. Because the result of the encryption of the previous pixels is taken into account for each pixel to be encrypted, the problem of homogeneous zones is solved. We are no longer dealing with block encryption systems, where two identical original blocks give the same encrypted block. We can observe that whatever the type of image with or without homogeneous zones, no texture appears in the encrypted images. In conclusion, in the case of stream cipher algorithms, the homogeneous zones are no longer visible either in the image or the histogram. Stream cipher method also carries another advantage: as the calculations which make it up are small in number, it proves to be very quick; even more so than AES. For example, a 7 MByte image is encrypted (or decrypted) in five seconds with a standard PC, rather than the 15 seconds required algorithms using a block encryption.

2. Confidentiality and integrity of medical images by data encryption and data hiding

The applications of watermarking medical imaging are numerous. In this section, we aim to illustrate the combination of cryptography and watermarking in secure image exchange. We know that the encryption process could be either symmetrical or asymmetrical, by block or by stream [SCH 97]. Whereas asymmetric algorithms are not appropriate for image encryption due to their calculation time, algorithms by block present security problems (due to homogeneous zones) and problems with the data integrity. Figures 3 demonstrate this problem. The AES block algorithm [AES 01] with a 128-bit key has been applied to the original image (Figure 3.a) in order to obtain the encrypted image Figure 3.b. If the encrypted image is modified during the transfer, it is not necessarily possible to detect this alteration. For example, in Figure 3.c a small region of the encrypted image has been copied and pasted onto another zone of the image. After decryption, it is possible to view the images, but their integrity cannot be guaranteed as shown in Figure 3.d.

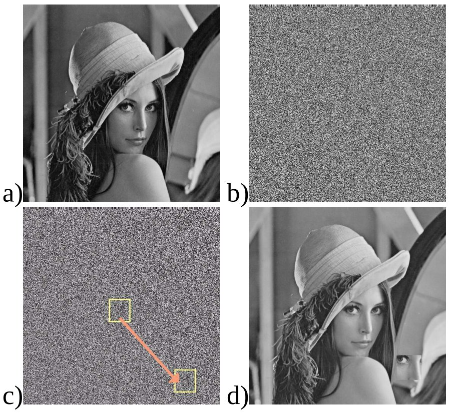

Figure 3. *a) original Lena image, b) image encrypted by AES by 128-bit block, c) copy of a region of the encrypted, pasted onto another zone, d) decryption of (c)*

In order to solve the integrity problem, it is possible to combine a stream cipher algorithm with a secret key for the image and an asymmetrical algorithm to encrypt the secret key. A substitutive watermarking method then allows for the embedding of the encrypted key into the encrypted image [PUE 04], [PUE 07a]. If person A sends an image over a network to person B, sender A will use a stream cipher algorithm with the secret key K to encrypt the image. To send key K, A can encrypt it using an algorithm with a public key such as RSA. Let pub(e,n) be the public key and priv(d,n) the private key for RSA with e = d^{-1}mod(n), so A has his public and private keys $pub_a(e_a,n_a)$ and $priv_a(d_a,n_a)$, and B has his public and private keys $pub_b(e_b,n_b)$ and $priv_b(d_b,n_b)$. As a result, A generates a secret key K for this session and encrypts the image with the stream cipher algorithm. Next, A ciphers the key with the RSA algorithm using his private key $priv_a$ in order to achieve a key K':

$$K' = K^{d_a} \bmod(n_a) \tag{5}$$

This key K' is encrypted a second time with RSA using the public key pub_b of the recipient B to generate K'':

$$K'' = K'^{e_b} \bmod(n_b) \tag{6}$$

The size of the message to be embedded into the image depends upon the size of the recipient's public key and is known to the sender A and the recipient B. We can therefore calculate the embedding factor and calculate the number of blocks required for the embedding. This key K'' is embedded into the ciphered image. Finally, A sends the image to B as shown in Figure 4. This procedure of K encryption with $priv_a$ and pub_b ensures the authenticity, and only B can decrypt the image. The embedding of the key into the image makes the method autonomous and guarantees its integrity. If, during transfer, the image is attacked, then it is no longer possible to extract the right key on reception, and so the image cannot be decrypted.

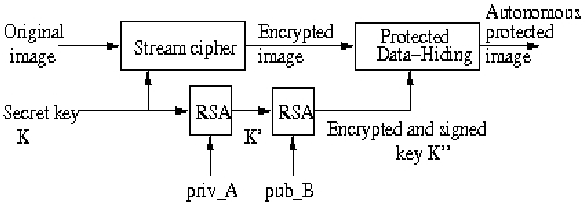

Figure 4. *Combination of secret key encryption, public key encryption, and a watermarking method*

Person B receives the encrypted and watermarked image, and can then extract the encrypted key K''. He can then identify the sender, A, and decrypt the key K'' using the private key $priv_b$ and the public key pub_a belonging to A:

$$K = (K''^{d_b} \bmod(n_b))^{e_a} \bmod(n_a) \tag{7}$$

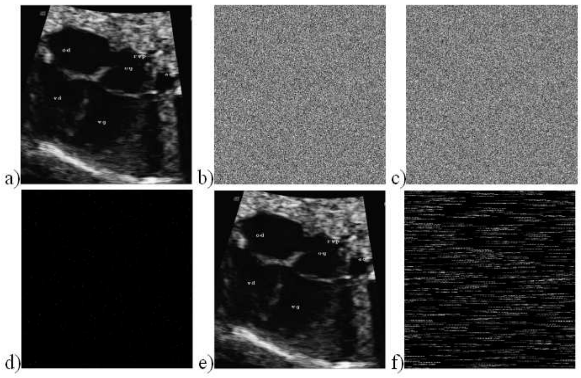

Figure 5. *a) original image, b) encrypted image with a stream cipher algorithm with 128-bit key, c) image (b) watermarked with the secret encrypted key, d) the difference between images (b) and (c), e) decryption of image (c), f) the difference between original image (a) and (e).*

With the acquired key K, B can decipher the image and therefore view it. Starting from the original ultrasound image (512x512 pixels), Figure 5.a, we have applied a stream cipher algorithm with a key K of 128 bits, in order to obtain the encrypted image Figure 5.b. If this image is decrypted, we can note that there is no difference between it and the original image. The 128-bit key K was encrypted twice with the RSA algorithm in order to obtain K''. Because of the length of B's public key, the length of K'' is in the region of 1024 bits. Next, using a watermarking technique in the spatial domain based on the LSB substitution, the key K'' is embedded into the encrypted image (Figure 5.c). The embedding capacity is of 1 bit for every 256 pixels. The difference between the watermarked, encrypted image and the original is shown in Figure 5.d. The pixels used for the embedding are visible, the PSNR = 75.14 dB. After the decryption of the watermarked, encrypted image, in Figure 5.c, we reach the final image shown in Figure 5.e. The difference between the original image and the final one is shown in 5.f. This Figure shows that the differences between the two images (PSNR = 55.28 dB) are spread throughout the image.

In order to compare the results of this hybrid method, the watermarking method was applied to the encrypted medical image using the AES algorithm with the ECB and OFB modes (stream cipher mode). After decryption, the image watermarked and encrypted by AES in ECB mode shows a great deal of variation compared to the original image (PSNR = 14.81 dB). After decryption, the image watermarked and encrypted by AES in OFB mode presents variations which were not diffused by this mode. The final image quality is good (PSNR = 52.81 dB) but an overflow problem remains with the OFB AES mode. The black pixels become white, and vice versa. In conclusion, the combination of encryption and watermarking allows for an autonomous transmission system, and guarantees the integrity of the data transmission.

3. Conclusion

In this paper, we have shown that there are many solutions for ensuring security when sending and storing medical images. In current practice, those solutions offered to secure medical data are based on very traditional protection techniques. These old approaches require either the introduction of certain specific mechanisms, or a longer execution time. These traditional approaches are not suitable for real-time applications or for access from a doctor's surgery. Some of the solutions proposed in this paper can be integrated into systems for sending medical images, if they can be proven robust. The main advantage of all these hybrid approaches is the ability to link several types of coding in one algorithm. In years to come, the appearance of standards in the encryption and watermarking of images will be of great benefit to the safe transmission of medical data [PUE 05], [PUE 07b].

References

[AES 01] AES. Announcing the Advanced Encryption Standard. Federal Information Processing Standards Publication, 2001.

[KER 83] Kerckhoffs A., « La cryptographie militaire », *Journal des sciences militaires*, vol. 9, p. 5-38, 1883.

[MAN 01] Maniccam S.S., Bourbakis N.G., « Lossless Image Compression and Encryption using SCAN », *Pattern Recognition*, vol. 34, p. 1229-1245, 2001.

[MAN 04] Maniccam S.S., Bourbakis N.G., « Lossless Compression and Information Hiding in Images », *Pattern Recognition*, vol. 37, p. 475-486, 2004.

[PUE 04] Puech W., Rodrigues J.M., « A New Crypto-Watermarking Method for Medical Images Safe Transfer », *In proc. EUSIPCO'04*, pp.1481-1484, Vienna, Austria, September 2004.

[PUE 05] Puech W.,. Rodrigues J.M., « Crypto-Compression of Medical Images by Selective Encryption of DCT », *In proc. EUSIPCO'05*, Antalya, Turkey, September 2005.

[PUE 07a] Puech W., Rodrigues J.M., « Method for Secure Transmission of Data», Licence WO 2007/045746, April 2007.

[PUE 07b] Puech W., Rodrigues J.M., Develay-Morice J.E., « A New Fast Reversible Method for Image Safe Transfer ». *Journal of Real-Time Image Processing (JRTIP), Springer*, vol. 2, n° 1, pp. 55-65, October 2007.

[SCH 97] Schneier B., «Applied cryptography ». Wiley, New York, USA, 1995.