Medical Video Watermarking Scheme for Electronic Patient Records

Nisreen I. Yassin
National Research Center,
Cairo, Egypt.

Nancy M. Salem
Faculty of Engineering,
Helwan University,
Cairo, Egypt.

Mohamed I. El Adawy
Faculty of Engineering,
Helwan University,
Cairo, Egypt.

ABSTRACT

This paper proposes a blind watermarking algorithm for transferring medical data securely over the public network. A text watermark is embedded into (YCBCR) color channels of each medical video frame using Discrete Wavelet Transform and Principle Component Analysis. In our experiments, the watermark includes the electronic records for patients with three different sizes. Experimental results show high imperceptibility and robustness against attacks. The maximum PSNR achieved by the proposed technique is 61 dB while the least is 45 dB. The maximum number of characters embedded in the medical video frame is 146 characters.

General Terms

Internet Security, Telemedicine, Digital Watermarking.

Keywords

Medical watermarking, Electronic Patient Record, Blind watermarking, Principal Component Analysis, Discrete Wavelet Transform, Binary watermark, Image entropy, Quantization Index Modulation.

1. INTRODUCTION

Digital watermarking techniques play an important role in health data management systems to protect the confidentiality of medical data, monitoring the access and the retrieval of the data, and preserving their integrity. Several medical imaging techniques are used in diagnostic decisions such as: Magnetic Resonance Imaging (MRI), Computer Tomography (CT), Ultrasound, and X-Rays. A watermark containing medical information such as (patient record, hospital signature, and medical diagnostic) can be embedded into these images when sharing it through the network. Sharing EPR (Electronic Patient Record) over the networks requires; confidentiality, reliability, and availability [1-3]. The quality of the medical image is very important in the correct diagnostic process, so extreme care must be considered when watermark embedding process takes place [4]. Telemedicine is one of the important fields that use digital watermarking for medical signals and images [5-7].

Giakoumaki et al. propose a wavelet based algorithm that embeds multiple watermarks into medical images in order to help in the authentication of doctor's digital signature and in the integrity control of the data [8]. Khamlichi et al. present a combined technique for embedding the patient data record directly into mammography images for tamper detection [9]. Chemak et al. use wavelet transform in medical image watermarking technique for the service of neurological diseases. Information about patients is transmitted to doctor's mobile phone by embedding the medical information inside diagnostic images [10]. Umaamaheshvari et al. [11] present Independent Component Analysis and Ridgelet transform for watermarking baby scan image. Ramesh et al. [12] use discrete wavelet transform to protect the copyright of digital signature of medical images. Hajjaji et al. present an approach for watermarking medical images using the techniques of Code Division Multiple Access (CDMA), Discrete Wavelet transform (DWT) and Error Correcting Code (ECC) [13]. Kumar et al. [14] propose a high capacity scheme for using in telemedicine applications. Their algorithm is based on Haar wavelet transform of radiological images. Spread spectrum is used for embedding medical information into radiological images based on pseudo-random sequence pairs. Wakatani et al. [15] proposed a wavelet based medical image watermarking. Lim et al. [16] presented a web based image authentication system for verifying the integrity of medical images.

In [17] Giakoumaki et al. proposed a wavelet based multiple watermarking scheme. In this scheme, the medical image is decomposed into four levels DWT. A robust watermark is embedded in the 4th level where high capacity is not a required. While, patient information is embedded in the second decomposition level. An index watermark is embedded in the third level. Memon et al. [18] proposed robust and fragile watermarking algorithm. Firstly, the ROI and RONI regions of the medical image were separated. The robust watermark was embedded in high frequency coefficient of IWT in RONI region. Also, a fragile watermark was embedded into the spatial domain of ROI region of medical image. In [4], a medical image watermarking scheme based on segmentation is proposed. GUI segmentation based approach is used for separating ROI and RONI parts of medical image. The RONI parts were watermarked using second generation lifting based DWT while the ROI parts were preserved. In [19], a watermarking algorithm based on LSB (Least Significant Bit) of medical images to check the security issues of patient data sharing.

This paper is organized as follows: section 2 presents the proposed watermarking scheme. Section 3 introduces the experimental results and the conclusion is given in section 4.

2. PROPOSED SCHEME

2.1 Embedding Process

Step 1: Divide video into frames $(2N \times 2N)$, and then convert RGB frames to YCBCR frames.

Step 2: Choose the luminance component Y of each frame, apply DWT on it. This result in four multi-resolutions sub-bands $(N \times N)$: $LL_1, HL_1, LH_1, and\ HH_1$. For each band apply DWT again to get 16 sub-bands $(N/2 \times N/2)$. For each band

in the 16 sub-bands, apply one more DWT to get 64 sub-bands each is $(N/4 \times N/4)$.

Step 3: Divide each sub-band I_s with $(N/4 \times N/4)$ dimension into $n \times n$ non-overlapping blocks where the number of blocks is $k = (N/4 \times N/4)/(n \times n)$.

Step 4: Calculate the entropy E_n of each $n \times n$ block in each sub-band I_s, where the entropy is defined as a statistical measure of randomness that can be used to characterize the texture of the input image [20]:

$$E_n = -\sum (\mathrm{P} .^{\times} \log_2(\mathrm{P})) \quad (1)$$

where, P contains the histogram counts, and the operator $(.^{\times})$ means multiplication of each element of matrix A with its corresponding element of matrix B.

Step 5: Select maximum entropy blocks which are the edges blocks of the frame. The position of these selected blocks is saved to be used in the extraction process and can be considered as a secret key. Then apply PCA to each selected block.

Step 6: For building the QIM quantizer, two uniform quantizers q_0 and q_1 are required to apply equation (2). These quantizers must be defined in the range of the maximum and minimum values of the principle components of the entropy selected blocks all over each wavelet sub-band. The minimum value in that range is selected to be q_0, then q_1 will be as follows:

$$\mathrm{q}_1(\mathrm{x}) = \mathrm{q}_0(\mathrm{x}) + \frac{\Delta}{2} \quad (2)$$

where, Δ is the step size of the quantizers.

Step 7: Watermark preparation:

1-
nsert the medical information into a text file.

2-
onvert the text file to a binary form and according to the size of the text file, generate a watermark image of size $16 \times 16, 32 \times 32,$ and 64×64. Convert the binary image into a vector $W = \{w_1, w_2, \dots, w_{h \times h}\}$ of zeros and ones.

Step 8: Divide the vector W into 64 parts $p_1, p_2, \dots, p_{64}$. Each watermark part p_i is embedded in each corresponding sub-band I_s. The number of the selected maximum entropy blocks is equal to the number of the bits in each watermark part p_i. The watermark bits are embedded with strength α into the maximum coefficient M_i of each PC block Y_i. For embedding process, if the watermark value is 1 (resp. 1) each element M_i is quantized with $q_0$which has the minimum distance from M_i and if -1 (resp. 0) is to be embedded then M_i is quantized with q_1.

$$M_i' = Q + \alpha W \quad (3)$$

where Q is corresponding to q_0 or q_1 and α is the watermark embedding strength (Impact factor). Q is saved as a second key for using in the extraction process. The value of α in this algorithm is 9 for all selected wavelet bands. If the watermark bit is 1 then adding α to the maximum coefficient in the Y block but if it is zero, then α is subtracted from the same coefficient.

Step 9: Apply inverse PCA on the modified PC block Y_i' to obtain the modified wavelet block.

Step 10: Apply the inverse DWT to obtain the watermarked luminance component of the frame. Finally reconstruct the RGB watermarked frame and obtain the watermarked video.

The embedding steps are repeated for CB and CR channels of the frame to compare the results obtained from each channel.

2.2 Data Extraction Process

The steps used for watermark extraction is the same as the steps in the embedding but no need for the original video sequence. Only the watermarked video and the two secret keys are required for the extraction procedure.

Step 1: Convert the watermarked video into frames. Each RGB frame is converted to YCBCR representation.

Step 2: For each Y, CB, and CR component, apply DWT to decompose the channel into 64 multi-resolution sub-bands. Divide each sub-band into $n \times n$ non-overlapping blocks.

Step 3: Using the first secret key, one can get the watermarked blocks. Apply PCA transformation for each block.

Step 4: By using the second secret key, one can extract the watermark by applying the following equation:

$$W' = \frac{\mathrm{M}_i' - \mathrm{Q}}{\alpha} \quad (4)$$

Step 5: The extracted watermark is compared with the original watermark by computing the similarity measure between them as follows:

$$NC = \frac{\sum_i \sum_j W(i,j).W'(i,j)}{\sum_i \sum_j W(i,j)^2} \quad (5)$$

where, NC is the normalized correlation. NC value is 1 when the watermark and the extracted watermark are identical and zero if the two are totally different from each other.

Step 6: Convert the binary extracted watermark to a text. The extracted text is compared with the original text and the number of error characters is counted. The character error rate is computed as follows:

$$CER = \frac{E_{ch}}{T_{ch}} \quad (6)$$

where, E_{ch} is the number of error characters and T_{ch} is the total number of characters.

3. EXPERIMENTAL RESULTS

The performance of the proposed algorithm is tested using CT video frames. The size of the frame is 512×512, the algorithm is evaluated when varying the watermark size by changing the number of characters in the embedded text. For evaluating the performance of any watermarking system, Peak

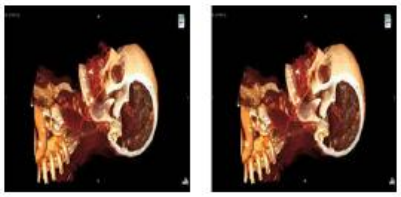
Signal to Noise Ratio (PSNR) is used as a common measure of the visual quality of the watermarking system. To calculate the PSNR, first the Mean Square Error (MSE) between the original and watermarked frame is computed as follows:

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{j}=1}^{\mathrm{N}} [\mathrm{I}(\mathrm{i},\mathrm{j}) - \mathrm{I}'(\mathrm{i},\mathrm{j})]^2 \quad (7)$$

where, M, N are the size of the frame, and $I(i,j), I'(i,j)$ are the pixel values at location (i,j) of the original and watermarked frames. Then, PSNR is defined as:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (8)$$

The watermarked frames appear visually identical to the original frames. Figure 1 shows an original frame and its corresponding watermarked frame. The following cases describe the embedded text watermark and results for each case.



(a) (b)

Fig 1: (a) The original frame, (b) the watermarked frame.

- Case 1: The text contains 36 characters (each character is represented by seven bits) which mean that the binary text contains 252 bits. This text is formatted to be a watermark with size 16×16 (256 bits). The text contains the following information:

First name:	Yasser
Second name:	Ibrahim
Family name:	Yassin
Age:	030
Sex:	1
Hospital signature:	57357

The embedded text will be in the form:

* Yasser * Ibrahim * Yassin * 0 3 0 * 1 * 5 7 3 5 7 *

Authentication is done by extracting the watermark text from the frames of the video file. Then, the extracted watermarks are compared with each other for a window of frames. Finally, taking the most repeated characters to be compared with the original watermark. Here, the used window of frames is 5 frames. Table 1 shows the extracted watermarks from the first window, PSNR, and NC. Then, the rest of the table contains the comparison results for the Y channel and the corresponding CER values. CER values are calculated for each window of first 5 frames, the first10 frames, then the first 15 frames and so on.

In a similar way, Tables 2 and 3 summarize results of extracting the watermark from CB and CR channels respectively. As declared, the watermark needs 50 frames to be extracted from Y channel while needs 20 frames for both CB and CR channels. The value of PSNR in case of CB and CR channels is higher than its value in case of Y channel. This means that embedding in color channels is better than embedding in luminance channel using the proposed algorithm. In this case the authentication is achieved with 1 error character.

- Case 2: The text contains 73 characters (each character is represented by seven bits) which mean that the binary text contains 511 bits. This text is repeated twice to be a watermark with size 32×32

(1024 bits). Two new fields are added to the text, first could be the treatment and the second could be the diagnostic. The embedded text is:

*Yasser*Ibrahim*Yassin*normal_abcdefghijk*pain_l mnopqrstuvw*030*1*57357*#

In this case repetition of the text inside the watermark reduces the number of frames needed for extraction process. The text is extracted with 1 error character by using 20 frames in case of Y channel and 10 frames in case of color channels.

- Case 3: The text contains 146 characters (each character is represented by seven bits) which means that the binary text contains 1022 bits. This text is repeated 4 times to be a watermark with size 64×64 (4096 bits).The embedded text is:

*Yasser*Ibrahim*Yassin*normal_abcdefghijklmnopqrst uvwxyz_abcdefghijklmnopqrstuvwxyz*pain_abcdefghij klmnopqrstuvwxyz_abcdefghijklmnop*030*1*57357*#

Table 1. Extracting 16x16 watermark from Y channel

Frame No.	PSNR	NC	Extracted watermark
1	59.1916	0.9853	*Yaswer*Ibrano*{k{s`n>478*5*u7{57*#
2	59.1047	0.9853	*Yas{ar.Ibrahm*yk{sa~>5;8.1*u7{57*#
3	59.0100	0.9632	*Iassar*Mbrao{myk{qa~>6;6?1*u7{57*#
4	58.6087	0.9706	*Xiswur2cryhsm2yaswin>0s0z5*u7{u7*#
5	58.7093	0.9632	*Ya3{orzIbRghomyasw`n;:32:1*u73uw+#
	Extracted Watermark		**CER**
1:5	*Yas r*Ibrah m*y s 1* 7 57#*		0.3889
1:10	*Yass r*Ibrah m*yass n 1* 7357*#		0.2500
1:15	*Yass r*Ibrahim*yassin 1* 7357*#		0.1944
1:20	*Yass r*Ibrahim*yassin *1* 7357*#		0.1667
21:25	*Yasser*Ibrahim*yassin *1* 7357*#		0.1389
26:30	Yasser*Ibrahim*yassin* 3 *1* 7357*#		0.0833
30:40	*Yasser*Ibrahim*yassin* 3 *1* 7357*#		0.0833
41:45	*Yasser*Ibrahim*yassin* 30*1* 7357*#		0.0556
46:50	*Yasser*Ibrahim*yassin*030*1* 7357*#		0.0278

Table 2. Extracting 16x16 watermark from CB channel

Frame No.	PSNR	NC	Extracted watermark
1	61.3997	1	*Yassev*Ibsahim*ya{sinj030*1*u7357*#
2	61.4464	1	*Yawms*Mbrehim*yaswinj430*1*u7357*#
3	61.1314	1	*[ases*}csahim*yassin*930*1*u7357*#
4	61.2983	0.9926	*Xawses.Ibrahim*yassin*230*1*u7357*#
5	60.6897	0.9853	*Yaq{eR.y{rahim*yas{in*030*1*u7357*#
	Extracted Watermark		**CER**
1:5	*Ya e *Ibrahim*yassin* 30*1* 7357*#		0.1389
1:10	*Yaer*Ibrahim*yassin*030*1* 7357*#		0.0833
1:15	*Yaser*Ibrahim*yassin*030*1* 7357*#		0.0556
1:20	*Yasser*Ibrahim*yassin*030*1* 7357*#		0.0278

Table 3. Extracting 16x16 watermark from CR channel

Frame No.	PSNR	NC	CER	Extracted watermark
1	60.8848	1	0.3611	*ycse~zicsqhim*yassinj0{1*1*u7357*#
2	60.9737	0.9853	0.3056	*y%sr.Ib{ahim*yas{inj50*1*u7357*#
3	61.1682	1	0.3056	*Yeer.Mbahim*yas{inj5?0*1*u7357*#
4	61.7171	1	0.1944	*Ye{ser*Ibsahim*yas{inj730*1*u7357*#
5	61.6346	1	0.1944	*Yesser*Ibsahim*ya{in*870*1*u7357*#
	Extracted Watermark			CER
1:5	*Y s erIbahim*yas in 0*1* 7357*#			0.2500
1:10	*Y sser*Ibrahim*yas in* 0*1* 7357*#			0.1389
1:15	*Yasser*Ibrahim*yas in*030*1* 7357*#			0.0556
1:20	*Yasser*Ibrahim*yassin*030*1* 7357*#			0.0278

Table 4. Summary table

Watermark size	16x16 36 characters			32x32 73 characters			64x64 146 characters		
Color Channel	Y	CB	CR	Y	CB	CR	Y	CB	CR
PSNR	59.13	61.15	61.10	51.95	54.18	54.16	45.00	46.68	46.52
Extraction Frames	50	20	20	20	10	10	5	3	6
CER	0.027	0.027	0.027	0.013	0.013	0.013	0	0	0

Increasing the repetition of the text in the watermark to 4 times decreasing the number of frames required for extraction of the text to 5 frames in case of Y channel, to 3 frames in case of CB channel, and to 6 frames in case of CR channel as summarized in Table 4. As can be seen, the authentication using number of frames is more efficient and more powerful than using one image. Embedding the watermark in the color channels CB and CR gives higher values of PSNR than embedding in luminance Y channel. Also, its extraction results comes faster using less number of frames. A comparison between the proposed algorithm and algorithms in [4] and [19] has been done. In [19] the number of medical information bits that embedded in the medical image is 425 bits while in the proposed algorithm the medical information bits are 252, 511, and 1022. The comparison with the scheme in [4] is concluded in table 5.

Table 5. Comparison table

Schemes	PSNR	No. of Characters	Frame Size
[4]	45.12	137	512x512
Proposed scheme	46.68	146	512x512

4. CONCLUSIONS

This paper presented a high capacity watermarking scheme which can be used in telemedicine applications. The algorithm depends on embedding a patient record into medical videos. DWT in conjunction with PCA transform are used in the embedding process to get the best location for hiding the watermark. Different radiological video frames were used for evaluation. The proposed scheme is imperceptible and robust against several attacks and has a good performance compared with previous medical schemes.

6. REFERENCES

[1] Chao, H. M., Hsu, C. M., and Miaou, S. G. 2002. A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. IEEE Transactions on Information Technology in Biomedicine, vol. 6, no. 1, 46-53.

[2] Navas, K. A., Thampy, S. A., and Sasikumar, M. 2008. ERP hiding in medical images for telemedicine. In

[3] Proceedings of World Academy of Science and Technology, vol. 28.

[4] Zain, J. and Clarke, M. 2005. Security in telemedicine: issues in watermarking medical images. The 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications SETIT, March 27-31.

[5] Rathi, S. C. and Inamdar, V. S. 2012. Medical images authentication through watermarking preserving ROI. Health Informatics, International Journal (HIIJ), vol. 1, no. 1.

[6] Kong, X. and Feng, R. 2001. Watermarking medical signals for telemedicine. IEEE Transaction on Information Technology in Biomedicine, vol. 5, no. 3, 195-201.

[7] Coatrieux, G., Lecornu, L., Roux, Ch., and Sankur, B. 2006. A Review of image watermarking applications in healthcare. IEEE Eng. Med. BiolSoc, vol. 1, 4691-4695.

[8] Raul, R. C., Claudia, F. U., and Gershom, T. B. 2007. Data hiding scheme for medical images. International Conference on Electronics, Communications and Computers.

[9] Giakoumaki, A., Pavlopoulos, S., and Koutouris, D. 2003. A medical image watermarking scheme based on Wavelet transform. In Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, vol. 1, 856 - 859.

[10] Khamlichi, Y., Machkour, M., Afdel, K., and Moudden, A. 2006. Medical image watermarked by simultaneous moment invariants and content-based for privacy and tamper detection. In Proceedings of the 6th WSEAS International Conference on Multimedia Systems & Signal Processing, Hangzhou, China, April 16-18, 109-113.

[11] Chemak, C. , Lapayre, J. C., and Bouhlel, M. S. 2007. New Watermarking Scheme for Security and Transmission of Medical Images for Pocket Neuro Project. Radio Engineering, vol. 16, no. 4.

[12] Umaamaheshvari, A. and Thanushkodi, K. 2011. Digital image watermarking based on Independent Component Analysis and Ridgelet transform. International Journal of Computer Science and Network Security, IJCSNS, vol. 11, no. 4.

[13] Ramesh, S. M and Shanmugam, A. 2011. An efficient robust watermarking algorithm in filter techniques for embedding digital signature into medical images using discrete Wavelet transform. European Journal of Scientific Research, vol. 60, no.1, 33-44.

[14] Hajjaji, M. A, Mtibaa, A. and Bourennane, E. B. 2011. Watermarking of medical image: new approach based on multi-layer method. International Journal of Computer Science Issues, IJCSI, vol. 8, Issue 4, no. 2.

[15] Kumar, B., Anand, A., Singh, S. P., and Mohan, A. 2011. High capacity spread-spectrum watermarking for telemedicine applications. World Academy of Science, Engineering and Technology, vol. 79.

[16] Wakatani, A. 2002. Digital watermarking for ROI medical images by using compressed signature image. International Conference on System Sciences.

[17] Lim, Y., Xu, C. and Feng, D. 2001. Web based image authentication using invisible fragile watermark. Workshop on Visual Information Processing, VIP.

[18] Koumaki, G., Pavlopoulos, S., and Koutsouris, D. 2006. Multiple image watermarking applied to health information management. IEEE Transactions on Information Technology in Biomedicine, vol. 10, no. 4.

[19] Memon, N. A., Gilani, S. A. M., and Qayoom, S., 2009 Multiple watermarking of medical images for content authentication and recovery. IEEE International Multi-topic Conference.

[20] Hajjaji, M. A., Mtibaa, A. and Bourennane, E. B. 2011. A watermarking of medical image: method based "LSB". Journal of Emerging Trends in Computing and Information Sciences, vol. 2, no. 12.

[21] Gonzalez, R. C., Woods, R. E., and Eddins, S. L. 2004 Digital image processing Using Matlab. Pearson Prentice Hall, New Jersey.