Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 112 (2017) 369–376

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES2017, 6-8 September 2017, Marseille, France

A Novel Selective Encryption Scheme for Medical Images Transmission based-on JPEG Compression Algorithm

Med Karim Abdmouleh[a,*], Ali Khalfallah[a], Med Salim Bouhlel[a]

[a] *University of Sfax*
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology, Sfax--Tunisia

Abstract

The medical imagery is a transverse activity for all medical disciplines. Its remarkable development is due to the large use of telecommunications and information technologies in the medical domain. However, since the telemedicine is a medical act that must answer to stern rules, and follow the easiness that is offered by the informatics sciences to violate the confidentiality and authenticity of medical data, the medical community is, actually, in state of opposition facing the computerization of data. To resolve this problem, a lot of methods combining compression and encryption have been developed in the literature to secure the transmission and the storage of medical images. This work presents a method of a partial or selective encryption for medical Images. It is based on the integration of the encryption in a compression process based on the Discrete Cosine Transform (DCT) in order to reduce the processing time in the encryption-decryption operation. The results of several experiments show that the proposed scheme is rapid, efficient, secure and it perfectly preserves the performances of the new one.

© 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of KES International

Keywords: Telemedecine, Telediagnostic, Compression, Encryption, Crypto-Compression, DCT, RSA

1. Introduction

When it is necessary to transmit medical data through networks, both compression and encryption must be performed[1]. Indeed, the digital images have a gigantic size. Therefore, we must compress them in order to improve the capacity of storage and to optimize their transmission (reduction in the transmission time and in the obstruction of networks). In addition, network communication can be intercepted especially in the Wide World Web. Consequently, the encryption of the medical images is imposed to safeguard the confidentiality of medical data during their transmission.

To satisfy these two conditions, the classical approach consists of applying a compression algorithm to the medical image, and then its output is encrypted with independent cryptographic algorithm[1] (Fig. 1).

* Corresponding author. Tel.: +216-53-654-586
E-mail address: medkarim.abdmouleh@isggb.rnu.tn

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of KES International
10.1016/j.procs.2017.08.026

Unfortunately, we believe that the classical approach is not very efficient because the encryption processing time is relatively important especially in the emergency cases.

Multitude of methods combining compression and encryption have been proposed to reduce the overall processing time[2,3,4,5,6,7], but they are either insecure or too computationally intensive.

In this paper, we propose an efficient DCT-based algorithm which combines encryption and compression. We apply this algorithm to the most efficient DCT-based compression norm: JPEG[8] (Fig. 2).

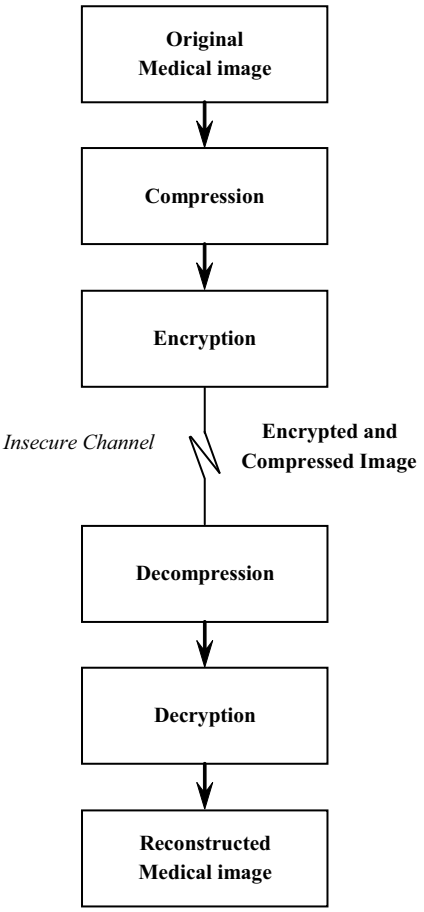

Fig. 1: Classical approach

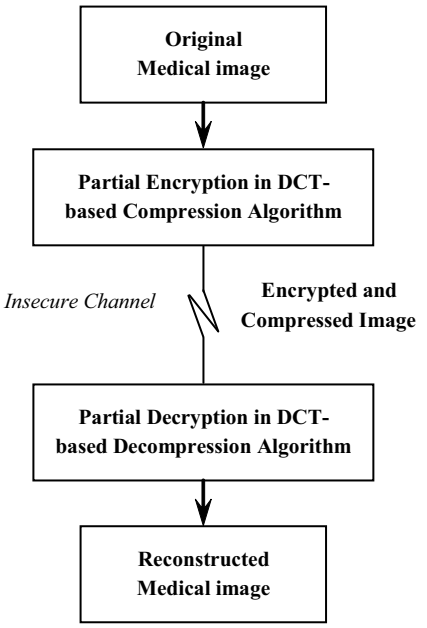

Fig. 2: Proposed approach

In the next section of this paper, Section 2, the DCT and the encryption algorithm RSA are briefly described. Section 3 presents the principle and the results of the novel crypto-compression scheme. In Section 4, the advantages of our algorithm are enumerated. Section 5 concludes the paper.

2. Background

2.1. Discrete Cosine Transform (DCT)

The DCT, used in the JPEG algorithm, transforms the pixels of one block (8×8) of one image into another block of (8×8) containing the corresponding frequency components. This transformation, which is specially studied for the compression of the images, is the most efficient as the data are correlated (Fig. 3).

Download English Version:

https://daneshyari.com/en/article/4960615

Download Persian Version:

https://daneshyari.com/article/4960615

Daneshyari.com