A new selective encryption technique of JPEG2000 codestream for medical images transmission

Zahia BRAHIMI[1], Hamid BESSALAH[1], A. TARABET [1], M. K. KHOLLADI [2]
[1]Centre de Développement des Technologies Avancées, BP 17, Baba Hassen Alger - ALgérie
Tél : 213 21 35 10 40, Fax : 213 21 35 10 39
[2] Université Mohamed Mentouri de Constantine

Abstract: - In this paper, a novel selective encryption image scheme based on JPEG2000 is proposed, which encrypts only the code-blocks corresponding to some sensitive precincts. In order to improve the security level we introduce the permutation of codeblocks contributing in the selected precincts. Symmetric encryption AES with CFB mode is used to encrypt swapped codeblocks.

The idea of combining permutation and selective encryption is used in order to minimize the amount of processed data encryption while ensuring the best possible degradation through the permutation.

The proposed process encryption doesn't introduce superfluous JPEG2000 markers in the protected codestream, i.e, the protected codestream format is compliant to JPEG2000 codestream one. It keeps file format and compression ratio unchanged and doesn't degrade the original error robustness. The proposed scheme works with any standard ciphers and introduces negligible computational cost.

Key-Words: - Security, JPEG2000 Compression, Selective Encryption, AES,codeblocks, permutation, medical images,

1 Introduction

With the development of multimedia technology, the research on multimedia encryption becomes a hot topic. For the properties of larges volumes and real time requirement, multimedia data are difficult to be encrypted by traditional ciphers completely or directly. Therefore, better encryption algorithms are required. The latest international still image compression standards JPEG 2000 [1] is widely used and make it necessary to study image encryption based on JPEG2000 codec. Some algorithms have been reported [2]-[4] in the literature. They keep file format unchanged and are often low cost. However, they are secure enough against attacks.

The processing time for encryption/decryption is a major bottleneck in image and video communication and processing. Moreover, we must also take into account the processing time required for compression/decompression and for other processing [5].

Chang and Liu [6] noted that is still difficult to perform both compression and encryption quickly. Researchers have proposed methods to combine compression and encryption into a single process to reduce the total processing time [7][8] but these methods are insecure or too computationally intensive. Partial or selective encryption is proposed to reduce encryption and decryption time in image and video communication and processing.

In practice, partial encryption algorithms are more suitable for most applications since they obtain high speed by encrypting only some sensitive data [9].

Norcen and all [10-11] proposed a selective encryption scheme for JPEG2000 bitstream which encrypts 20% of the compressed bitstream except format information. However, this scheme is not suitable for all the encoding modes.

Pommer[12] proposed a selective encryption scheme for wavelet-packet encoded images, which is of low cost. But, it encrypts only tree structure while no coefficients' value, so the security can't be confirmed for different images.

In [13-14], others algorithms are proposed for selective encryption for jpeg2000 codec. These schemes are of low cost and support direct bit-rate control, but they are not secure against known plaintext and or select plaintext attacks.

Here, we propose an image encryption scheme based on JPEG2000 Codec for medical images. This scheme is based on the precincts organisation in jpeg 2000 for selecting sensitive data to encrypt where corresponding codeblocks are also permuted. This combination is used to improve the security of the image and reduce the amount of data to be encrypted. The rest of the paper is organised as follows. In section 2, a brief overview of the JPEG 2000 structure is given. In Section 3, the encryption scheme is proposed. And its performances of compute complexity, bit-rate control are analyzed in section 4.

Finally, some conclusions are drawn and future work is proposed in section 5.

2 JPEG2000 Codestream Structure

JPEG 2000 is a wavelet-based image coding standard [15]. It is based on a scheme originally proposed by Taubman and known as EBCOT [16]. JPEG2000 scheme operate on independent, non-overlapping blocks which are coded in several bit layers to create an embedded scalable bitstream. In JPEG 2000, an image can be partitioned into smaller rectangular region called tiles. Each tile is encoded independently. Data in a tile is divided into one or more components in a colour space. A wavelet transform is applied to each tile component to decompose it into different resolution levels The wavelet coefficients are quantized by a scalar quantization to reduce the precision of the coefficients except in the case of lossless compression. Each Subband is portioned into rectangular blocks, known as "code-blocks" each of is independently encoded.

Packets are the most fundamental building blocks of JPEG 2000 codestreams. A packet is identified by four parameters: C (Component), R (Resolution level), P (Precinct) and L (Layer Quality). They can be sorted with respect to these four parameters in Five progression order: LRCP, RLCP,RPCL, PCRL and CPRL.

3 Proposed Method

Although each code-block is coded independently, their bitsreams are not explicitly identified within a JPEG2000 data stream. Instead, code-blocks are collected into larger groupings known as "precincts". The region occupied by image resolution LLd is partitioned into multiple precincts. Each precinct on LLd consists of the code-blocks belonging to the same spatial region, within subbands LLd+1, HLd+1 and HHd+1 (if d<D) or within subband LLD (if d=D) (Figure 1.).

Each precinct is represented as a collection of packet with one packet by layer.

We propose a secure encryption scheme, where only some sensitive precincts of the entire image are encrypted. The codestream is parsed to select only packets containing code-blocks which belong to the selected precincts. The remaining packets are sent without encryption.

In a case of color image, Precincts are selected from each component (Y,Cb,Cr).

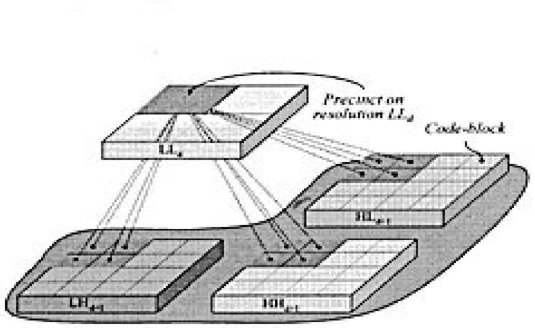

Fig 1. Precincts, Resolution and Code –Blocks

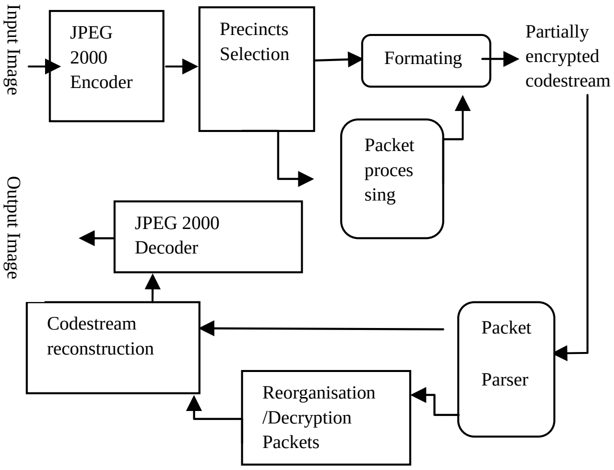

Fig 2. Encoding and encrypting precincts with AES-CFB

To perform a compliant encryption, we have to output a protected codestream whose length is the same as that of the input codestream, and words in the output encrypted bitstream is not in the interval [0xFF90,0xFFFF].

Block diagram of encoding and encrypting is described in Fig 2.

The formatter receives non encrypted and encrypted packets and works to reconstruct a compliant partially permuted/encrypted codestream. The block packets processing is used to only encrypt codeblocks or to permute and encrypt them. The permutation of codeblocks contributing in the selected precincts is introduced to improve the security level.

The idea of combining permutation and selective encryption is used in order to minimize the amount of processed data encryption while ensuring the best possible degradation through the permutation.

First, a pre-processing stage is performed where data packets are separated from packets headers using the markers included within the codestream.

Only the codes blocks of the first packet are interchanged. The number of packets to be treated is increased until a threshold of the image quality PSNR (Peak Signal-to-Noise Ratio) degradation is reached.

Actually, the PSNR remains stable after a number of permutations. This is illustrated in Fig 3., where tests were achieved using three different medical images.

Codeblocks permutation is performed to scramble the image, but can not secure the content of the image as an encryption has not been introduced. To ensure the image security, AES (Advanced Encryption Standard) [17][18] with CFB (cipher feedback)[19] mode is used as a block cipher with variable data length to encrypt all interchanged codeblocks. Indeed, this combined method permits to reduce the amount of data to be encrypted. Fig 4- Illustrates the amount of data to be encrypted when only encryption is used and the case of permutation and encryption. We can observe that for the same medical image, best performances are achieved when combining codeblocks permutation and encryption.

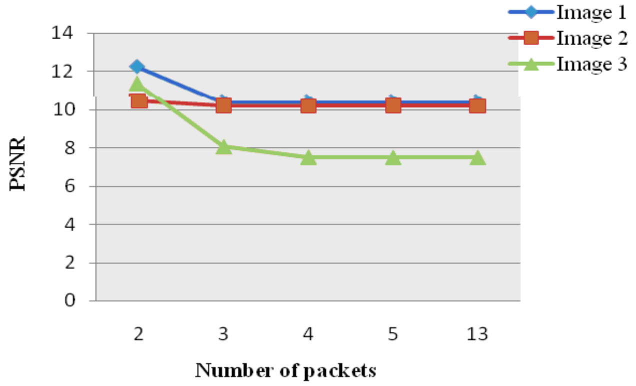

Fig 3. PSNR obtained using only permutation operation

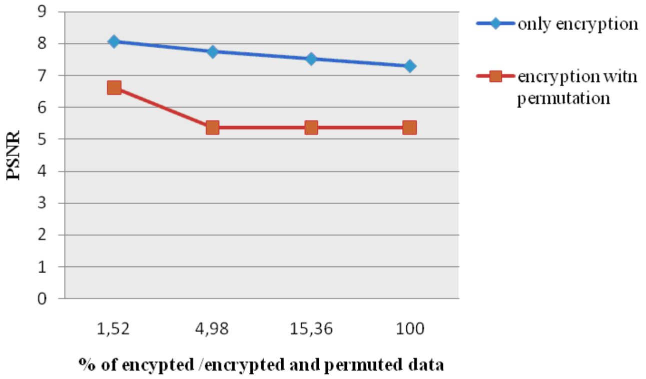

Fig 4. PSNR evolution depending on amount (%) of encrypted data

The encryption key and information about the permutation operation are encrypted using RSA (Rivest Shamir Adlema) Algorithm before transmitting them.

For the image reconstruction, inverse process is followed using permutation information to reorganise permuted codeblocks and the key encryption for decrypting it.

4 Experiments Results

Various experiments have been done to exam the performances of the proposed selective encryption scheme. Various medical images were taken as original images and decomposed into 3-level DWT coefficients. Shown results were obtained with a 256x256X8bits radiological image. The Kakadu 2.2.3 was used as JPEG 2000 Coder. All performances were performed by a Pentium 4, 2.8 GHZ personal Computer.

For selecting the precincts candidates for the “Packet Processing”, we achieve tests on most interesting subbands of the image which are:

- All precincts contained in all the LL_i (i=0...3)
- All precincts contained in the LL0
- All precincts contained in the LL0 and in all subbands of the third resolution(R=3)

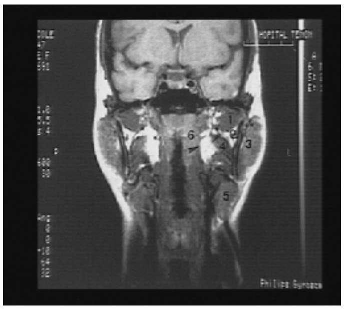

Fig 5. Original 256x256 radiological image

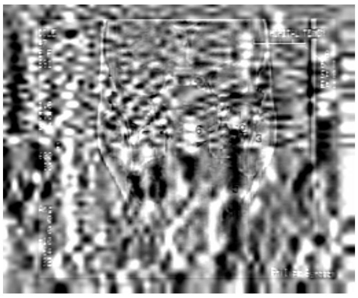

Fig 6. Encrypted radiological Image
PSNR : 7,47 dB, encrypted data=11,64%

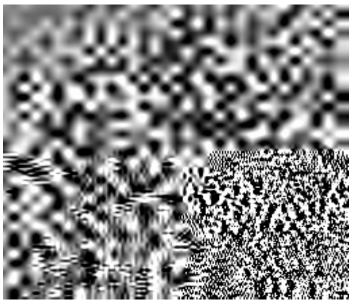

Fig 7. Encrypted radiological Image with permutation PSNR : : 6,74 dB, encrypted data=11,64%

The best performances are obtained in the third case. Actually, we obtain interesting PSNR values in this case. The results shown below are obtained by precincts of the LL0 subband and those contained in the subbands of the third resolution(R=3).

Fig 6. shows that using only encryption doesn't perform good performances even if the PSNR = 7,47 dB. The encrypted image contains visual information (visible contours). When permutation is associated (Fig 7), not only visual information disappear, but also the value PSNR is improved (6,74dB).

5 Conclusion

A new selective encryption scheme is presented in this paper. This scheme is based on combining permutation and selective encryption in order to minimize the amount of processed data encryption while ensuring the best degradation through the permutation.

Good performances are achieved on medical images. Only 11% of the packets data are encrypted for very interesting values of the PSNR. Good performances are also obtained with the other kind of images.

Future work consists on improving this selective encryption scheme for medical images by using data hiding technique to transmit permutation information and the encryption key.

Also, we work on selecting packets of one or several ROIs (Region Of Interest) of medical images, where encryption would concern header packets also.

References:

[1] ISO/IEC 15 444-1 : Information Technology-JPEG 2000 Image Coding System –Part 1 : Core Coding System (2000).

[2] Y. Wu, D.Ma & R. H. Deng," Progressive protection of JPEG2000 Codestreams," Proc. IEEE Conference on ImageProcessing- pp 3447-3450, Singapore, Oct. 2004.

[3] O. Watanabe,A. Nakazaki & H. Kiya, "A fast Image-Scramble method using public-Key encryption allowing backward compatibility with JPEG2000", Proceedings of the 2004 International Conference on Image Processing (ICIP 2004), Singapore, October 24-27, 2004, IEEE pp. 3435-3438.

[4] R. Grobois,P. Gerbelot, T. Ebrahimi, "Authentification and Access Control in the JPEG2000 Compressed Domain", Proc. Of the SPIE 46th Annual meeting, Applications of digital image processing XXIV, July 29th-August 3rd, 2001.

[5] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, ",A new encryption algorithm for image cryptosystems", The journal of Systems and Software vol. 58, September 2001, Pages 83-91-Elsevier

[6] Chang H.K.-C.; Liu J.-L. , "A linear quadtree compression scheme for image encryption," Signal Processing Image Communication, Volume 10, Number 4, September 1997, pp. 279-290(12).

[7] N. Bourbakis and C. Alexopoulos, "Picture data encryption using scan patterns," Pattern Recognition, vol. 25, no. 6, pp. 567–581, 1992.

[8] Y. Matias and A. Shamir, "A video scrambling technique based on space filling curves," in Proc. CRYPTO , 1988, pp. 398–417.

[9] S. Lian, J. Sun,D. Zhang, and Z. Wang,"A selective Image Encryption Scheme Based on JPEG2000 Codec", Lecture Notes in Computer Science
Vol. (3332/2004) Advanced in Multimedia Information Proceesing PCM 2004.

[10] R. Norcen, M.Podesser, A.Pommer, H. P. Schmidt, A. Uhl, "Confidential storage and transmission of medical data", Computers in Biology and Medecine 33/3, 2003 , PP 277-292.

[11] R. Norcen, A. Uhl," Selective encryption of the JPEG2000 Bitsream",,Lecture notes in computer science, Volume 2828/2003 – Communication and Multimédias Security.

[12] A. Pommer, A. Uhl, "Selective Encryption of Wavelet-Packet encoded Image Data --- efficiency and security", ACM Multimedia Systems (Special issue on Multimedia Security), 9(3):279-287, 2003.

[13] V. Conan, Y. Sadourny and S. Thomann,"Symmetric Blocks Cipher Based

Protection : Contribution to JPSEC,"ISO/IEC JTC I/SC 29/WG1 N2771,Oct.2003.

[14] Y. Wu, R. Deng and Di Ma ," Im Access : A Method for JPEG 2000 Access Control," Presentation on 29th ISO/ IEC JTC 1/SC 29/WG 1 meeting, Seoul March 2003.

[15] D. Taubman, Michael W. Marcellin," JPEG2000 Image Compression Fundamentals,Stqndards and Practice", The springer International series in Engineering and computer science, 2002 Springer Science+Businees Media, Inc.

[16] D. Taubman, "High Performance Scalable Image Compression with EBCOT", IEEE Transactions on Image Processing, vol. 9, N°7, July 2000.

[17] National Institute of Standards and Technology: FIPS 197: Advanced Encryption Standard, November 2001

[18] J. Daemen and V. Rijmen, AES Proposal: Rijndael (Version 2). NIST AES Website; http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndaelammended.pdf

[19] M. Dworkin, SP 800-38A 2001, "Recommendation for Block Cipher Modes of Operations," December 2001.