Sādhanā Vol. 37, Part 6, December 2012, pp. 723–729. © Indian Academy of Sciences

Watermarking patient data in encrypted medical images

A LAVANYA* and V NATARAJAN

Department of Instrumentation Engineering, Madras Institute of Technology,
Chennai 600 044, India
e-mail: lavanyaananthan@gmail.com

MS received 6 June 2012; revised 24 July 2012; accepted 6 September 2012

Abstract. In this paper, we propose a method for watermarking medical images for data integrity which consists of image encryption, data embedding and image-recovery phases. Data embedding can be completely recovered from the watermarked image after the watermark has been extracted. In the proposed method, we utilize standard stream cipher for image encryption and selecting non-region of interest tile to embed patient data. We show that the lower bound of the PSNR (peak-signal-to-noise-ratio) values for medical images is about 48 dB. Experimental results demonstrate that the proposed scheme can embed a large amount of data while keeping high visual quality of test images.

Keywords. Encryption; watermarking; non-region of interest; embedding; medical images.

1. Introduction

Due to the advancement of technology, internet has become an indispensable part of life for many people. Information can be sent very quickly by the internet. However, it causes the problems of the information securities and multimedia copyright protections. Therefore, network securities protections have become more important topics. Watermarking is an important technology for these topics. Medical images play a significant role in diagnosis of many diseases. Doctors diagnose from medical images, so more care is required to hide patient information in medical images without affecting quality of image. A Region of Interest (ROI) of a medical image is an area including important information and must be stored without any distortion.

Coatrieux *et al* (2000) concluded that digital watermarks could be used in addition to the current security tools, in order to protect medical records. Giakoumaki *et al* (2004, 2006) proposed a wavelet transform-based watermarking, the drawback is medical images are overwritten which may be unacceptable in diagnosis. Tian (2003) proposed a technique of pixel-value difference expansion. However, not all pairs expanded for data hiding. A location map is used to indicate whether pairs are expanded or not. Enhanced pixel-value difference expansion method proposed by Kim *et al* (2008) to achieve higher data hiding capacities while keeping the resulting image

*For correspondence

distortion as low as that yielded by Tian's method (Tian 2003). Ni *et al* (2006) proposed a lossless reversible data-hiding algorithm based on the shifting of an image histogram and selecting the peak point of the histogram to embed a message. While embedding a message into the image, the pixel value at the maximum point is altered by 1 if the message bit is '1' or left unchanged if the message bit is '0'. This enables to embed a large amount of data guaranteeing the PSNR (peak-signal-to-noise-ratio) of watermarked images. Also, the original image is always higher than 48 dB. But, gray level values of peak point and zero point should be transmitted to the receiver which is necessary for data retrieval, is not discussed by Ni *et al* (2006). Tseng & Hsieh (2008) used image histogram as data hiding method and by embedding the secret data in the peak's neighbouring pixels.

Peak point of the histogram remains unchanged for retrieving hidden data. Lin *et al* (2008) proposed multilevel reversible data hiding scheme based on the difference of image histogram modification using the peak point to hide messages. This has achieved large hiding capacity keeping the distortion low. Lee *et al* (2008) proposed a novel adaptive technique of centralized difference expansion for lossless data hiding scheme. This concept utilizes a block-based lossless data embedding algorithm choosing smoother areas to conceal more secret bits. Fallahpour & Sedaaghi (2007) presented the block-based histogram modification scheme. Chang *et al* (2008) studied pixel difference to embed more data than other histogram-based lossless data hiding algorithms and used histogram shifting technique to prevent overflow and underflow problems. In our proposed method the patient details are embedded in non-ROI region of an image.

This work proposes a novel method for hiding patient details in encrypted image, which is made up of image encryption, data embedding and data-extraction/image-recovery phases. The data of original cover tile image are entirely encrypted, and the additional message is embedded by modifying a non-ROI part of encrypted data. At receiver side, the patient information is successfully extracted while the original image is perfectly recovered.

2. Methodology

A sketch of the proposed scheme is given in figure 1. Original uncompressed image using an encryption key to produce an encrypted image. The encrypted image is divided into non-overlapping tiles to identify region of interest and non-region of interest. In examination site, examiner embeds patient details in non-ROI of encrypted image using a data-hiding key. With an encrypted image containing patient details, a receiver may first detile and decrypt it using the encryption key, and the decrypted version is similar to the original image.

2.1 *Embedding algorithm*

1. Original image is divided into tiles.
2. Tiled image is encrypted using standard stream cipher

$$\begin{aligned} B_{i,j,k} &= b_{i,j,k} \otimes r_{i,j,k} \\ b_{i,j,k} &= \text{Original data} \\ r_{i,j,k} &= \text{Pseudo-random bits (encryption key)} \\ B_{i,j,k} &= \text{Encrypted data.} \end{aligned}$$

3. Identifying non-region of interest and region of interest from encrypted tiles.
4. Selecting non-region of interest tiles to hide patient details.

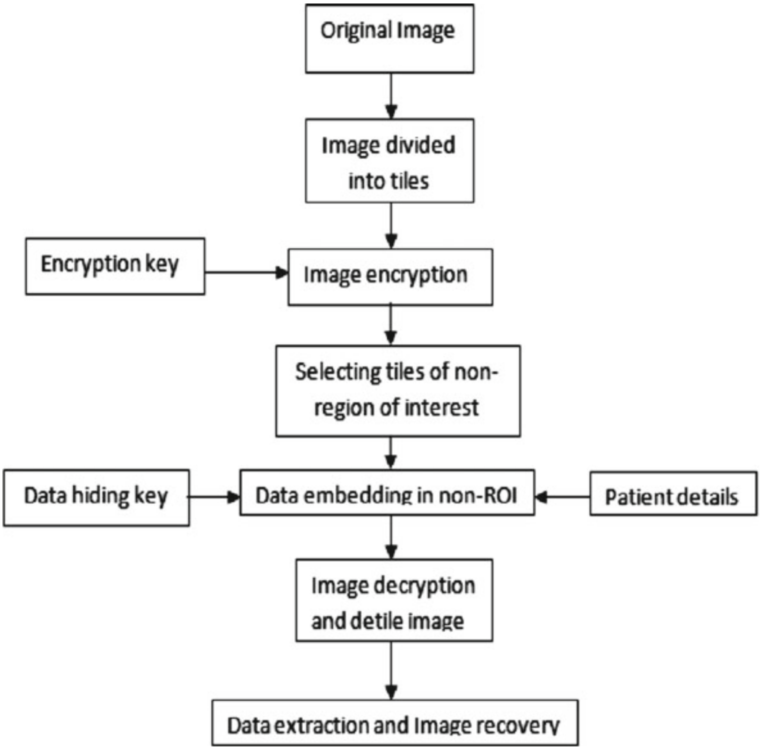
Original Image
Image divided into tiles
Encryption key
Image encryption
Selecting tiles of non-region of interest
Data hiding key
Data embedding in non-ROI
Patient details
Image decryption and detile image
Data extraction and Image recovery

Figure 1. Sketch diagram of the proposed scheme.

5. Each non-region of interest tile is divided into two sets I_0 and I_1. Probability that pixels belong to I_0 or I_1 is 1/2.
6. Patient informations such as patient name, patient Id, patient age, date of birth, doctor name, etc… are converted to ASCII codes, and then the ASCII codes are converted into binary.
7. If the patient information to be embedded is 0, flip the 3 least significant bits (LSB) in I_0. If the patient information to be embedded is 1, flip the 3 least significant bits (LSB) in I_1.
8. Continue steps 5–7 till all the patient information to be embedded.
9. Detile the image for transmission.

2.2 *Extraction algorithm and image recovery*

1. Received Image is divided into tiles.
2. In Expert centre firstly generates $r_{i,j,k}$ according to the encryption key and calculates the exclusive-or of the received data and to decrypt the image.

$$
\begin{aligned}
b'_{i,j,k} &= r_{i,j,k} \oplus B\prime_{i,j,k} \\
&= r_{i,j,k} \oplus \overline{r_{i,j,k} \oplus b_{i,j,k}} \\
b'_{i,j,k} &= \overline{b_{i,j,k}} \\
b'_{i,j,k} &= \text{Decrypted Image.}
\end{aligned}
$$

3. Identifying non-region of interest and region of interest from decrypted tiles.

4. Each non-region of interest tile of decrypted block is to flip all the three LSB of I_0 pixels to form new block, and flips all the three LSB of I1 pixels to form another new block. The new blocks are denoted as I_0' and I_1', either I_0' or I_1' is the original block and other one is interfered due to flip operation.
5. The function is to calculate original block and interfered block of size SxS is given below

$$f = \sum_{u=2}^{s-1}\sum_{v=2}^{s-1}\left|p_{u,v} - \frac{p_{u-1,v} + p_{u+1,v} + p_{u,v+1} + p_{u,v-1}}{4}\right|.$$

   The fluctuation function of original block is generally lower than interfered block. Receiver can perform image recovery by comparing f_0 and f_1. If $f_0 < f_1$, I_0' regard as the original content of the block and let the extracted bit be 0. Otherwise if $f_0 > f_1$, I_1' regard as the original content of this block and extract a bit 1.
6. Continue steps 4–5 till all the patient's details are extracted.

3. Experimental results and discussion

In this section, we show the experimental results of our proposed schemes. To evaluate the performance of the proposed scheme, we performed computer simulations on many medical images (i.e., chest X-ray, CT image, MRI image) of size 512 × 512 pixels and were run on MS Windows XP SP2, Intel Core 2 Duo @ 2.2 GHz with 1 GB RAM and MATLAB 7.8.

Brain CT image sized 512 × 512 of figure 2e divided into 25 segments and numbered from left to right and top to bottom, the four corner tiles 1,5,21 and 25 in addition being non-region of interest can be chosen for watermarking patient data (tiles are numbered in the scan order from left to right and top to bottom) shown in figures 2a–d. The tiles 1,5,21 and 25 cover the background and the bones appear white, remaining 21 tiles (6, 10, 11, 15, 16 and 20 cover both region and non-region) covers the region of interest have not been touched at all. Brain MRI image sized 512 × 512 is shown in figure 3a is divided into 16 segments is shown in figure 3b and the corners of the tile (1, 4, 13 and 16) shown in figures 3c–f are chosen for data hiding. Identifying of tiles required to embed patient details in non-region of interest without effecting

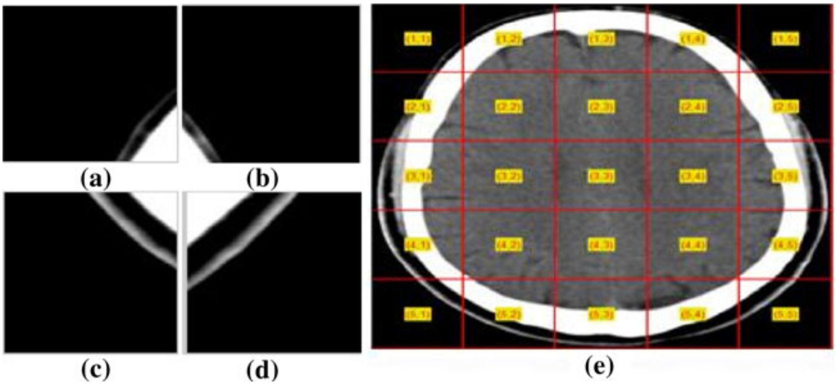

Figure 2. Region of non-interest (**a**) 1st tile, (**b**) 5th tile, (**c**) 21th tile, (**d**) 25th tile and (**e**) whole CT brain image.

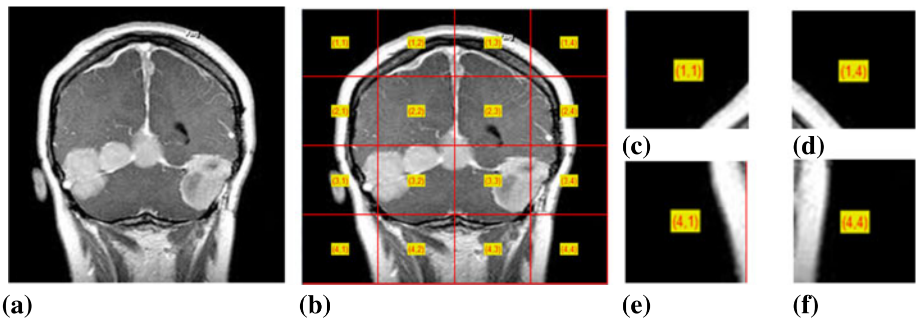

Figure 3. Regions of non-interest. (**a**) Original image, (**b**) 16 segment image, (**c**) 1st tile, (**d**) 4th tile, (**e**) 13th tile and (**f**) 16th tile.

region of interest plays an important role in data hiding. Number of tiles based on image and covering non-region of interest for hiding patient details. The subjective quality of the image, in the marked and unmarked areas, cannot be differentiated.

Original image shown in figure 4a tumour as region of interest is divided into 25 segments is shown in figure 4b. In figure 4b except 7th, 8th and 12th, remaining any tiles can be considered

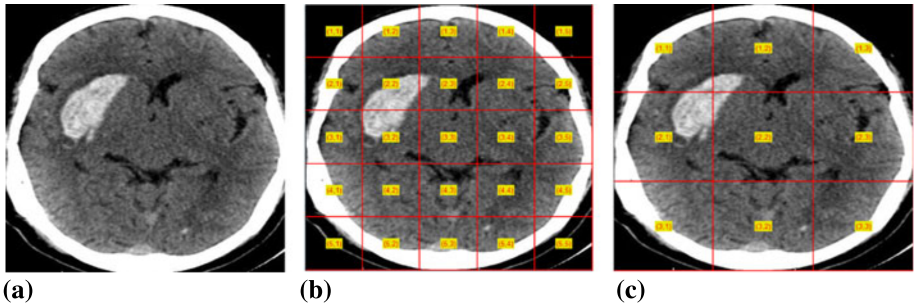

Figure 4. Regions of non-interest. (**a**) Original tumour image, (**b**) 25 segment image with 7th, 8th and 12th tiles as region of interest and remaining 22 tiles as non-region of interest, (**c**) 9 segment image with 1st, 2nd, 4th, 5th as region of interest and remaining 5 tiles as non-region of interest.

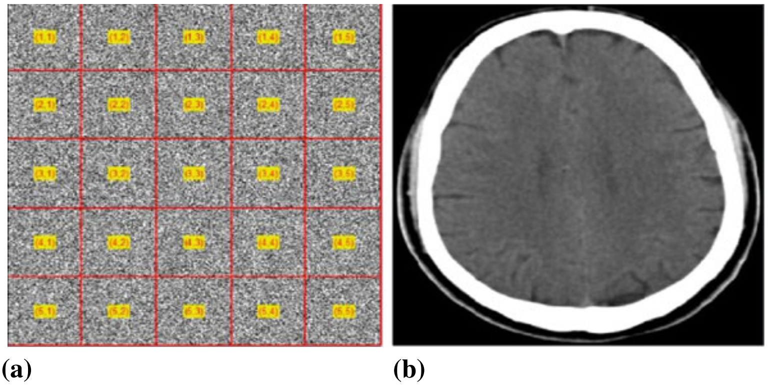

Figure 5. (**a**) Encrypted version of CT brain image and (**b**) decrypted version of CT brain image.

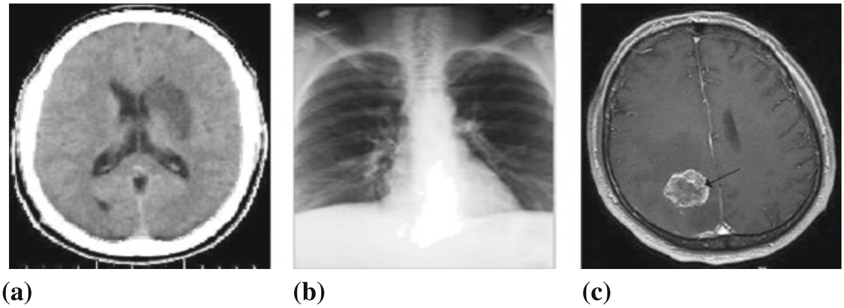

Figure 6. Test images.

Table 1. Experimental results.

Test images (512 × 512)	PSNR (dB)
CT brain tumor image (figure 4b)	49.68
CT brain image (figure 5b)	49.26
CT brain image (figure 6a)	48.74
X-ray chest image (figure 6b)	49.85
CT brain image (figure 6c)	48.92

as non-region of interest to embed patient details. Reducing the number of segments reduces the choice of selecting non-region of interest to hide patient details as shown in figure 4c.

The encrypted image is shown in figure 5a. We have embedded patient details into the encrypted image by using side length of each block s > 32. The decrypted image is shown in figure 5b containing embedded data and the values of PSNR caused by data embedding is > 48 dB. Figure 6 shows further three test images. Table 1 summarizes the experimental results. This table shows that the PSNR values of all images watermarked with patient details are above 48 dB.

Watermarking the original image slightly degrades the original images as far as peak signal to noise ratio (PSNR) is concerned. But it is well within the visual perception and we do not readily visualize the watermark and the degradation. The visual quality of the marked image is measured in PSNR.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

$$MSE = \frac{1}{n} \sum_{i=1}^{n} \left(I_m(i) - I_w(i)\right)^2$$

I_w = Watermarked image
I_m = Original image
n = Total no of pixels in the image.

4. Conclusion

We have proposed a method for watermarking medical images which consists of image encryption, data embedding and image-recovery phases. The original image is divided into tiles and data are entirely encrypted by a stream cipher. Patient details can be embedded by modifying encrypted non-region of interest. With an encrypted image containing embedded data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image.

Embedded data can be correctly extracted while the original image can be perfectly recovered. Although someone with the knowledge of encryption key can obtain a decrypted image and detect the presence of hidden data using LSB methods, if he does not know the data-hiding key, it is still impossible to extract the additional data and recover the original image. Experimental results showed that the proposed scheme provides PSNR values of all watermarked images are above 48 dB.

References

Chang C C, Tai W L and Chen K N 2008 Lossless data hiding based on histogram modification for image authentication. *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, 506–511

Coatrieux G, Maitre H, Sankur B, Rolland Y and Collorec R 2000 Relevance of watermarking in medical imaging, in: Information Technology Applications in Biomedicine, *Proceedings IEEE EMBS International Conference*, 250–255

Fallahpour M and Sedaaghi M H 2007 High capacity lossless data hiding based on histogram modification. *IEICE Electronics Express* 4: 205–210

Giakoumaki A, Pavlopoulos S and Koutsouris D 2004 A multiple watermarking scheme applied to medical image management, in: Engineering in Medicine and Biology Society. IEMBS'04. *26th Annual International Conference of the IEEE*, Sep 1–5 2004 vol. 2, pp. 3241–3244

Giakoumaki A, Pavlopoulos S and Koutsouris D 2006 Multiple image watermarking applied to health information management. *IEEE Trans. Inf. Technol. Biomed.* 10(4): 722–732

Kim H J, Sachnev V, Shi Y Q, Nam J and Choo H G 2008 A novel difference expansion transform for reversible data embedding. *IEEE Transactions on Information Forensics and Security* 3: 456–465

Lee C C, Wu H C, Tsai C S and Chu Y P 2008 Adaptive lossless steganographic scheme with centralized difference expansion. *Pattern Recogn.* 41: 2097–2106

Lin C C, Tai W L and Chang C C 2008 Multilevel reversible data hiding based on histogram modification of difference images. *Pattern Recogn.* 41: 3582–3591

Ni Z, Shi Y Q, Ansari N and Su W 2006 Reversible data hiding. *IEEE Trans. Circuits Syst. Video Technol.* 16: 354–362

Tian J 2003 Reversible data embedding using a difference expansion. *IEEE Trans. Circuits Syst. Video Technol.* 13: 890–896

Tseng H W and Hsieh C P 2008 Reversible data hiding based on image histogram modification. *Imaging Sci. J.* 56: 271–278