Effective Crypto-compression Scheme for Medical Images

Med Karim ABDMOULEH and Med Salim BOUHLEL
University of Sfax
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology
Sfax–Tunisia
medkarim.abdmouleh@isggb.rnu.tn, medsalim.bouhlel@enis.rnu.tn

Abstract: The use of telecommunications and information technologies in the medicine sector were evolved breathtakingly last years. This involves the developpement of the applications bound to the telemedicine. Seen the importance of this discipline in the improvement of the care quality, the reduction of treatment costs, and in the universalization of the medical practices and knowledges, the optimization of medical related applications remains a necessity. In this meaning, we propose in this work an efficient scheme for the transmission and the storage of medical images. This scheme is applied to the on line medical folder sector that is, currently, one of the most potential sector in telemedecine. A new approach concerning the integration of the partial encryption in compression algorithms based on the RLE encoding technique, will be presented and developed.

Key–Words: Telemedecine, RLE, Encryption, Triple DES, Crypto-compression.

1 Introduction

Telemedicine is a discipline which is currently undergoing considerable development due to the remarkable development of information and telecommunications technologies, thus improving both the quality of care and the costs of treatment. The online medical records industry is one of the most recent applications that are derived from Telemedicine. This is a new service offered by a few companies on the Internet that gives anyone the opportunity to put their personal medical information in a secure online file. The major advantage of this type of service is accessibility. In case of emergency, the data stored in the patient's file will be immediately available to the doctors of the emergency service via a secret key that the patient must have on him at all times. Therefore, this service allows to consult the patient's file whatever its state of consciousness, and wherever an accident may occur. This sector is currently considered among the most potential sectors.

Since the effectiveness of this type of application depends essentially on two fundamental criteria, which are the degree of security with which medical data are transmitted, stored and consulted, and how quickly they are consulted, a new effective scheme for securing and optimizing the transmission of medical images, which are the main components of online medical records.

The rest of this paper is organized as follows. The principle of our approach is described in section 2. Section 3 presents the principle of the proposed scheme. The advantages of the proposed scheme are discussed in section 4. Finally, conclusion is drawn in section 5.

2 Principle of our approach

2.1 Position of Problem

In medical applications, the size of digital images is very important. Therefore, they must be compressed in order to improve the storage and archiving capacity and to optimize their transmission across the networks (speed of transmission and reduction in network congestion). In addition, the encryption of medical images is necessary in order to ensure the confidentiality of personal medical data during transfer to the network, and also during the period in which the information is stored on the internet [3]. To satisfy these two conditions, the classical approach (Fig. 1) consists in applying an independent encryption algorithm to the data after the compression step [1]. In the case of online medical records, the problem lies in the time required for the encryption-decryption operation generated by the conventional algorithms. This time is too large and can't meet the needs of physicians, especially since the need for consultation of these records only arises in a case of extreme urgency where a few seconds can save a patient's life. Many methods have been developed to combine compression operations and encryption to reduce processing

time [12, 9, 8, 5, 4]. According to [6], these methods are either unsafe or very demanding in terms of computation time.

In this work, we propose a new approach which consists in performing a partial encryption on the compression algorithms using the RLE coding technique [2] (Fig. 1). Its application in the JPEG compression standard is envisaged.

2.2 The proposed scheme

Based on the JPEG compression process, Fig. 2 illustrates our block diagram, which consists in performing partial encryption with the Triple DES encryption algorithm [10] on the data which is encoded by the RLE. To restore the initial information, the same decompression process as that of the JPEG is applied, but with an additional step of performing a decryption just before the RLE decoding step (Fig. (3).

3 Development of the approach

In this section, we will first present the encryption algorithm adopted in our scheme. We will define the RLE coding technique in order to develop our approach.

3.1 Cryptosystem: Triple DES

3.1.1 DES

The DES (Data Encryption Standard) [7] was the global standard for more than 17 years. It was derived from a code called "Lucifer" developed by IBM for the N.B.S. (National Bureau of Standards). It is a 64-bit block encryption system, that is it accepts 64-bit input and provides 64-bit encrypted output. The DES uses a 56-bit K-key. From the key K, 16 subkeys (K_1, ..., K_{16}) are retrieved in a deterministic way by 48 bits each. The DES algorithm mainly uses Shannon's two major laws: scattering (using bit permutations) and confusion (using bit substitutions) to break redundancy in the data structure, and complicate the link between the Encrypted file and the secret key used [11].

3.1.2 Triple-DES

The size of the secret key (56 bits) of the DES algorithm now makes it vulnerable to exhaustive key search attacks. This is why most applications now use the Triple-DES algorithm [10] which consists simply of applying three successive DES digits. There are several variants of this algorithm:

- DES-EEE3: Three DES encryption with three different keys.
- DES-EDE3: Three DES operations in the sequence encryption - decryption - encryption with three different keys.
- DES-EEE2 and DES-EDE2: Same sequence as EEE3 and EDE3 but with the use of the same key for the first and last operation. The two-key
- DES-EDE2 is adopted in the ANSI X9.17 and ISO 8732 standards. It is widely used for banking applications.

In our case, we opt for the second method DES-EDE3 insofar as the use of three different secret keys allows us to increase the security of the algorithm with respect to an attack by exhaustive search of keys. In fact, the DES-EDE2 makes it possible to obtain a key of length 112 bits, against a key of 168 bit for the DES-EDE3 and this while maintaining the same robustness as the DES-EDE2. The Triple-DES, is a well-known algorithm. Indeed, there is not until today an attack that is both practical and effective against this algorithm.

3.2 Partial encryption with RLE

The coding technique known as RLE (Running Length Encode) is not a statistical technique but it is a very interesting technique in the case of image compression by TCD (in particular JPEG compression). Indeed, after the quantization step, most of the DCT coefficients are truncated to zero values. The RLE encoding exploits this property and encodes the contents of the block by recording information about the value and position of the coefficients. RLE encoding is actually a combination of two types of encodings. The first coding is an encoding of the sequence lengths of null values. The second coding is an integer coding of variable length. If one considers the principle of coding with the RLE technique, one notes that the data resulting from a compression with the RLE algorithm are divided into two parts. Indeed, for encoding a sequence length, the encoder emits two values. The first value is a zero value used to indicate that it is a coding of a sequence of zeros. The second value is the number of consecutive zeros. For encoding a non-zero coefficient, the encoder also transmits two numbers. The first is the number of bits used to code the coefficient. The second is the amplitude of the coefficient to be coded [2].

The basic idea of our approach is as follows: since the RLE algorithm, in both types of coding, gives

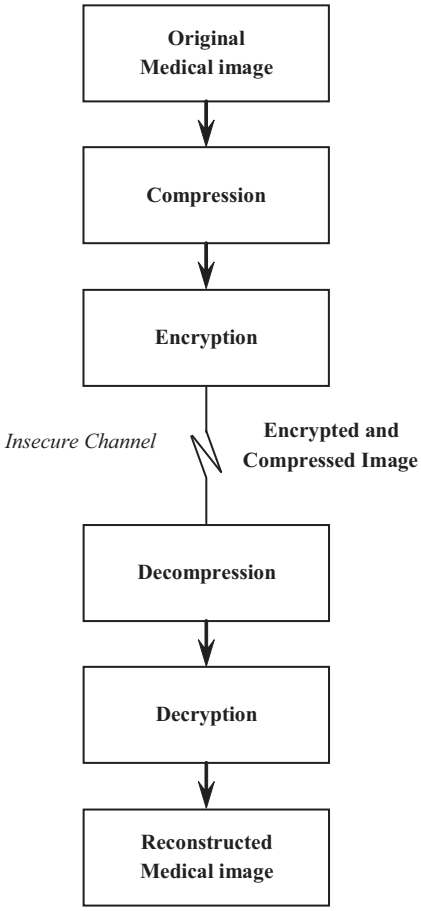

Figure 1: Classical approach

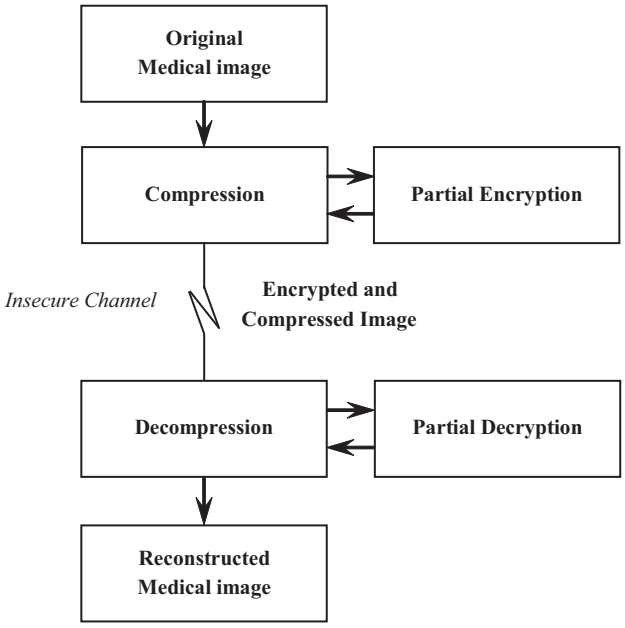

Figure 2: Proposed approach

two types of information that are complementary: sequences and sequence lengths then it is enough to encrypt a small parts whose size is multiple of 64 bits to make the reconstitution of the image impossible.

The attack on such an encryption method can only be performed if the encryption algorithm with which the data has been encrypted is broken.

It should be noted that it is necessary to add to the file, partially encrypted, the bit size of the part on which the encryption was performed in order to be able to reconstitute the initial image.

4 Advantages of the proposed scheme

- Our schema is very fast. Indeed, our approach allows a reduction of at least 90% of the processing time during the encryption-decryption process since only a small part of all the information contained in the file ensuring thus the total illegibility of the image.

- Our scheme perfectly preserves the performance of the JPEG standard in terms of compression ratio, because, on the one hand, the partial encryption that has been applied is done after the RLE encoding step, and the compression ratio depends essentially from this stage. On the other hand, the Triple DES encryption algorithm processes 64 bits as input and gives 64 bits to the output.

- In our scheme, we use a symmetric encryption algorithm that is fast and convenient [1]. Indeed, in cryptography, there are two categories of encryption algorithms: symmetric algorithms (with secret key) and asymmetric (public key) algorithms. In our application, we adopted a symmetric algorithm for its speed. Indeed, the symmetric algorithms are much faster than the asymmetric algorithms [11] and this represents an advantage

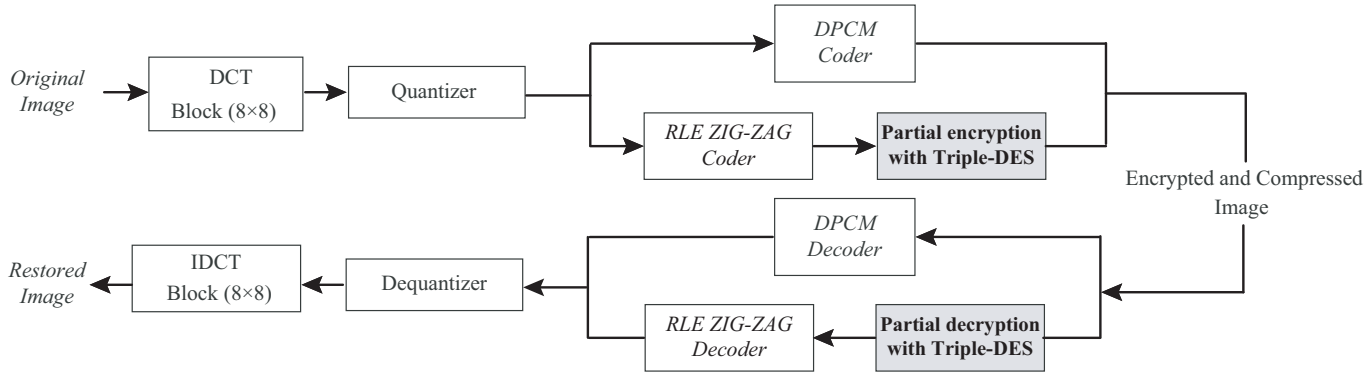

Figure 3: Diagram for our approach

in the field of online medical records because in most cases they are consulted in cases of extreme urgency, although the speed could make the algorithm sensitive to cryptanalysis (attack) by the greedy method.

- Our scheme is adapted to the online medical records sector. Indeed, asymmetric algorithms use two different keys: the first, called public key, for encryption, and the second, called private key, is used for decryption. On the other hand, symmetric algorithms such as Triple DES use the same secret key for encryption and decryption [11], which represents a major advantage in the case of securing online medical records. Indeed, a person wishing to ensure the confidentiality of his file, will be able to encrypt it with a secret key that he will choose himself. However, this person must have it with him constantly so that in case of emergency, the medical frame that will take care of it can immediately access his medical file (Fig. 4).

5 Conclusion

In this paper, an efficient crypto-compression scheme of medical images has been presented in which an approach has been developed concerning the integration of encryption within compression algorithms using the RLE encoding technique, in particular JPEG. This scheme is adapted to the online medical records sector. It makes it possible to reduce the processing time in the encryption-decrypting process in a notable way thus improving the management and the speed in the transmission of the medical images on the one hand, and the storage capacity in the servers on the other hand.

Our approach has the advantage of being applicable in several sectors related to telemedicine such as tele-diagnosis, tele-expertise and tele-consultation.

References:

[1] M. K. Abdmouleh, H. Amri, A. Khalfallah, and M. S. Bouhlel. An efficient crypto-compression scheme for medical images by selective encryption using DCT. *International Journal of Advanced Intelligence Paradigms*, page Inpress, 2016.

[2] M. K. Abdmouleh, A. Masmoudi, and M. S. Bouhlel. A new method which combines arithmetic coding with rle for lossless image compression. *Journal of Software Engineering and Applications*, 5(1):41–44, January 2012.

[3] M. S. Bouhlel, F. Kammoun, and E. Garcia. An efficient DCT-based crypto-compression scheme for a secure and authentic medical image transmission. *Journal of Testing and Evaluation for Applied Sciences and Engineering*, 34(6):459–463, 2006.

[4] N. Bourbakis and C. Alexopoulos. Picture data encryption using scan patterns. *Pattern Recognition*, 25(6):567–581, 1992.

[5] H. K-C. Chang and J-L. Liu. A linear quadtree compression scheme for image encryption. *Signal Processing: Image Communication*, 10(4):279–290, 1997.

[6] H. Cheng and Xiaobo Li. Partial encryption of compressed images and videos. *Trans. Sig. Proc.*, 48(8):2439–2451, August 2000.

[7] D. Coppersmith. The data encryption standard (DES) and its strength against attacks. *IBM J. Res. Dev.*, 38(3):243–250, May 1994.

[8] L. Dubois, W. Puech, and J. Blanc-Talon. Smart selective encryption of H.264/AVC videos using confidentiality metrics. *Annales des Telecommunications*, 69(11–12):569–583, 2014.

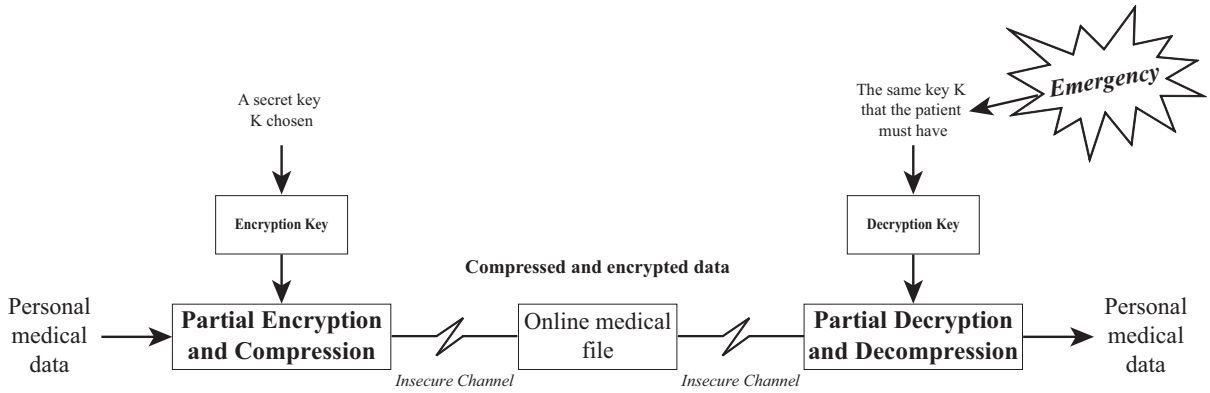

Figure 4: Principle of key management

[9] L. Dubois, Z. Shahid, and W. Puech. Chapter 6: Selective Encryption of Images and Videos: From JPEG to H.265/HEVC through JPEG2000 and H.264/AVC. In *Progress in Data Encryption Research.*, pages 137–177. Nova Publishers., 2014.

[10] B.S. Kaliski Jr. and M.J.B. Robshaw. Multiple encryption: weighing up security and performance. *Dr. Dobb's Journal*, pages 123–127, 1996.

[11] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, and R. L. Rivest. Handbook of applied cryptography, 1997.

[12] L. Pu, M. W. Marcellin, A. Bilgin, and A. Ashok. Compression based on a joint task-specific information metric. In *Data Compression Conference*, pages 467–467, April 2015.