Securing EPR Data Using Cryptography and Image Watermarking

Youssef Zaz, Abdelmalek Essaâdi University, Morocco
Lhoussain El Fadil, Ibn Zohr University, Morocco
Mohamed El Kayyali, Universidad Tecnologica del Peru, Peru

ABSTRACT

This paper demonstrates new methodology to improve security and avoid data overlapping between patients records which are defined as Electronic Patient Records (EPR), a combination of digital watermarking techniques and cryptography are used to ensure the non-separation of EPR and medical images during communications within open networks. The EPR data is encrypted, by a symmetric key algorithm based on an Elliptic Curve Cryptosystem (ECC), and inserted in liberated zone of the Least Significant Bit plan (LSB) of the medical image by compressing the original one using the Huffman coding. The proposed method improves security issues and reduces the computation cost related to data encryption and decryption.

Keywords: Electronic Patient Records (EPR), Elliptic Curve Cryptosystem (ECC), Huffman Coding, Least Significant Bit Plan (LSB), Semantic Security, Symmetric Key Cryptosystem, Watermarking

1. INTRODUCTION

Electronic or not, patient records related to medical secrecy must be confidential. The digital handling of EPR on network requires a systematic security enhancement as proven in Zain and Clarke (2005). Using reversible watermarking techniques to embed EPR in medical images becomes inescapable to hide the EPR data, avoiding its detachment from the image and saving the transmission bandwidth (Cox et al., 2004; Navas et al., 2008).

In Jurisic and Menezes (1997), it was proven that to achieve reasonable security, a 1024-bit modulus would have to be used in a RSA cryptosystem, while160-bit modulus is sufficient for ECC which started receiving commercial acceptance in the late 1990s. Moreover, as elliptic curve cryptosystems operate on points of elliptic curves and derive their security from the hardness of the elliptic curve discrete logarithm problem, it follows that sub-exponential algorithm cannot solve their security.

In previous work, Zaz and El Fadil (2010) proposed to watermark encrypted EPR data in the Region-of-None-Interest (RONI) of the image. However, it isn’t easy to detect the RONI
with automatic process. Sometimes, to ensure the Region-of-Interest data integrity, the intervention of medical specialist is unavoidable to delimitate that region.

In this paper, we propose a new method that combines watermarking with encryption techniques and using a symmetric key encryption algorithm, which is semantically secure, to enhance considerably the security performance.

In order to save the original LSB bit-plan data, we propose to compress it using Huffman coding (Hu & Chang, 2000) and exploit the liberated area to watermark the encrypted EPR data.

In further use of the watermarked image, the medical staff can easy rescue the exactly original image and the EPR data. Thus, we achieve medical requirements in terms of integrity and confidentiality.

This paper organized as follow: Section 2, requirements needed to store EPR data. In Section 3, an elliptic curve crypto-system algorithm proposed. Section 4, withdraws the Huffman coding. Section 5, describes the algorithm steps, and finally: the conclusion.

2. REQUIREMENTS STORAGE NEEDS OF THE EPR IN MEDICAL IMAGES

Most watermarking techniques counting on modify and hence distort the host image in order to embed the given data. In many applications, loss of image fidelity is not prohibitive as long as the original and modified images are perceptually equivalent. In medical applications, where the need for authentication is often paramount, there are typically stringent constraints on data fidelity that prohibit any distortion during the watermarking process. In certain cases, artifacts in a patient’s diagnostic image may cause errors in diagnosis and treatment with possible life threatening consequences (Zain et al., 2009).

A well-known medical image standard DICOM (Digital Image Communication in Medicine) can be used to insert EPR data in to an image, but this method has a risk of data loss in case of anonymization process. Even Munch et al. (2004) proposed a web based method to integrate the data and images but the best way of integration of EPR and medical images is the hiding EPR in images using watermarking techniques.

The frequently used approach in spatial domain is Least Significant Bit (LSB) insertion. Since the least significant bit-plane does not contain visually significant information, it can be easily replaced by a large amount of watermark bits. But this technique doesn’t satisfy medical requirements in terms of data integrity. In order to use it, we propose to compress the original LSB bit-plan using lossless technique that offers high level compression.

Run Length Encoding (RLE) is a well known lossless compression algorithm; it only offers decent compression ratios with files that contain lots of repetitive data. Several other compression techniques exist in the literature; we opt for Huffman coding algorithm (Hu & Chang, 2000) which offers a reasonable compression rate and it is adapted to binary data exiting in the LSB bit-plan.

To ensure high security, data encryption is unavoidable. But nowadays, online diagnosis is widely used, which means we should find an efficient and speedy encryption algorithm.

3. ELLIPTIC CURVE CRYPTOSYSTEM

Miller (1985) and Koblitz (1987) independently proposed using elliptic curves cryptosystems. Strong cryptosystems like RSA (Rivest, Shamir and Adleman who first publicly described an algorithm for public-key cryptography) are often too computationally expensive for small devices. In Jurisic and Menezes (1997), it was proven that to achieve reasonable security, a 1024-bit modulus would have to be used in a RSA cryptosystem, while a 160-bit modulus should be sufficient for ECC. In the late 1990s, elliptic curve systems started receiving commercial acceptance. Thanks to its small key size and high security, ECC is one of the best public...
Misbehavior Detection in VANET: A Survey
www.igi-global.com/chapter/misbehavior-detection-in-vanet/86304?camid=4v1a

Secure Routing and Scheduling in Ad-Hoc Cognitive Radio Networks for Public Safety
www.igi-global.com/article/secure-routing-and-scheduling-in-ad-hoc-cognitive-radio-networks-for-public-safety/124959?camid=4v1a