Image Encryption and Compression for Medical Image Security

William Puech

Image Encryption and Compression for Medical Image Security

W. Puech[1,2]
[1] LIRMM Laboratory, UMR 5506 CNRS
University of MONTPELLIER, 161, rue Ada, 34392 MONTPELLIER CEDEX 05 ,FRANCE
e-mail: william.puech@lirmm.fr
[2] University of NIMES, Place G. Péri, 30021 NIMES CEDEX 1, FRANCE

***Abstract*— This tutorial presents the problem of protecting the transmission of medical images. The presented algorithms will be applied to images, videos and 3D objects. The main keywords are compression, encryption, watermarking and data hiding.**

***Keywords*— Image protection, compression, encryption, watermarking and data hiding.**

I. Introduction

The amount of digital visual data (image, video and 3D object) has increased rapidly on the Internet. Image, video and 3D object security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of visual data is a daily routine and it is necessary to find an efficient way to transmit them over networks.

Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption[5], [6]. In this group, proper decryption of data requires a key. The second group bases the protection on digital watermarking or data hiding, aimed at secretly embedding a message into the data. In order to not increase the processing time, these two approaches must be combined with the compression stage. Nowadays, the challenge is to perform simultaneously for example image encryption and compression.

The works presented in this tutorial 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. When a physician receives a visit from a patient, he often requires a specialist opinion before giving a diagnosis. One possible solution is to send images of the patient, along with a specialist report, over a computer network. Nevertheless, computer networks are complex and espionage is a potential risk. We are therefore faced with a real security problem when sending data. 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 tutorial, in a first part, I will recall the standard information of encryption (block cipher, stream cipher, asymmetric and symmetric encryption) and I will show the application of standard algorithms to images. In a second part I will present combination of image encryption and compression. To finish this second part I will talk of selective encryption methods. In this part I will address the problem of simultaneous partial encryption (PE), selective encryption (SE) and image compression. Indeed, in order to visualize on line images in real time, they must be quickly transmitted and the full encryption is not really necessary. To finish this tutorial I will present some watermarking and data hiding algorithms developped by our team applied to visual data and I will show how these can be suited to medical imagery.

II. A New Crypto-Watermarking Method for Medical Images Safe Transfer [3], [2]

The use of encryption schemes to assure confidentiality in digital networks is a common routine. The drawback of the traditional symmetric ciphering is the risk involved in sending the secret key. This work presents an autonomous method for safely transferring digital images. It is based on three steps. The first one is the encryption of the image with a new asynchronous stream cipher that is resistant to noise. The second step is the ciphering of the secret key with an asymmetric algorithm. The last step is the embedding of the enciphered key into the previous encrypted image. We fully present the proposed asynchronous stream cipher as well as the used data hiding method. The most important features of the proposed procedure is that the proposed stream cipher method is robust to noise and that we send the coded image and the secret key concomitantly. In this way the proposed method is autonomous and ensures the integrity because the key is spread in the whole image. We have applied and shown the results of our method to more than 100 medical images for statistically representative results [3], [2]. The keywords of this work are safe image transmission and combination of watermarking and encryption algorithms.

III. A New Fast Reversible Method for Image Safe Transfer [4]

In this section a novel reversible method for fast and safe image transfer is proposed. The method combines compression, data hiding and partial encryption of images in a single processing step. The proposed approach can embed data into the image according to the message size and partially encrypt

the image and the message without changing the original image content. Moreover, during the same process the image is lossless compressed. Nevertheless, the compression rate depends on the upper bound of message size to embed in the image. The main idea is to decompose the original image into two sub-images and to apply various processes to each sub-image in order to gain space and increase the amount of embedded data. The two sub-images are then scrambled and partially encrypted. The most significant characteristic of the proposed method is the utilization of a single procedure to simultaneously perform the compression, the reversible data hiding and the partial encryption rather than using three separate procedures. Our approach reduces then the computational effort and the required computation time. This method is specially suited for medical images where one can associate the patient diagnostic to the concerned medical image for safe transfer purpose [4]. The keywords of this work are fast and safe image transmission, lossless compression, reversible data hiding, partial encryption, image protection and real time image processing.

IV. A Reversible Data Hiding Method for Encrypted Images [1]

Since several years, the protection of multimedia data is becoming very important. The protection of this multimedia data can be done with encryption or data hiding algorithms. To decrease the transmission time, the data compression is necessary. Since few years, a new problem is trying to combine in a single step, compression, encryption and data hiding. So far, few solutions have been proposed to combine image encryption and compression for example. Nowadays, a new challenge consists to embed data in encrypted images. Since the entropy of encrypted image is maximal, the embedding step, considered like noise, is not possible by using standard data hiding algorithms. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images. In this paper we propose an analysis of the local standard deviation of the marked encrypted images in order to remove the embedded data during the decryption step. We have applied our method on various images, and we show and analyze the obtained results [1]. The keywords of this work are image encryption and noise removing.

V. Conclusion

In this tutorial we have presented several methods in order to protect the transmissions of medical images. The protection of visual data can be done by using encryption or watermarking algorithms or by combining these two approaches.

References

[1] W. Puech, M. Chaumont, and O. Strauss. A Reversible Data Hiding Method for Encrypted Images. In *Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, volume 6819, pages 68191E–1–68191E–9, San Jose, CA, USA, January 2008.

[2] W. Puech and G. Coatrieux. *Chapter 10: Coding: Encryption-Watermarking-Compression for Medical Information Security*. Compression of Biomedical Images and Signals, A. Naït-Ali and Christine Cavaro-Menard, Digital Signal Processing, ISTE-Wiley, May 2008.

[3] W. Puech and J.M. Rodrigues. A New Crypto-Watermarking Method for Medical Images Safe Transfer. In *Proc.* 12^{th} *European Signal Processing Conference (EUSIPCO'04)*, pages 1481–1484, Vienna, Austria, 2004.

[4] W. Puech, J.M. Rodrigues, and J.E. Develay-Morice. A New Fast Reversible Method for Image Safe Transfer. Journal of Real-Time Image Processing. *Journal of Real-Time Image Processing (JRTIP)*, 2(1):55–65, Oct. 2007.

[5] B. Schneier. *Applied cryptography*. Wiley, New-York, USA, 1995.

[6] A. Uhl and A. Pommer. *Image and Video Encryption: From Digital Rights Management to Secured Personal Communication*. Springer, 2005.

Biography

W. Puech was born in December 1967, in France. He received the diploma of Electrical Engineering from the University of Montpellier, France, in 1991 and the Ph.D. Degree in Signal-Image-Speech from the Polytechnic National Institute of Grenoble, France in 1997. He started his research activities in image processing and computer vision. He served as a Visiting Research Associate to the University of Thessaloniki, Greece. From 1997 to 2000, he had been an Assistant Professor in the University of Toulon, France, with research interests including methods of active contours applied to medical images sequences. Since 2000, he is Associate Professor at the University of Montpellier, France. He works now in the LIRMM Laboratory (Laboratory of Computer Science, Robotic and Microelectronic of Montpellier, UMR 5506 CNRS UMII). His current interests are in the areas of protection of visual data (image, video and 3D object) for safe transfer by combining watermarking, data hiding, compression and cryptography. He has applications on medical images, cultural heritage and video surveillance. He is the head of the ICAR team (Image & Interaction).