A NEW CRYPTO-WATERMARKING METHOD FOR MEDICAL IMAGES SAFE TRANSFER

W. Puech and J.M. Rodrigues.

Laboratory LIRMM, UMR CNRS 5506, University of Montpellier II
161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE

william.puech@lirmm.fr, jose-marconi.rodrigues@lirmm.fr

ABSTRACT

This work presents a new method that combines image encryption and watermarking technique for safe transmission purpose. This method is based on the combination of public-private keys and secret key ciphering, and watermarking. The encryption algorithm with secret key is applied to the image. We encrypt the secret key with an encryption method based on public-private keys. Then, this secret key is embedded in the encrypted image. We apply and show the results of our method to medical images.

1. INTRODUCTION

The amount of digital medical images has increased rapidly in the Internet. The necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images became a daily routine and it is necessary to find an efficient form to transmit them over the net. In this paper we propose a new technique to encrypt an image for safe transmission.

Our research deals with image encryption and watermarking. There are several methods to encrypt binary or grey level images [3, 2, 11].

Watermarking can be an answer to make secure image transmission. For applications dealing with images, the watermarking objective is to embed invisibly message inside the image data. The length of the transmitted message can be relatively important, in fact, longer that just for identification. Insertion can be made in a different way according to the length of message or desired robustness. The combination in the spatial and frequency domains for the image watermarking is also possible [10].

An encryption method which depends on the secrecy of the encryption algorithm is not considered to be a true encryption method [8]. In the same way, watermarking algorithms are well-known. The existing encryption methods are based on secret keys and not on secrecy of encryption algorithms. In the traditional approach, the image is encrypted with a secret key method, and the secret key is encrypted with a public key encryption. The problem is to transfer, in same time, the encrypted secret key and the encrypted image.

The encryption can be done by block or by stream. But the encryption block methods have presented two inconvenients applied to image. The first one was when you have homogeneous zones, all blocks of this kind are encrypted on the same manner. The second problem was that block encryption methods are not robust to noise. The stream cypher method is robust to moderate noise like JPEG compression with hight quality factor. To embed the encrypted secret key in the image we have used a new DCT-based watermarking method [5]. We have chosen to work in the frequency domain because of the robustness to JPEG compression of the stream cypher method. An important application is the secure transfer of medical image [1, 6].

In the Section 2, firstly we present encryption algorithm per flux, then we explain how to apply to images this method. Section 3, we describe the combination method. Section 4, we apply the methods and the combination to medical images.

2. STREAM CIPHER

2.1 The general method

Algorithms of flux ciphering (stream ciphers) can be defined as being algorithms of ciphering by blocks, where the block has an unitary dimension (1 bit, 1 byte, etc.) or relatively small. Their main advantages are their extreme speeds and their capacity to change every symbol of the plaintext. Besides, they are less numerous than those of ciphering by blocks, they are useful in an environment where mistakes are frequents, because they have the advantage of not propagate them (diffusion) [4].

The most widespread and used coding stream ciphers are the synchronous, and the most widely used is the RC4 [9]. The algorithm RC4 has been thought in 1987 by Ron Rivest and has been developed for the RSA Security. It is based on the random permutations into the byte. The algorithm has a variable key length (of 1 to 256 bytes). The key is used to initialize a table of 256-byte states. This table is used for the pseudo-random byte generation to produce a random pseudo flux with which the plaintext will be transformed.

Current interest in stream ciphers is most commonly attributed to properties of the one-time pad, called the Vernam cipher [12]. It uses a string of bits that is completely random generated. The keystream has the same length as the plaintext message. The random string is combined using *exclusive OR* operations with the plaintext to produce the ciphertext.

The Linear Feedback Shift Register (LFSR), illustrated Figure 1, is a mechanism very often applied in applications that require very fast generation of a pseudo-random sequence. The symmetrical ciphering uses LFSR to generate some pseudo-random bit sequences called register's vector. This vector is generally the key of the ciphering process and it is defined in relation to a meter. For every iteration, the content of the register is baffled toward the right of a position, and the XOR operation is applied on one under whole of bits whose result is placed to the left extreme of the register.

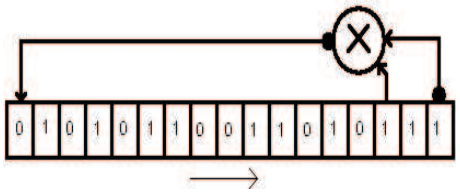

Figure 1: Linear Feedback Shift Register (LFSR).

2.2 Image encryption by stream cypher

Generally, the private key length of the stream ciphering can be eventually as long as the length of the message. The method detail resides in the fact that for every pixel the encryption depends previously of the original pixel value, of the key, and of the k pixels previously ciphered [7].

For every pixel $p(n)$ of the original image, if k is the length of the key, we calculate the pixel value $p'(n)$ of the ciphered image using the equation:

$$\begin{aligned} p'(n) &= p(n) + \alpha(1)p'(n-1) + \alpha(2)p'(n-2) \\ &+ \ldots + \alpha(k-1)p'(n-k-1) + \alpha(k)p'(n-k), \end{aligned} \quad (1)$$

with $n \in [k,N]$, $k \in [1,n]$ and $\alpha(\iota)$ a sequence of coefficients generated by the secret key, N is the number of image pixels. The equation (1) can be written where k, recurrence order, corresponds to the length of the key:

$$p'(n) = p(n) + \sum_{\iota=1}^{\iota=k} \alpha(\iota)p'(n-\iota), \quad (2)$$

where the $\alpha(\iota)$ are the integer coefficients the order -2 to $+2$. The principle of ciphering is illustrated in Figure 2.

Another information also appears in the key. Indeed, considering that the ciphering of a pixel takes account of the k previous pixels, we can not cipher the k first pixels of the picture in the same way. It is necessary to associate the sequence of $\alpha(\iota)$ coefficients with a sequence of k pixels therefore virtually encrypted $p'(-\iota)$, for $\iota \in [1,k]$, corresponding to the vector of initialization. We have showed that it is possible, with this algorithm, to express $p'(n)$ only from initial data preceding the pixel to be ciphered [7]. Therefore, a vector of initialization is coded in the key: k values of virtual grey levels on which lean the k first pixels as if they were their predecessors.

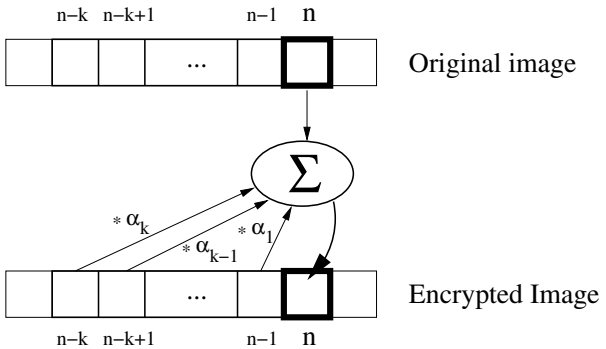

Figure 2: Pixel encryption by stream cipher.

The chosen value of k must be larger enough to turn the system safe. Suppose $k = 64$, we have still 2 bits per coefficient, an effective 128-bit key. In relation to the initialization vector, we showed that it was necessary for ciphering the k first pixels, but it is secondary for security point of view. We did not give him the supplementary place in the key, but their values are deducted from the effective key of 128 bits, by an operation that we have defined. This operation is based merely on a sliding window that reads bits of the key. The window reads the first 8 bits for the first virtual pixel, then it baffles itself on the key, to read the next 8 new bits.

3. DESCRIPTION OF THE COMBINATION METHODS

In this section we describe how it is possible to combine the technics of encryption and watermarking in images. Indeed, we constructed a new method with encryption algorithm with secret key for the image, with encryption based on public-private key for the secret key and with watermarking method. For example, if a medical doctor M wants to send, by network, a medical image to a specialist S, it should be made in a safe way. To do that, the doctor M can use a fast encryption algorithm with secret key K to cipher the image. In order to transfer K, M can encrypt the key K by using encryption algorithm with public key, like RSA for example [9]. If pub is a public key and $priv$ a private key for RSA, then M possesses the public and private keys pub_m and $priv_m$, and S the public and private keys pub_s and $priv_s$.

Firstly, M generates a secret key K for this session and ciphers the image with this encryption algorithm. Secondly, M should encrypt the key K with RSA algorithm by using his private key, $priv_m$, in order to get an encrypted key K'. This encrypted key K' is encrypted twice with RSA by using the public key pub_s of his corresponding S in order to get K''. This encrypted key K'' is then embedded in the ciphered image by using a DCT-based watermarking method [5]. Finally, the doctor M sends this image to the specialist S as presented in Figure 3.

The specialist S receives the image and extracts from it the encrypted key K''. He can then authenticate M and decrypt the key K'' by using his self private key $priv_s$ and the public key pub_m of M. With the obtained key K, S can then decipher the image and visualize it.

If the specialist S wants to send an other image to the doctor M, he will use a new secret key K_1 for this new session. The process will be the same, but the private and public key for RSA will not be applied in the same order.

Even, if five keys are necessaries for each session, most of them are transparents for the users. Indeed, the private key can be associated to the software used by the receptor, and for the two correspondants it is not necessary to know the secret key which is encrypted and embedded in the image. However, for each session the value of the key K must change. Otherwise, if the key has no changing, all the people who have the software can decrypt the images.

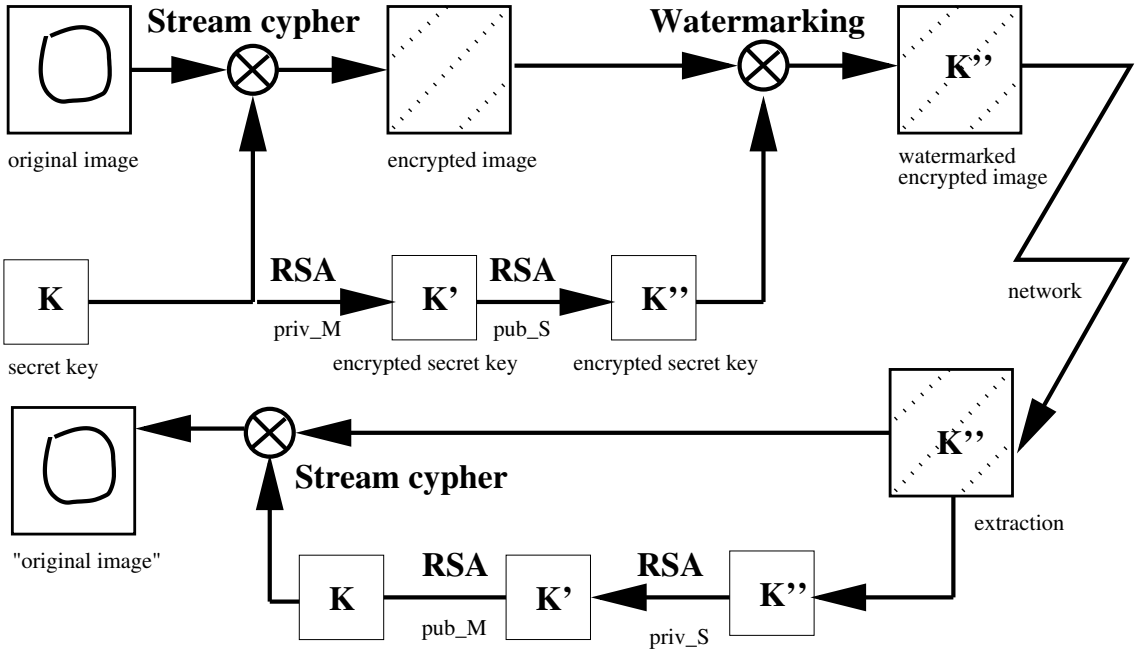

Figure 3: Combination of public key encryption, secret key encryption, and watermarking.

4. RESULTS

From the image, Figure 4.a, we have applied the stream cypher algorithm with a key of 128 bits. We notice that the initial information is not any more visible. By comparing the histogram of the initial image, Figure 4.c with the histogram of the encrypted image, Figures 4.d, we remark that the probabilities of appearance of each grey level are equitably distributed. Consequently, the entropies of the encrypted images are very hight (near 8 bits/pixel).

We present now the results of the combination of encryption and watermarking methods. From the original image, Figure 5.a, we apply the stream cypher method to obtain the encrypted image, Figure 5.b. If we decrypt this image, we can noticed that there is no difference. The length of the key is 128 bits. Then, we embed the RSA encrypted key in the encrypted image, Figure 5.c. The difference between the encrypted and the watermarked encrypted images is presented Figure 5.d. We see the pixel blocks where we have embedded our message (encrypted key), the $PSNR = 42.12\ dB$. Finally, after decryption of the watermarked encrypted image we obtain the image illustrated in Figure 5.e. The difference between the original image and the decrypted watermarked one is presented Figure 5.f. We see, Figure 5.f, that the differences between this two images are spread out in the image region where we have embedded the message, the $PSNR = 43.71dB$. Indeed, owing to the fact that the mean value of the coefficients $\alpha(\imath)$ is equal to zero, the noise due to the watermarking is attenuated during the decryption process.

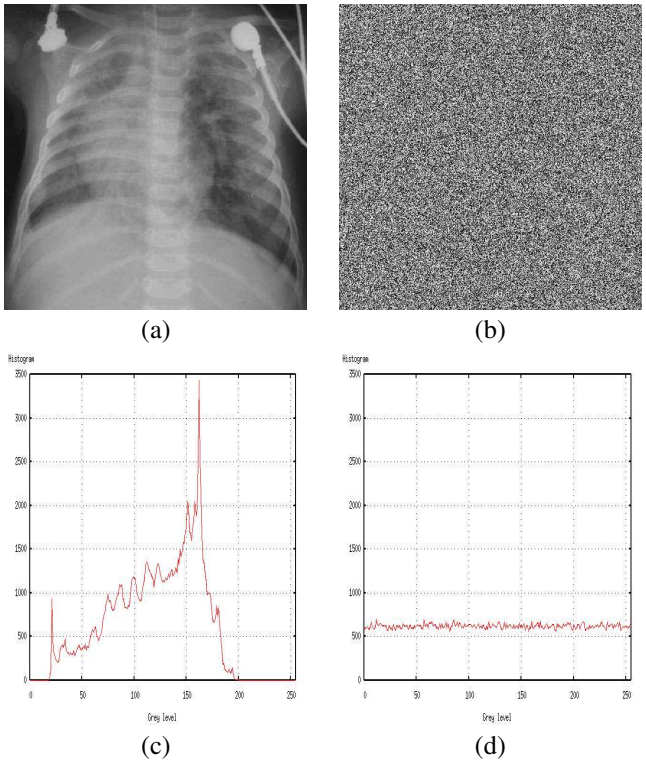

Figure 4: a) Original image, b) Encrypted image with the stream cypher algorithm, with a key of 128 bits, c) Original image histogram, d) Histogram of the encrypted image by stream cypher algorithm.

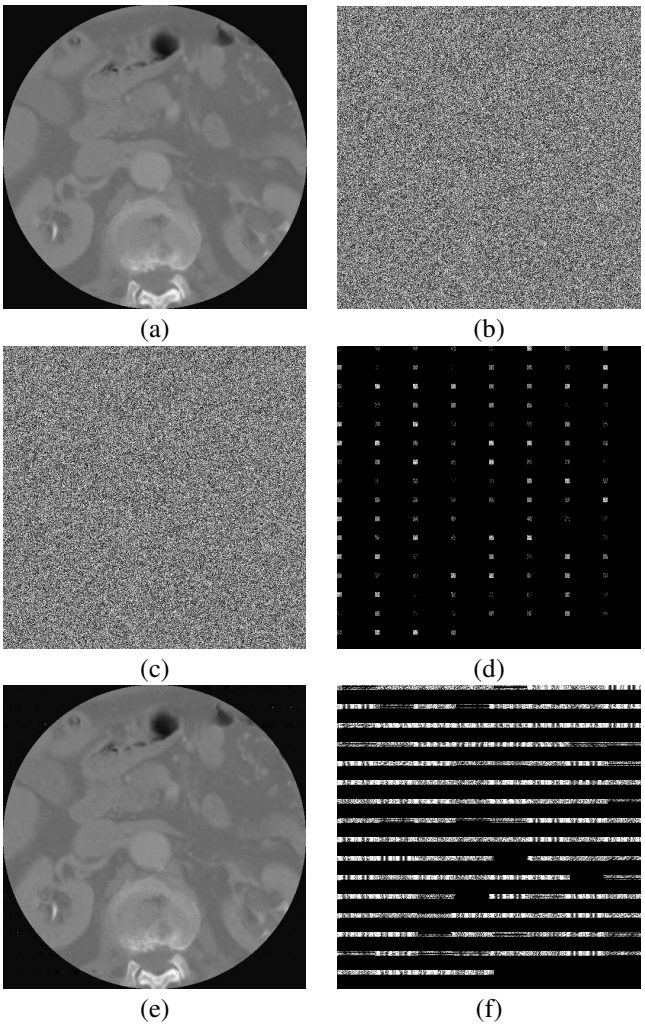

Figure 5: a) Original medical image, b) Encrypted image, c) Watermarked encrypted image with the 128-bit key, d) Difference between the encrypted image and the watermarked encrypted image, e) Decryption of the watermarked encrypted image, f) Difference between original image and the decrypted watermarked one.

5. CONCLUSION

In this paper we have presented a method combining encryption and watermarking for image safe transmission purpose. To do that, we have used the advantage of both encryption algorithm with secret key and with public-private keys. In our combination method, we have chosen to encrypt the image with secret key method, and to encrypt the secret key with public and private key method.

The stream cypher method is robust to moderate noise like JPEG compression with hight quality factor. To embed the encrypted secret key in the image we have used a new DCT-based watermarking method [5]. We have chosen to work in the frequency domain because of the robustness to JPEG compression of the stream cypher method.

We have applied part of our method (encryption) to medical images and finally we have presented a result of the full combination method on medical image.

REFERENCES

[1] J. Bernarding, A. Thiel, and A. Grzesik. A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encrytion. *International Journal of Medical Informatics*, 64:429–438, 2001.

[2] C.C. Chang, M.S. Hwang, and T-S Chen. A new encryption algorithm for image cryptosystems. *The Journal of Systems and Software*, 58:83–91, 2001.

[3] K.L. Chung and L.C. Chang. Large encrypting binary images with higher security. *Pattern Recognition Letters*, 19:461–468, 1998.

[4] S. Guillem-Lessard. http://www.uqtr.ca/∼delisle/Crypto. 2002.

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

[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] W. Puech, J.J. Charre, and M. Dumas. Transfert sécurisé d'images par chiffrement de Vigenère. In *NimesTic 2001, La relation Homme - Système : Complexe, Nîmes, France*, pages 167–171, Dec. 2001.

[8] B. Schneier. *Applied cryptography*. Wiley, 1995.

[9] RSA Security. http://www.rsasecurity.com/. 2003.

[10] F. Y. Shih and S. Y.T. Wu. Combinational image watermarking in the spatial and frequency domains. *Pattern Recognition*, 36:969–975, 2003.

[11] A. Sinha and K. Singh. A technique for image encryption using digital signature. *Optics Communications*, 218:229–234, 2003.

[12] G.S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *In Journal of the American Institute of Electrical Engineers*, 45:109–115, 1926.