Selective Encryption Techniques 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
zbrahimi@cdta.dz http://www.cdta.dz

Abstract: - In this paper, novel selective encryption image schemes based on JPEG2000 are proposed. The first one 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. 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.
Many of proposals format compliant encryption schemes for JPEG2000 that have been made encrypt packet body data, but leave header packet in plaintext. The second approach, combines code-blocks data encryption to a cyclic permutation of all packets headers in the bitstream. Actually, in the JPEG2000 codestream, packet header information is specific to the visual content, and it is can be used as a fingerprint of the codestream.
Symmetric encryption AES with CFB mode is used to encrypt in the two schemes.
The proposed schemes don't introduce superfluous JPEG2000 markers in the protected codestream, i.e, its 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: - Communication system security, JPEG2000 Compression, Selective Encryption, permutation, medical images, Computer applications.

1 Introduction

With the development of multimedia technology, the research on multimedia encryption becomes a hot topic. Digital images are used more and more widely in our lives. The security of digital images has been concerned because they can be accessed on the internet without any effort. The security of digital images involves several different aspects, including copyright protection, authentication, confidentiality, and access control.

Generally, the copyright protection is addressed by digital watermarking which embeds the owner's private information, called watermark, into the original image and extracts it when the ownership needs to be resolved. On the other hand, content confidentiality and access control are addressed by encryption, through which only authorized parties holding decryption keys can access content in clear text. Intuitively, we can apply generic encryption to digital images before or after compression. If we encrypt an image before compression, the statistical and structural characteristics of the original image could be significantly changed, resulting in much reduced compressibility. Moreover, much more computational overhead will be introduced. If we directly encrypt the compressed code, relatively small computational overhead will be introduced, but it may destroy the syntax of the encoded codestream. As a consequence, the encrypted bitstream cannot be decoded by generic image decoders. Also, for the properties of large 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 and watermarking [2,3] based on JPEG2000 codec. Some algorithms have been

reported [4]-[6] in the literature. They keep file format unchanged and are often low cost. However, they are not 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 [7].

Chang and Liu [8] 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 [9][10] 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.

Selective encryption is a technique which only encrypts a portion of a compressed bitsream. Consequently, selective encryption is sometimes called partial encryption. An important property of the selective encryption is that the encrypted and unencrypted portions of the compressed bitstream can be exactly decode and displayed. According to the selective encryption schemes proposed in the literature, an efficient selective encryption should possess the following basic properties:

(1) Compressibility equivalent : the size of the encrypted code should be similar to that original compressed code.
(2) Complexity equivalent: The computational averhead added to a compression scheme should be as small as possible.
(3) Backward compatible: the encrypted code should be decoded by generic image decoder.
(4) Computationally secure: the key space should be large enough to resist the attack of exhaustive key structure.

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 [12-13] 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[14] 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 [15,19], 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 two image encryption schemes based on JPEG2000 Codec for medical images.

The First scheme is based on the precincts organisation in jpeg 2000 for selecting sensitive data to encrypt where corresponding codeblocks are permuted. This combination is used to improve the security of the image and reduce the amount of data to be encrypted. The second scheme uses the first scheme combined to packets header permutation to improve its performances. 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 procedure is presented. Proposed schemes are detailed in section 4, their performances in terms of compute complexity, bit-rate control are analyzed in section 5. Finally, some conclusions are drawn and future work is proposed in section 6.

2 JPEG2000 Codestream Structure

The image compression standard JPEG2000 has been defined for use in various multimedia applications such as good quality at high compression ratios, scalability, and region of interest to mention few. The JPEG2000 project (ISO/JTC 1 15444) was born with the goal to create a new coding system for different types of still images : bi-level, grey level, colour and muticomponent with different characteristics : natural images, scientific, medical , remote sensing, text, … allowing different imaging models such as client /server, real time

transmission, image library archival, and limited buffer.

JPEG 2000 is a wavelet-based image coding standard [20][21]. It is based on a scheme originally proposed by Taubman and known as EBCOT [22]. 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 partitioned 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.

2.1 Pecincts, Layers and Packets Strucrure

JPEG2000 uses an extensive mechanism to format the encoded coefficient to the final datastream. In the last cioding step, all grouped and encoded coefficients of a subband covered by one cell of a defined regular grid are combined to a precinct. The cell size of the grid can be chosen independently for every resolution level. For every resolution level precinct-triples (HL, LH, HH) are created by concatenating precincts belonging to the same spatial region. Thus, the structure represents the complete encoded information of a spatial region at a particular resolution level. To enable the SNR Progressive refinement, it is necessary to spread this information using a number of layers. Every layer contains a certain amount of data from the considered precincts. This partial data from precinct-triple is formatted and called a packet. If there is no information to include, an empty packet is created. The whole procedure is done on every resolution level, precinct and layer. The resulting packets are formatted to the final datastream. A single packet can be decoded independently from another, but it doesn't carry any tag to derive its position. This information is derived from a fixed packet order and the position of the packet in the final stream.

A packet comprises a packet header and a part of the bit-stream from an entropy coded binary image. Therefore, the final generated JPEG 2000 Compressed data consist of multiple such packets and a mian header. Packet header is a portion of a packet that provides auxiliary information about the binary data that follows. The coded binary data of each packets comes from at least one complete code-block.

In the JPEG2000 codestream, the main header contains general information on the bitstream. The information is too general to infer from it anything substantial with regard to the specific visual content. The situation is different for the packets headers where information is specific to the visual content, and it is specific to be used as a fingerprint of the codestream. Four properties are contained in the header packet [23]:

- The zero length packet, locates the first of the packet header and consists of one bit. Zero means that the packet has no body data.
number of leading zeo-bitplanes : shows the number of zero bitplanes from the significant bit-plane.

- The inclusion information of each codeblock: Commonly, when a layer structure is used, code-blocks are related to multiple layers, and the image data in the code-blocks is distributed to each layer according to its contribution to image quality. The codeblock inclusion shows the distribution coded by tag-tree coding and is after the zero length packet area

- The number of coding passes for each codeblock: Arithmetic coding is done for multiple sub-bitplanes, and are separated from wavelet coefficients. The sub-bit plane is called the coding pass. Coding pass show

the number of coding passes in a current packet.
- Length of the code-block compressed image data from a given codeblock.

3 Encryption Procedure

We employ AES (Advanced Encryption System) in CFB (Cipher Feed-Back)mode for data encryption, since in this mode, an arbitrary number of data bits can be encrypted, which is not offered by the ECB (Electronic Code Book) and CBC (Cipher Block Chaining) encryption modes.
The AES algorithm mainly consists of a symmetric block cipher that can process data blocks of 128, 192 or 256 bits by using key lengths of 128, 196 and 256 bits. The algorithm is based on round function, and different combinations of the algorithm are structured by repeating this round function different times. The number of rounds depends on the size of the key and the size of the block data. Each round function contains uniform and 4 parallel steps, Byte Substitution, Row Shifting, Column Mixing and Key Addition, and each step has its own particular functionality. A full description of the AES is detailed in the Rijndael proposal [24,25].

An encryption algorithm is never used stand-alone for security reasons. Therefore, it is combined with
so-called modes of operation. Reference [26] shows the US National Institute of Standards and Technology recommendations for block cipher modes of operation. These are Electronic Code Book (ECB), Output Feed-Back (OFB), Cipher Block Chaining (CBC), and Cipher Feed-Back (CFB) modes of operation.
In ECB encryption, the forward cipher function is applied directly and independently to each block of the plaintext. The resulting sequence of output blocks is the ciphertext.
The Electronic Codebook (ECB) mode is a confidentiality mode that features, for a given key, the assignment of a fixed ciphertext block to each plaintext block, analogous to the assignent of code words in a codebook. In ECB encryption and ECB decryption, multiple forward cipher functions and inverse cipher functions can be computed in parallel.
In the ECB mode, under a given key, any given plaintext block always gets encrypted to the same ciphertext block. If this property is undesirable in a particular application, the ECB mode should not be used.
The Cipher Block Chaining (CBC) mode is a confidentiality mode whose encryption process features the combining ("chaining") of the plaintext blocks with the previous ciphertext blocks. The CBC mode requires an IV (Initialization Vector) to combine with the first plaintext block. The IV need not be secret, but it must be unpredictable.

The Cipher Feedback (CFB) mode is a confidentiality mode that features the feedback of successive ciphertext segments into the input blocks of the forward cipher to generate output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. The CFB mode requires an IV as the initial input block.

The Output Feedback (OFB) mode is a confidentiality mode that features the iteration of the forward cipher on an IV to generate a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. The OFB mode requires that the IV is a nonce, i.e., the IV must be unique for each execution of the mode under the given key.

The Counter (CTR) mode is a confidentiality mode that features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. The sequence of counters must have the property that each block in the sequence is different from every other block. This condition is not restricted to a single message: across all of the messages that are encrypted under the given key, all of the counters must be distinct.

4 The Proposed Methods

For selectively encrypting the JPEG 2000 bitsream, we need to achieve format compliance. Since the aim is to operate directly on the bitstream without any decoding we need to discriminate packet dat from packet headers in the bitsream . This can be achieved by using two

special markers “Start Of Paccket : SOP” and “End of Packet Header: EPH”. The packet header is located between SOP and EPH, packet data finally may be found between EPH and the subsequent SOP.

Almost proposals for format-compliant encryption scheme for JPEG2000 that have been made only encrypt packet body data, and leave header dat in plaintext. In this paper, we show that introducing permutation of header packets increase the confidentiality.

Two selective encryption schemes of the codestream JPEG2000 are detailed in this paragraph. The aim is to improve security level of the medical images without increasing the amount of the data to encrypt.

4.1 Selected Codeblocks Permutation and Encryption

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).

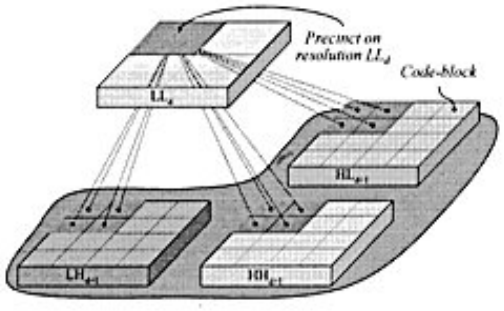


Fig 1. Precincts, Resolution and Code –Blocks

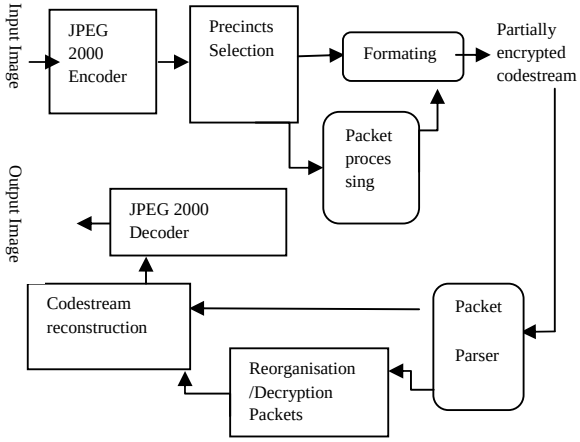


Fig 2. Encoding and encrypting precincts with AES-CFB

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.

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.

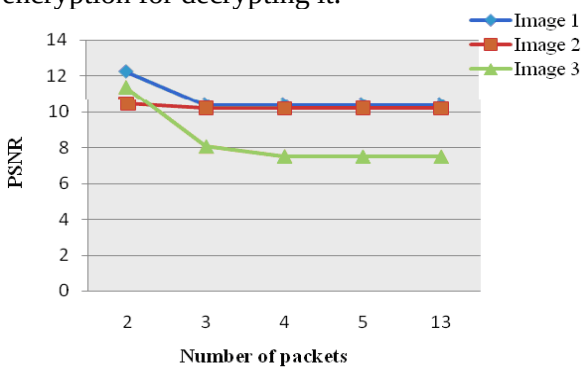


Fig 3. PSNR obtained using only permutation operation

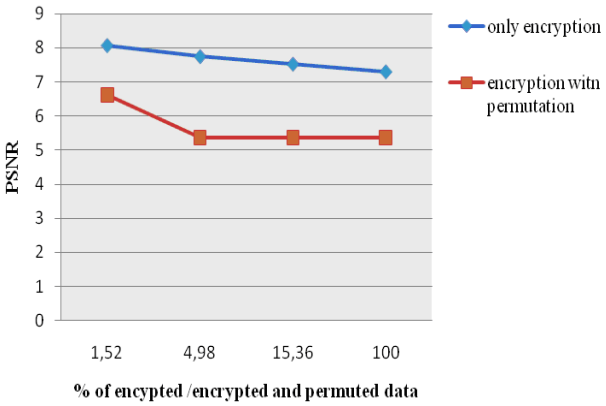


Fig 4. PSNR evolution depending on amount (%) of encrypted data

4.2 Codeblocks encryption combined to packets header permutation

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] corresponding to the markers. Fig 5. shows a block diagram of the basic idea. The JPEG2000 codestream input into the Selection Precincts Block where sensitive precincts i.e corresponding packets are selected.

Selected packets and the remaining codestream input into the packets analyser. All packets headers are separated from the bodies packets. Then, we process a cyclic permutation of all the header packets, when we encrypt only bodies of selected packets.
The cyclic permutation of all the packets header of the bitsream permits to destroy the information needed to create a strong fingerprint of the bitstream by creating confusion. Only a little percentage (less than 10% of data bodies) is necessary to encrypt the codestream. The AES (Advanced Encryption Standard) with CFB mode is used as a block cipher to encrypt data.
The remaining bodies packets in the codestream are coded and sent without encryption.
The formatter reconstruct the new bitsream with all permuted packets headers, encrypted bodies of selected packets and remaining ones.

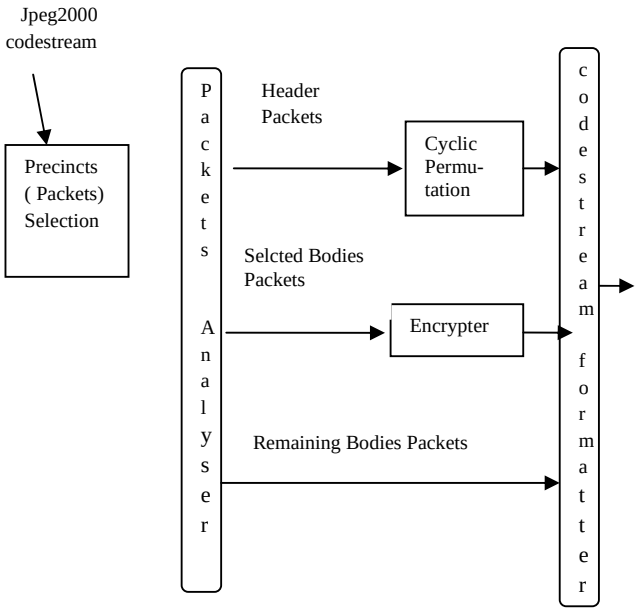


Fig 5. Diagram showing the process of selective encryption combined to packets header

5 Experiments Results

Various experiments have been done to exam the performances of the proposed selective encryption schemes. 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 tests were performed on a Pentium 4, 2.8 GHZ personal Computer.

For selecting the precincts candidates for the "Packet Processing", in the first approach, we achieve tests on most interesting subbands of the image which are:

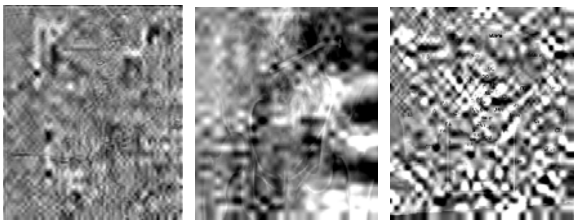
- All precincts contained in all the LL_i (i=0...3)
- All precincts contained in the LL0
- All precincts contained in the LL0 and in all subbands of the third resolution(R=3)

The best performances are obtained in the third case. Actually, we obtain interesting PSNR values in this case. The results shown below are obtained for 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 = 7,37 dB. The encrypted image contains visual information (visible contours). When permutation is associated (Fig 7 (c)), not only visual information disappear, but also the value PSNR is improved (6, 28 dB).

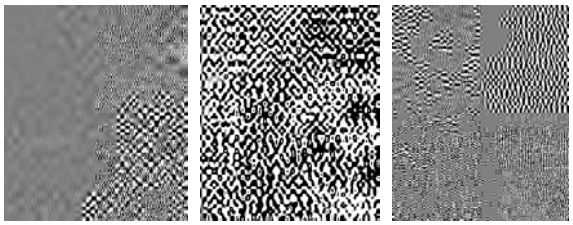
(a) Hematological (b) Radiological (c) Neurological

Fig 6. Original medical images



(a) Hematological	(b) Radiological	(c) Neurological
Psnr= 12,98 dB	Psnr= 7,74 dB	Psnr= 7,37 dB
13,22 % of data	11 % of data	8,77 % of data

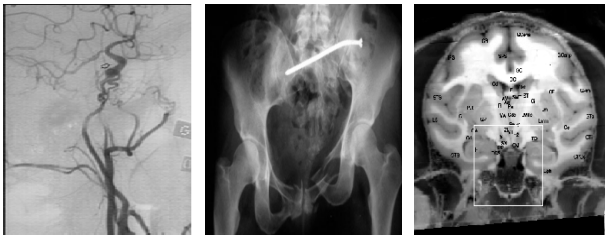
Fig 7. Encryption of sensitive precinct's codes blocks



(a) Hematological	(b) Radiological	(c) Neurological
Psnr= 9,79 dB	Psnr= 5,36 dB	Psnr= 6,28 dB
13,22 % of data	11 % of data	8,98 % of data

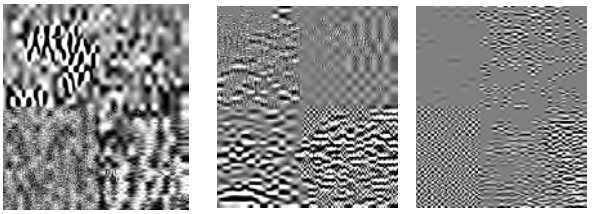
Fig 8. Performances of cyclic Permutation combined to encryption of selected codes blocks

For the second approach, tests are done on various medical images. Results for three medical images (hematological, radiological and Neurological ones) shown in Fig 9., are discussed here.
In all the following figures, images are referenced by (a) for hematological image, (b) for Radiological and (c) for neurological ones.



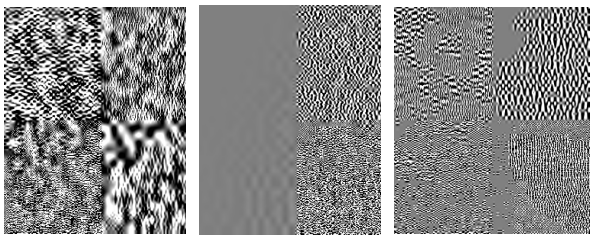
(a) Hematological (b) Radiological (c) Neurological

Fig 9. Original Medical Images



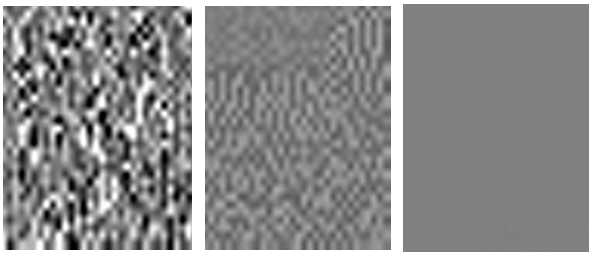
(a) Psnr= 8,48 dB (b) Psnr=7,40 dB (c) Psnr= 8,19 dB

Fig 10. Performances of only cyclic Permutation of all packets header



(a) Psnr= 7,18 dB, 8,7532 % of data (b) Psnr= 7,65 dB, 10,4772% of data (c) Psnr= 6,26dB, 8,7723% of data

Fig 11. Performances of cyclic Permutation of all packets header combined to encryption of selected bodies data



(a) Psnr =10,88 dB, 8,7532% of data (b) Psnr= 10,45dB, 10,4772% of data (c) Psnr = 9,89 dB, 8,7723% of data

Fig 12. Zero Concealment

Figure 10. Shows results achieved by only cyclic permutation of all packets header without any encryption. Figure 11. Shows results achieved when we combined permutation of the packets headers and packets bodies encryption
We achieved very good performances for the three images with only packets header cyclic permutation (PSNR=7,40 dB for radiological images). This result is explained by the fact that packet header information is important for visual content.
On other hand, we evaluate performances of the selective encryption combined to the packets headers permutation. We obtain best performances (PSNR=6,26 dB) for Neurological and hematological images (Figure 11.) and equivalent ones for Radiological one.

The image content and structure influence the encryption performances. Actually, we note that, for the hematological and neurological images, only 8,7 % of bodies data were necessary for encryption. This percentage corresponds to the three first packets. When 10,4 % of data, corresponding to the two first packets, was necessary to encrypt the radiological image.

For the security evaluation, we exploit a built-in resilience functionality to simulate a bitsream-based replacement attack. If an error is detected during decoding, the affected data is cancealed and no more passes should be decoded for this code-block's bitsream. Therefore, the encrypted packets are simply ignored during decoding. Results of decoding operation are shown in Figure 12. No visual information appear on the images (PSNR = 9,89 dB for neurological image).

6 Conclusion

Computationally efficient techniques for confidential transmission of medical images have been discussed. We propose two partial encryption techniques where partial encryption is combined to a permutation of selected codeblocks in the first approach. In the second approach, encryption is combined to a permutation of the packets headers of corresponding. Best performances are obtained with the latest one because header packets information is very important in the codestream reconstruction.

The amount of data subjected to encryption while maintaining high confidentiality is significantly reduced as compared to full encryption. Less than 10% of data is encrypted.

The proposed schemes do not decrease the compressibility and do not increase the complexity of the standard JPEG 2000 coder. Equivalent performances are obtained with and without selective encryption scheme. The output encrypted codestream is compliant with the JPEG2000 and can be easily decoded.

Results show that packet header security is very important. Future work focuses on improving these schemes for medical images by using Region of Interest in the codestream JPEG2000 and introducing an adequate encryption of the packets header.

References:

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

[2] K. Yoon, S.Choi, S. Bae & al,"Adaptive Block Watermarking and its SOC Implementation Based on Jpeg2000 DWT", *Proceedings of the 7th WSEAS International Conference on Signal, Speech and Image Processing, Beijing, China, September 15-17, 2007,PP 183-186.*

[3] R. Alvarez, F.M. Martinez, J. F. Vicent and A. Zamora,"A New Public Key Cryptosystem based on Matrices", *6th WSEAS International Conference on Information Security and Privacy, Tenerife, Spain, December 14-16, 200,PP 36-39.*

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

[5] 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.

[6] 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.

[7] 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

[8] 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).

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

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

[11] 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.

[12] 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.

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

[14] 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.

[15]V. Conan, Y. Sadourny and S. Thomann,"Symmetric Blocks Cipher Based Protection *: Contribution to JPSEC,"ISO/IEC JTC I/SC 29/WG1 N2771,Oct.200*3.

[16] 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.*

[17] S. Lian,J. Sun,D. Zhang and Z. Wang,"A selective Image Encryption Scheme Based on

Jpeg 2000 Codec",*Lecture Notes in Computer Science* vol (3332/2004). Advanced in Multimedia Information Processing 2004.

[18] J. L. Liu, " Efficient selective encryption for JPEG2000 images using private initial table", *The journal of pattern recognition society*, *39* (2006) 1509-1517.

[19] D. Engel, T. Stutz, and A. Uhl, " Format compliant JPEG2000 encryption with combined Packet Header and packet body protection", *MM&Sec'07*, September 20-21, 2007-Dallas,USA.

[20] 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.

[21] M.S.Bhuyan,N. Amin,MD.Azrul Hasni Madesa, MD.Shabiul Islam," An Efficient VLSI Implementation of Lifting Based Forward Discrete Wavelet Transform Processor for JPEG2000", *Proceedings of the 7th WSEAS International Conference on Signal, Speech and Image Processing, Beijing, China, September 15-17, 2007,PP 177-182.*

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

[23] M. Kurosaki ;A.IKEDA,K. Munadi and H. Kiya,"Packet analyser for JPEG2000 codestreams and its VHDL Model", the 2004 IEEE Asia-pacific Conference on Circuits and Systems 6-9 december ,2004, PP 905-908.

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

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

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