J. Vis. Commun. Image R. 39 (2016) 51–57

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

A ROI-based reversible data hiding scheme in encrypted medical images ☆

Yuling Liu [a,*], Xinxin Qu [a], Guojiang Xin [b]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[b] College of Management and Information Engineering, Hunan University of Chinese Medicine, Changsha 410082, China

ARTICLE INFO

Article history:
Received 26 July 2015
Revised 21 April 2016
Accepted 17 May 2016
Available online 18 May 2016

Keywords:
Reversible data hiding
Image encryption
The medical image
ROI-based
LSB substitution

ABSTRACT

A novel ROI-based reversible data hiding scheme in encrypted medical images is proposed. Firstly, a content owner partitions an original medical image into the region of interest (ROI) and the region of noninterest (RONI), and then encrypts the image using an encryption key. A data-hider concatenates the least significant bits (LSB) of the encrypted ROI and Electronic Patient Record (EPR), and then embeds the concatenated data into the encrypted image by LSB substitution algorithm. With the encrypted medical image containing the embedded data, the receiver can extract the embedded data with the data-hiding key; if the receiver has the encryption key, a medical image similar to the original image can be obtained by directly decrypting the encrypted medical image; if the receiver has both the data-hiding key and the encryption key, the embedded data can be extracted without any error and ROI can be losslessly recovered after extracting the embedded data.

1. Introduction

The rapid development of the Internet and the hospital information system offers new means of sharing and remote access to patient data. In particular, the medical image plays an important role in applications like telesurgery, telediagnosis and so on. Medical information, such as the medical image and EPR, is often closely related to patients' privacy which needs to be kept secret. However, the Internet not only brings to convenience but also many security issues in terms of confidentiality, availability and reliability [1].

In order to protect patients' privacy, medical images should be encrypted after they were taken. Patient information (such as name, age, and EPR) needs to be embedded into the encrypted medical image in that the encrypted medical image corresponds to the corresponding patient. Additionally, the medical image should be losslessly recovered after the embedded information is extracted at the receiving end. Therefore, the reversible data hiding (RDH) scheme in encrypted images is needed.

Some RDH techniques in encrypted images have been proposed. Zhang [2] divided the encrypted image into several blocks, and then the pixels in each block randomly partitioned into two pixel sets with a data hiding key. Each block could be embedded with one bit by flipping 3 LSB-planes of one pixel set. Data extraction and image recovery proceeded by finding which pixel set had been flipped in each block. This process utilized the spatial correlation in the decrypted image. Hong et al. [3] improved Zhang's method at the receiving end by further exploiting the spatial correlation using a different estimation equation and side match technique to achieve lower error rate. These two methods rely on spatial correlation of the original image to extract data. That is, the encrypted image should be decrypted first before data extraction.

To separate the data extraction from image decryption, Zhang [4] located space for data embedding, which followed the idea of compressing the encrypted image [5,6]. The method compressed the encrypted LSBs to vacate room for additional data by finding syndromes of a parity-check matrix, and the side information used at the receiving end was also the spatial correlation of decrypted images. Qian et al. [7] proposed a framework of reversible data hiding in an encrypted JPEG bitstream. Zhang et al. [8] losslessly compressed the partition of the encrypted image using Low Density Parity Check Code and obtained the extra room for embedding data; with the help of compressed data and the uncompressed data, the image could be recovered on the receiving end. In order to increase the embedding payload, Qian and Zhang [10] proposed a method combining the MSB estimation with distributed source coding.

☆ This paper has been recommended for acceptance by M.T. Sun.

* Corresponding author.
E-mail address: yuling_liu@126.com (Y. Liu).

http://dx.doi.org/10.1016/j.jvcir.2016.05.008
1047-3203/

Wu and Sun [11] presented two reversible data hiding methods in encrypted images, namely a joint method and a separable method, which were introduced by adopting prediction error; Zhou et al. [12] proposed an encrypted-domain secure RIDH scheme without data hiding key. All the above methods try to directly vacate room from the encrypted images and recover the image through the correlation of pixels. However, since the entropy of encrypted images has been maximized, these methods can only achieve small embedding rate, directly generate decrypted image with poor quality for large payload and all of them are subject to the error rates on data extraction or image recovery.

Another concept of existing work is to reserve room before encryption. Ma et al. [9] reversibly embedded LSBs of some pixels into other pixels by employing the traditional RDH algorithms, and then the emptied positions of these LSBs used to embed data. Zhang et al. [14] proposed a method based on estimation technique to reserve room before encryption. A few parts of pixels were estimated by the rest pixels before encryption. The estimated errors were trimmed and modified to vacate room for embedding data. Fujiyoshi [13] proposed a scheme taking a hierarchy into account histogram and spatial permutation, which could always recover the original image. Cao et al. [16] proposed to consider the patch-level sparse coding technique when hiding the secret data. Due to the powerful representation of sparse coding, a large vacated room could be achieved, and thus the data hider could embed more secret messages in the encrypted image. These methods can achieve real reversibility, that is, data extraction and image recovery are free of any error.

In view of the characteristic of the medical image, Wu et al. [17] proposed a reversible data hiding method with contrast enhancement for medical images. Kundu and Das [18] presented a watermarking scheme that combined lossless data compression and encryption technique in application to medical images. Tan et al. [19] presented a fully reversible, dual-layer watermarking scheme with tamper detection capability for medical images. Lavanya and Natarajan [15] proposed a ROI-based method, which the medical images were firstly divided into blocks; then 3 LSB-planes substitution was utilized in RONI for embedding data. Moreover, in our previously published paper [20], we proposed a ROI-based reversible data hiding scheme for medical images with tamper detection, which combines prediction error expansion with the sorting technique for embedding EPR into ROI, and the recovery information is embedded into the region of non-interest (RONI) using the histogram shifting (HS) method. Although all the above methods combine the reversible data hiding techniques and the encrypting schemes for the security of the medical images, they are not directly applied to the encrypted medical images.

The reversible data hiding technique for encrypted medical images should consider the following points: (1) the division of ROI and RONI; (2) the integrity authentication of ROI; (3) high embedding payload; and (4) the security of the system. By considering the above problems, a ROI-based reversible data hiding scheme for encrypted medical images is proposed in this paper. ROI can be losslessly recovered after the embedded data is extracted.

The rest of the paper is organized as follows. The proposed scheme is described in Section 2. The experimental results and discussions are presented in Section 3. Some conclusions are made in Section 4.

2. Proposed method

The proposed method is composed of three primary stages: image encryption, data embedding in the encrypted image, data extraction and image recovery. Fig. 1 illustrates the framework of the proposed scheme.

2.1. Image encryption

To construct the encrypted medical image, the first stage can be divided into two steps: image partition and image encryption. The original image is a 16-bit gray-scale medical image with size of $M \times N$ and its pixels $p(i,j) \in [0, 65535]$, $1 \leqslant i \leqslant M$, $1 \leqslant j \leqslant N$.

Step 1: Image Partition. The original medical image I is divided into three parts: ROI, RONI and the border area. Although ROI in a medical image is irregularly shaped in most cases, ROI is selected by a polygon defined by the content owner in our scheme. The border area is the bottom line of the image. The vertices of the polygon should be recorded for describing ROI, denoted by D_{roi} with length L_c.

Step 2: Calculate the hash value of ROI using the MD5 hashing algorithm (other hashing techniques can also be used) as follows:

$$H = H_{\text{MD5}}(D_{\text{roi}}) \tag{1}$$

where $H_{\text{MD5}}(\cdot)$ indicates the MD5 function. H can provide integrity authentication for ROI.

Step 3: Image Rearrangement. Place ROI in the front of the image concatenated by RONI and border area, as shown in Fig. 2. The rearrangement operation can improve the security.

Step 4: Image Encryption. After rearrangement, the image is encrypted to construct the encrypted image with a stream cipher. Denote the bits of a pixel as $b_{i,j,0}, b_{i,j,1}, \ldots, b_{i,j,15}$, where (i,j) indicates the pixel position. Thus

$$b_{i,j,k} = \lfloor \frac{p_{i,j}}{2^k} \rfloor \bmod 2, \quad k = 0, 1, \ldots, 15 \tag{2}$$

and

$$p_{i,j} = \sum_{k=0}^{15} b_{i,j,k} \times 2^k \tag{3}$$

In encrypting phase, the exclusive-or results of the original bits and pseudo-random bits are calculated as

$$B_{i,j,k} = b_{i,j,k} \oplus r_{i,j,k} \tag{4}$$

where $r_{i,j,k}$ are determined by an encryption key using a standard stream cipher. Then, $B_{i,j,k}$ are concatenated orderly as the encrypted image. Many secure stream cipher methods can be used here to ensure that anyone without the encryption key cannot obtain any information about the original content from the encrypted data.

Step 5: Finally, D_{roi} and H are embedded into LSBs of the border area from the appointed position $L(x,y)$ (the position can be controlled by the key). Note that after image encryption, the data hider or a third party cannot access the content of the original image without the encryption key, thus privacy of the content owner can be protected.

2.2. Data embedding in encrypted image

With the encrypted medical image, even though a data-hider does not know the original medical image content, the data can be embedded into the encrypted medical image.

Step 1: From the appointed position $L(x,y)$ (the position can be obtained by the shared key) of the border area, D_{roi} can be obtained by reading the LSBs.

Step 2: After knowing the vertex information of ROI, the data-hider can record LSB-plane of ROI, denoted by D_{lsb}.

Step 3: The embedded data W is formed by concatenating EPR and D_{lsb} as follows:

$$W = D_{\text{lsb}} + \text{EPR} \tag{5}$$

where "+" indicates the concatenation operation. Then the data-hider uses LSB substitution algorithm to embed W and an ending