MEDICAL VERIFICATION WATERMARKING FOR HEALTHCARE INFORMATION MANAGEMENT

Ki-Ryong Kwon, Seung-Seob Park
Division of Electronics, Computer & Telecommunication Engineering, Pukyong National University, South Korea

Suk-Hwan Lee
Department of Information Security, Tongmyong University, South Korea

Keywords: Medical image, Watermarking, Integrity verification, Healthcare information management.

Abstract: This paper presents a verification watermarking applied to healthcare information management. The proposed method uses the whole region based on the public-key cryptograph, which is transformed by the DWT transform to integrity verification. Furthermore, the public-key cryptograph algorithm is used for the embedded watermark image. We adaptively select the upper bit-plane including the LSB parts of each block when the watermark is inserted.

1 INTRODUCTION

With the development of information communication and computer technology, there has been come to digital hospital age that can be received remote medical treatment in network by database of digital medical image.

Images that were taken by various image modalities are digitalized through CR (computed radiography). PACS (picture archiving and communication system) is a system that stores these images on storage media such as a hard disk and transmits them to each terminal via network. With this system, doctors can monitor the images of the patients in real time wherever they have a workstation like a hospital or a consulting room. As a result, we can computerize and manage the medical images, related clinical information, and ADT effectively through the nexus between PACS and HIS (hospital information system) (http://www.pccgroup.com), http://www.dicomanalyser.co.uk). In addition, with the development of superhighway, it is possible to provide remote diagnosis and consultation and to pay for insurance, and to use as data to go on in the Military Manpower Administration by transmit this medical information via open-end network such as internet. However, there are some issues raised by the system, i.e. security problems of medical information, such as illegal reproduction of medical images and proprietary rights, and data authentication. Providing a duplicated CD is weak in reissuance of medical certificates by illegal forgery, or misapplication for draft evasion.

Anand et al. (Anand and Niranjan, 1998) proposed a watermarking method that puts data between medical images for watermarking of medical images. That is, a text document and data such as E.C.G is encoded together into the LSB, which is less important bit in the gray level pixel, and inserted between the medical images such as CT images. Wakatani et al. (Wakatani, 2002) proposed a method that inserts a watermark into the surrounding regions of ROI (region of interest) of a medical image by using encoded signature image. This method generates a bit stream by its importance, after subdividing the original image into ROI region and encoding the signature by gradual code. Then, this method inserts the bit stream into the area pixels around ROI with spiral and encodes it by HS (hierarchical segmentation) algorithm.

Thus, in this paper, as a counterproposal for the integrity and copyright protection of the medical images, we propose a medical image protection system that applied digital watermarking technology, which provides proprietary and data authentication of the multimedia contents. Proposed method used DWT transformation method based on open key

Kwon K., Park S. and Lee S. (2010).
MEDICAL VERIFICATION WATERMARKING FOR HEALTHCARE INFORMATION MANAGEMENT.
In *Proceedings of the Third International Conference on Bio-inspired Systems and Signal Processing*, pages 523-527
DOI: 10.5220/0002742005230527

coding to verify integrity. That is, to generate a watermark, this method transforms an original image onto wavelet domain and resolves the most low frequency image into bit plane. Then, to authenticate its proprietary, it maps the image with the logo image of LSB and displaces randomly. In addition, it divides the original image into blocks to embed a watermark and assigns the insertion position of the watermark randomly. In a selected block, a bit plane in the embedding position of the watermark is initialized to zero and execute the XOR operation with the watermark information using hash function. Inserted watermark image uses an open key security algorithm for more robust integrity verification. With embedding a watermark, we select the upper bit-plane adaptively that includes the LSB parts of each block, so the position the watermark inserted does not appear. This proposed algorithm is robust that attackers cannot modify or remove the original watermark. Experimental results show that integrity verification is more robust and invisibility is superior to the previous algorithms.

2 PROPOSED INTEGRITY WATERMARKING SCHEME

2.1 Embedding Process

The overall diagram of proposed watermarking embed is shown in Figure 1. First, to create information of a watermark, original images is transformed as two levels by DWT. To make the LL2, which is a basis region found, as binary bit, we organize the eight bit-planes. For the reorganization of the bit-plane, m bits contrast is expressed as Eq. (1), which is a polynomial with two bases.

$$a_{m-1}2^{m-1} + a_{m-2}2^{m-2} + \cdots + a_1 2^1 + a_0 2^0 \qquad (1)$$

The obtained bit-plane information is mapped within the same size of the original image. At this time, we used a school logo rather than a bit-plane value in the LSB, so it means the copyrighter's position when the watermark is extracted. Each bit-plane information for the rest upper seven bits, which is inserted twice, expands the number of possible comparison for estimating integrity of the watermark. Then, for the security of the bit-plane information according to each bit, random transposition is executed. M and M/2 are 512 and 256. We used a random noise form from the separately performed random displacement of the two regions as watermark information.

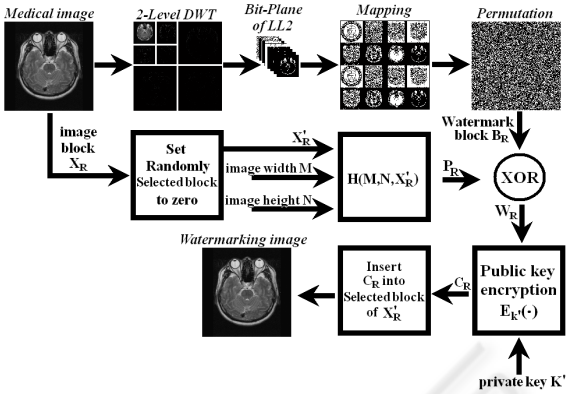


Figure 1: A block diagram of the proposed watermarking algorithm to embed a watermark.

$$W_p = permutation(W) = \{w_p(i,j) = w(i',j') \mid 0 \le i,i' \le M, 0 \le j,j' \le \frac{M}{2}\} \qquad (2)$$

The embedding position of the watermark is the image block, which is randomly selected within the lower three bits of the original image, and the ROI region becomes the LSB. These requirements prevent a wrong diagnosis by the watermark information in the property of medical images. In common cases, the central region in the image is the object for the ROI region, and in a particular case, the object may be assigned.

In the Eq. (3), X_R' means the zero-initialized relevant region X_R in the block, which is randomly selected and includes a watermark. M and N mean the horizontal and vertical size of the image. P_R is a bit stream that passed the MD5 cryptograph hash function H(.) with X_R' and M, and N. The Eq. (4) is a result of the XOR operation between the bit stream and the watermark information B_R. The public-key cryptograph system cryptographers W_R as shown in Eq. (5). $E_K(.)$ is a public-key cryptograph system and K' is a personal-key. The watermarked image is generates by inserting the data C_R into X_R'.

$$H(M,N,X'_R) = (p_1^R, p_2^R, \cdots, p_s^R), s = 128 \qquad (3)$$

$$W_R = P_R \oplus B_R \qquad (4)$$

$$C_R = E_{K'}(W_R) \qquad (5)$$

The procedure to embed a watermark is as follows.

[The embedding procedure**]**

(1) To generate watermark information, the DWT is executed for the original image by two levels.

(2) The composed 8-bit bit-planes make the LL2 as binary.

(3) Bit-plane information is mapped as the same size of the original image.

(A school logo was inserted rather than the bit-plane value of the LSB to express the copyrighter's position.)

(4) For protecting the bit-plane information for each bit, M and N is randomly displaced as two regions, 512 and 256, separately.

(5) The watermark embedding position is the image block, which is randomly selected and is within the lower 3 bit of the original image, and the ROI region becomes the LSB.

(6) The selected image block is initialized.

(7) M and N, and X_R' are used for the inputs of the MD5 cryptograph hash function.

(8) The XOR operation is performed between the watermark information and P_R generated by ⑦.

(9) A public-key cryptograph system cryptographers W_R, which is a result from (8).

(10) W_R is putted into X_R' and a watermarked image is obtained.

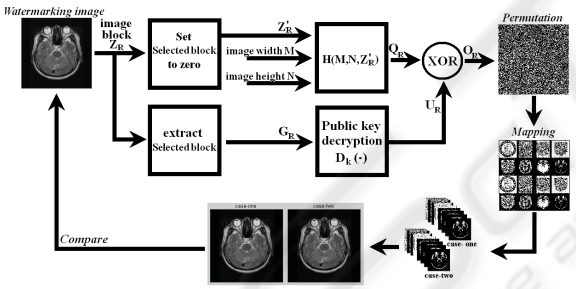


Figure 2: A block diagram of the proposed watermarking algorithm to extract a watermark.

2.2 Extracting Process

The procedure extracting a watermark in the watermark-embedded image is shown in Fig. 22. First, the watermarked image is divided into two regions, a block Z_R', which is a result of initializing a block Z_R that has a watermark as 0, and a block that includes a watermark value. A hash value from Z_R' and the image size M and N creates Q_R of 64 bits. The block that has watermark information is decoded as a public-key as shown in Eq. (6). Then, the XOR operation shown in Eq. (7) extracts the embedded watermark information, which is a form of random noise.

$$U_R = D_K(Z_R) \tag{6}$$

$$O_R = Q_R \oplus U_R \tag{7}$$

At this step, deteriorated part comes out if the watermarked image was manipulated. Unless the attack was severe, however, the part does not appear sufficiently since it is a form of random noise. For perfect integrity verification, we perform random inverse transposition to make it as 7-bit bit-plane, and combine them to organize an image. The position information of the LSB corresponds to the lowest bit finds the copyrighter's position by a school logo. Verifying the obtained two images and the watermarked image helps to estimate integrity. We can find the part that has a problem through the combined two images if a certain part of the watermarked image was manipulated, so it is possible to estimate integrity by compare it with the distorted image.

The procedure for extracting a watermark is as follows.

[The extracting procedure]

(1) A watermarked image is divided into a watermark-inserted block and a block that is a result of initializing Z_R as 0.

(2) Through a hash value from Z_R‘ and M and N, Z_R, the size of 64 bits, is created

(3) A watermark-embedded block G_R is decoded as a public-key.

(4) The XOR operation is performed between Q_R and U_R.

(5) Inverse random transposition produces 7-bit bit-planes of the original image. Then the algorithm makes the combined two image with a school logo pattern, and compare it with the watermarked image.

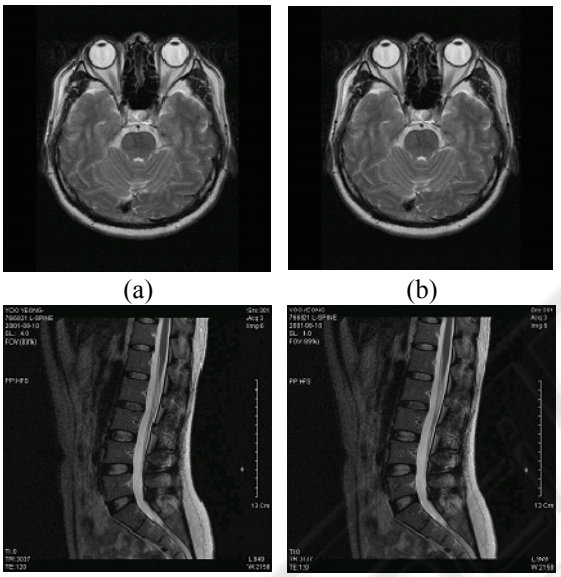
3 EXPERIMENTAL RESULTS

Computer simulations were carried out to demonstrate the performance of the proposed watermarking method. Performance of the PC is Pentium4 CPU 3GHz, 512MBRAM. We changed the stored files to common image data through the program VisualGate, which is offered on http://www.infinitt.com/ and stores image files with the form of DICOM. To estimate subject performance of invisibility, we generated many watermark-embedded images through various algorithms. The PSNR (peak signal-to-noise ratio) was used as an objective measure. The *NC* (normalized correlation), shown in Eq. (8), was used

to estimate robustness of the image. When the correlation is not about 1, then the algorithm regards the transmitted medical image as a modified one and requires retransmission. Otherwise, it extracts the watermark and determine the image was forged or not by verification through the watermark.

$$NC = \frac{\sum_{i=0}^{N/2-1}\sum_{j=0}^{N/2-1} W(i,j)\hat{W}(i,j)}{\sum_{i=0}^{N/2-1}\sum_{j=0}^{N/2-1}[W(i,j)]^2} \quad (8)$$

$W(i,j)$ means the embedded watermark, and $\hat{W}(i,j)$ means the extracted watermark.



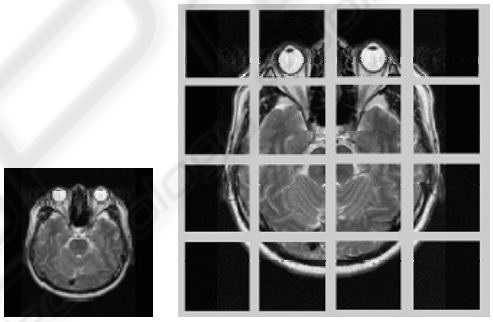
(a) (b) (c) (d)

Figure 3: (a) Brain Image, (b) Watermarked Brain Image, (c)) Spine Image, and (d) Watermarked Spine Image.

On the simulation of the DWT generation algorithm based on the public-key cryptograph algorithm, Brain and Spine, and Chest images was used with 512x512 sized. The coefficient of the wavelet filter bank uses Daubechies D4 and the original image was wavelet-transformed by binary level.

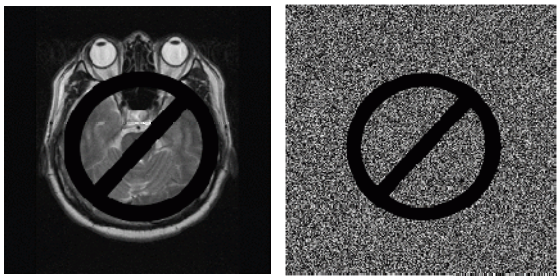
Invisibility of the watermark for Brain and Spine images are shown in Fig. 3. The original Brain image is shown in (a). The PSNR of the watermark-embbeded image, shown in (b), is 43.49[dB]. The original Spine image is shown in (c). The PSNR of the watermark-embbeded image, shown in (d), is 43.68 [dB].

On the simulation of Brain image using the DWT generation method based on the public-key cryptograph algorithm, we transformed the images 512x512 sized to binary level by the wavelet transform. The basis region image of the LL2, which was transformed by the binary level DWT, is shown in Fig. 4 (a). Its size is 128x128. The logo image will be embedded into the LSB of the bit-plane band for copyright verification. The mapped image about bit-plane of the LL2 basis region image is shown in Fig. 4 (b). The LSB bit-plane image replaces the logo image for copyright verification. The divided image, shown in (b), will include the mapped bit-plane image. A medical image, whose ROI region was severely forged, is shown in Fig. 5 (a). A watermark-extracted image is shown in Fig. 5 (b) and its NC value is 0.88. It means the medical image was forged. We transposed the watermark of the two layers randomly for integrity of the forged medical image. With looking at them, we can notice they were forged.



(a) (b)

Figure 4: (a) Watermark information for Brain Image and (b) bit-plane mapped images and divided images.



(a) (b)

Figure 5: (a) Illegally manipulated image and (b) Watermark-extracted image (NC=0.88).

With the results of simulation, invisibility is excellent even though the position of the watermark is expanded from the LSBs to MSBs. In addition, it is possible to verify integrity by extracting the embedded watermark from a forged image. Thus, the proposed method helps to prevent problems with illegal manipulation of medical images, such as

military service absurdity or medical insurance fraud.

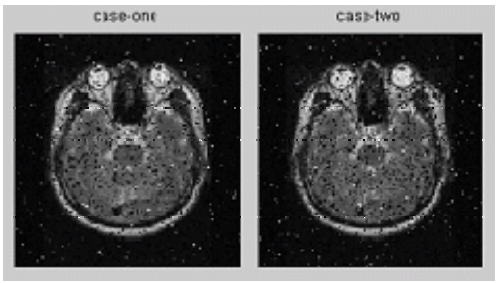


Figure 6: Extracting the watermark and verifying integrity.

4 CONCLUSIONS

To protect integrity and copyright protection of medical images, we proposed a medical image protection system by applying the digital watermarking algorithm that provides copyright and authentication of the multimedia contents. For integrity verification, the proposed method uses the whole region based on the public-key cryptograph, which is transformed by the DWT transform. To create a watermark, the wavelet-transformed watermarking method based on the public-key cryptograph divides the lowest frequency image into bit-planes. They are transposed randomly by mapping with the logo image of the lowest bit to verify its copyright. This proposed algorithm is robust that attackers cannot modify or remove the original watermark. Experimental results show that integrity verification is more robust and invisibility.

ACKNOWLEDGEMENTS

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (MEST)"(KRF-2009-0071269)

REFERENCES

http://www.pccgroup.com/

http://www.dicomanalyser.co.uk/

Anand, D., Niranjan, U.C., 1998. Watermaking medical images with patient information. *In proc. IEEE/EMBS Conference*, Hong Kong, China, pp. 703-706.

Wakatani, A., 2002, Digital Watermarking for ROI Medical Images by Using Compresses Signature Image. *HICSS*, vol. 6, pp. 157.

Shih, F.Y., Wu, Y., 2005, *Robust watermarking and compression for medical images based on genetic algorithms*,' Information Sciences, In Press.

Coatrieux, C., Maitre, H., Sankur, B., Rolland, Y., Collorec, R., 2000, Relevance of Watermarking in Medical Imaging. *2000 IEEE EMBS Conf. On Information Technology Applications in Biomedicine,* pp.250-255.

Giakoumaki, A., Pavlopoulos, S., Koutsouris, D., 2003, A medical image watermarking scheme based on wavelet transform. *In Proc. of the 25th Annual Int. Conf. of the IEEE-EMBS*, pp. 856–859.

Cox, I., Kilian, J., Leighton, T., Shamoon, T., 1997, Secure Spread Specturm watermarking for Multimedia. *IEEE Trans. on Image Processing*, vol. 6, no. 12, pp. 1673-1687.