Computer Methods and Programs in Biomedicine (2004) **76**, 13—19

Computer Methods and Programs in Biomedicine

www.intl.elsevierhealth.com/journals/cmpb

Simultaneous storage of patient information with medical images in the frequency domain

Rajendra Acharya U. [a,*], **U.C. Niranjan** [b], **S.S. Iyengar** [c], **N. Kannathal** [a], **Lim Choo Min** [a]

[a] *Electronic and Computer Engineering Division, School of Engineering, Ngee Ann Polytechnic, 535 Clementi Road, Singapore 599489, Singapore*
[b] *Department of Bio-Medical Engineering, Manipal Institute of Technology, Manipal 576119, India*
[c] *Department of Computer Science, Louisiana State University, Baton Rouge, LA 70808, USA*

Received 13 February 2004; accepted 13 February 2004

KEYWORDS
Interleaving;
DCT;
Watermarking;
Encryption;
DPCM;
JPEG

Summary Digital watermarking is a technique of hiding specific identification data for copyright authentication. Most of the medical images are compressed by joint photographic experts group (JPEG) standard for storage. The watermarking is adapted here for interleaving patient information with medical images during JPEG compression, to reduce storage and transmission overheads. The text data is encrypted before interleaving with images in the frequency domain to ensure greater security. The graphical signals are also interleaved with the image. The result of this work is tabulated for a specific example and also compared with the spatial domain interleaving.

1. Introduction

With the present trend of using Internet as a medium to transmit images and patient data, it is of utmost importance to preserve the authenticity of patient information. Any exchange of data between hospitals involves large amount of vital patient information such as bio-signals, word documents and medical images. Therefore it requires efficient transmission and storage techniques to cut down cost of health care. Interleaving one form of data such as 1D signal, or text file, over digital images can combine the advantages of data security with efficient memory utilization [1]. In this paper, the authors adapt this technique to store texts and graphical signals in medical images by sharing last bits of discrete cosine transform (DCT) coefficients from the middle frequency range onwards, in the frequency domain.

2. Methods and system description

The watermarking techniques are divided into two basic categories.

1. Spatial domain watermarking [2], in which the least significant bit (LSB) of the image pixels is replaced with that of the watermark (authentication text). This method of spatial domain watermarking is very susceptible to noise. A more robust watermark can be embedded in the same way that a watermark is added to paper. In this method, a watermark symbol may be superimposed over an area of the picture and then some fixed intensity value for the watermark is added

*Corresponding author.
E-mail address: aru@np.edu.sg (Rajendra Acharya U.).

0169-2607/$ — see front matter © 2004 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.cmpb.2004.02.009

to the varied pixel values of the image. The resulting watermark may be visible or invisible depending on the value of the watermark intensity. The main disadvantage of spatial domain watermarks is that picture cropping can be used to eliminate the watermark.
2. Frequency domain watermarking, in which the image is first transformed to the frequency domain (DCT) and then the low frequency components are modified to contain the authentication text [3].

Watermarking can be applied in the frequency domain by applying transforms like fast Fourier transform (FFT), discrete Fourier transform (DFT), discrete wavelet transform (DWT), discrete cosine transform (DCT). Similar to spatial domain watermarking, in this method the values of the chosen frequencies are altered from the original to contain the watermark (authentication text).

Since high frequencies will be lost by compression or scaling, the watermark signal is applied to the lower frequencies or applied adaptively to frequencies that contain important information of the original picture. Since watermarks applied to the frequency domain will be dispersed over the entirety of the spatial image upon inverse transformation, this method is not susceptible to defeat by cropping as the spatial technique.

2.1. Compression by JPEG standard

JPEG algorithm [4] is a lossy compression technique, which gives maximum compression with the least error. Blocks of 8 × 8 pixels are selected in a raster fashion from the image to be compressed. This forms the input to the encoder. Applying DCT to these blocks transforms the image from spatial domain to the frequency domain. The DCT contains the dc coefficient, which measures the zero frequency, and 63 ac coefficients. The DCT coefficients are quantized according to perceptual criteria. The dc coefficient is differentially encoded, while the ac coefficients are transformed into a single dimensional array by zigzag encoder. This is then run length coded. Separate Huffman coding is done for the differential dc coefficients and ac run length codes. The Huffman table consists of a series of variable length codes, which allocates less number of bits for the most commonly occurring DCT coefficients and more number of bits for the less frequently occurring ones. The inverse process of coding reconstructs the original image from the coded data (Fig. 1).

2.2. The interleaving process

Fig. 2, as shown below indicates the steps involved in interleaving an image (size: 128 × 128 pixels) with patient information. The information to be stored is encrypted before watermarking to enhance security [5]. Eight bits are usually employed to indicate the gray level of image pixel. The entire image is divided into 8 × 8 blocks. For interleaving the LSB of each DCT coefficient is replaced by the text data (after the quantization and zigzag encoding of JPEG compression). The eight bits of ASCII code in the text file will replace the LSBs of eight consecutive DCT coefficients of the image from the middle frequency range onwards (from 32ed to 63rd coefficients). If the data file is a graphic signal having 16-bit word, 16 consecutive DCT coefficients are used for interleaving a single word. The LSB is chosen for data interleaving because, the resulting degradation of image is minimal. In

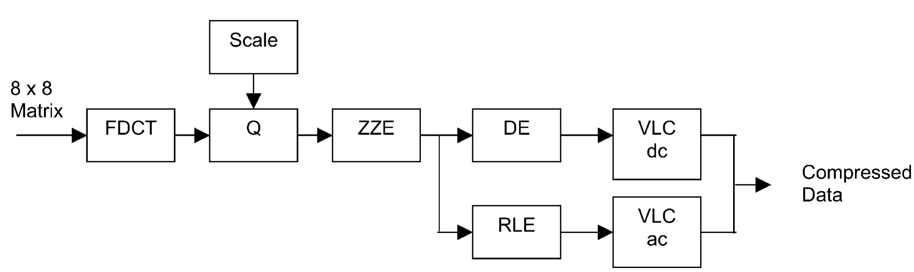


Fig. 1 Block diagram of an encoder. FDCT, forward discrete cosine transform; Q, quantization; ZZE, zigzag encoder; RLE, runlength encoder; DE, differential encoder; VLC, variable length coding; ac, ac coefficients; dc, dc coefficients.

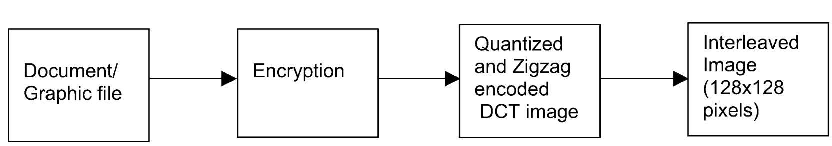


Fig. 2 Proposed scheme for storage.

the decoding side, the interleaved text or graphical signal can be obtained by de-interleaving, i.e., extracting the LSBs and concatenating the same, before inverse quantization and zigzag coding.

2.2.1. Encryption of the text file

A part of a typical patient record (text file) is shown in Fig. 3a. The document is a sequence of ASCII codes, which is encrypted by taking the logarithm of the ASCII codes. The encryption algorithm can be mathematically stated as:

$$T_e = (\log(T_o \times 2) \times 100) - 300 \tag{1}$$

where T_e is the encrypted text; T_o the ASCII code of the original text (or graphics file). The encrypted information (T_e) is stored as an integer.

The decrypted text is obtained by:

$$T_o = \exp\left\{\frac{T_e + 300}{100 - \log(2)}\right\} \tag{2}$$

The encryption transform pairs given in Eqs. (1) and (2) yield exact reconstruction, even when T_e is rounded off to the nearest integer. Fig. 3b shows the encrypted document corresponding to the file shown in Fig. 3a. It may be noted that both the files occupy the same amount of memory space.

2.2.2. Encryption of the graphical file

Analog ECG is usually recorded on magnetic tape (Holter). To store it in the digital form, the ECG signal is sampled at a suitable rate so as to retain relevant details of peaks, troughs and frequency. The sampled signal is converted into digital form, whose dynamic range is determined by the word length of analog to digital converter (ADC) output.

The differential pulse code modulation (DPCM) technique [5] is extensively used to reduce the dynamic range of the signal. The DPCM is used here for encrypting the ECG signal. The differential error output (which is random and uncorrelated) is used as the encrypted version of the original signal. The DPCM is a predictive coding technique where in the present sample x_n in a signal is expressed as a sum of linearly weighted past sample x_{n-1} and the error signal e_n [6].

$$x_n = p x_{n-1} + e_n \tag{3}$$

The predictor coefficient p is determined by the least square technique, as

$$p = \frac{r(1)}{r(0)}, \quad \text{where } r(m) = \sum_{n=0}^{N-1-m} x_n x_{n+m}$$

The differential error e_n is stored along with the first sample x_0 and the linear predictor coefficient p. The ECG signal x_n can be reconstructed from the error signal by auto-regression technique (Eq. (3)). Thus, the symbol pair (p, x_0) forms the key for the encrypted electrocardiogram (ECG) signal e_n. This quantized e_n is interleaved with the LSB of image DCTs. As the dynamic range of the error signal e_n is very small, it is coded with only 4 bits.

Fig. 4a and b displays the original and reconstructed ECG signals, while Fig. 4c elicits the prediction error signal e_n.

Adaptive delta modulation (ADM) is a DPCM scheme in which the error signal e_n is encoded into a single bit. This single bit, providing just two options, is used to increase or decrease the estimate of x_n denoted by $\hat{x}_n$. The amount of increase or decrease is specified by the step length $S(n)$, which is a multiple of the basic step size S_0 and is determined adaptively. At the nth sample instant the step length generated is related to the step length of the previous sampling instant (Eq. (4)).

$$S(n) = |S(n-1)| e_n + S_0 e_{n-1} \tag{4}$$

This step length is used to estimate $\hat{x}_n$ as shown:

$$\hat{x}_n = \hat{x}_{n-1} + S(n) \tag{5}$$

The encrypted signal for storage is the error signal and is generated on the basis whether the actual signal value x_n is larger or smaller than the

SINGAPORE HEART FOUNDATION
SINGAPORE

Patient Ref.No:493526311
Name of the doctor:Dr.Lim Hock
Name of the patient:Ms.Ann Liew
Age: 56 years
Address:Kismis Avenue, Block 90,
#05-02, Singapore
Date of Admission:2.11.1989
Results:T wave inversion

(a)

sÓÆÌÃºïÎÑÀsÄÀºÑÔsÂÎÕÌ¿ºÔÆÎÌ
sssssÓÆÌÃºïÎÑÀ

sÏâôêæïôsÑæç˜Ìð¯¤-¢¦¨¢□□
sÌâîæsðçsôéæsåðäôðr¯¿r˜ÊêîsÄðäì
sÌâîæsðçsôéæsñâôêæïô¯Ëó˜ºïïsÊêæ÷
sºèæ¯s¦¨syæâró
sºåårææóó¯Éêóîêósºöæïõæ“s¼íðäìs-œ“
s|œ¦•œ “sÓêïèâñðræ
s¿âôæsðçsºåîêóóêðï¯˜□□˜□-«-
sÑæóõíôó¯Ôs÷âö_

(b)

Fig. 3 Encryption of patient information: (a) original patient information; (b) encrypted patient information.

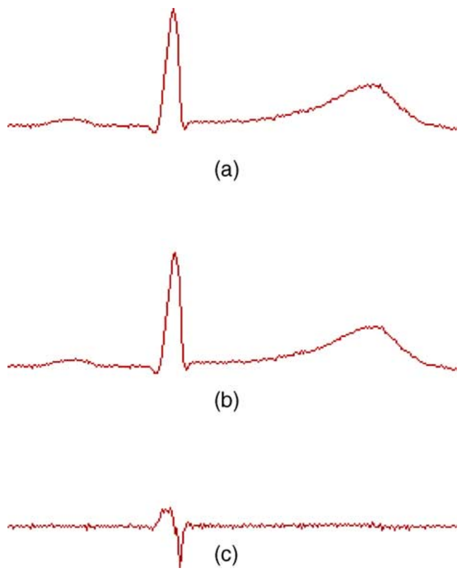


Fig. 4 Results of DPCM techniques: (a) original ECG signal; (b) reconstructed ECG signal; (c) error signal.

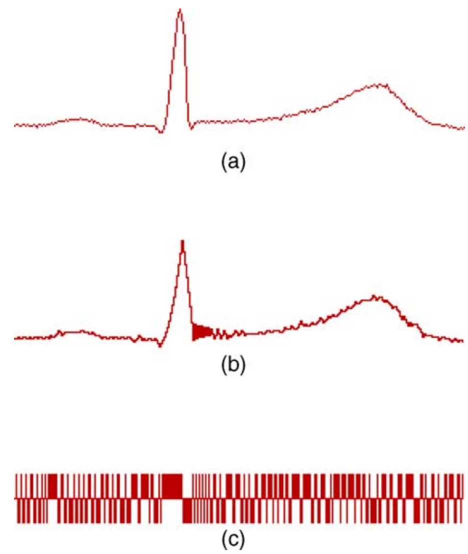


Fig. 5 Results of ADM techniques: (a) original ECG signal; (b) reconstructed ECG signal; (c) error signal.

estimated value $\hat{x}_n$.

$$e_n = +1 \quad \text{if } x_n > \hat{x}_n$$
$$e_n = -1 \quad \text{if } x_n < \hat{x}_n$$

Here e_n is just one bit in length and is interleaved with the LSB of the image pixel. The original heart rate signal, reconstructed signal and error signal are shown in Fig. 5a—c, respectively.

As can be seen from the results in DPCM and ADM, the error signal is random and uncorrelated and has no resemblance to the original heart rate signal x_n. This property of e_n is exploited by using the error signal as encrypted version of x_n. In the case of ADM, e_n is encoded with 1 bit while in DPCM e_n requires 4 bits for encoding. Thus, one sample of encrypted heart rate signal is interleaved into one pixel in case of ADM, while in DPCM, 4 pixels are required to interleave one encrypted sample. The heart rate signal is reconstructed from the error signal using regressive Eq. (4) or (5), and as can be seen from Figs. 4b and 5b, the reconstructed signals are good replicas of the original signals.

3. Result

The ASCII codes of the encrypted text shown in Fig. 3b are broken into bits and interleaved into the DCT coefficients of Angiogram image of Fig.6a. The resulting image is shown in Fig. 6b. The interleaving in the middle frequency from 32 coefficients onwards does not affect the picture quality. This is attributed to the fact that the change in LSB of these DCTs does not affect the quality of the picture considerably.

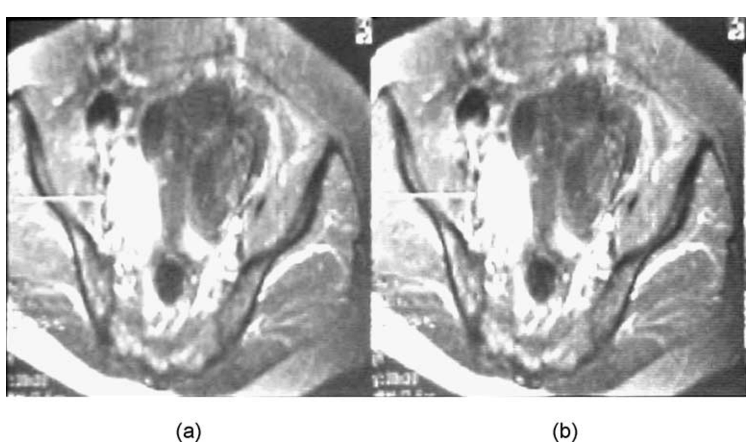
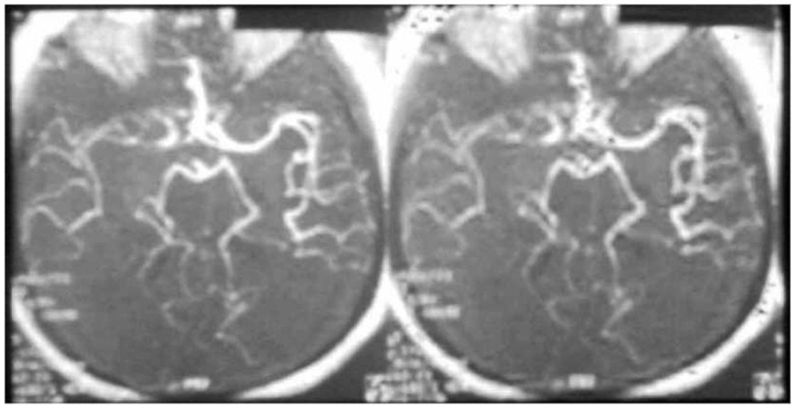


Fig. 6 Result of interleaving text in the Angiogram image: (a) original image; (b) interleaved image.



(a) (b)

Fig. 7 Result of interleaving text in the MRI image: (a) original image; (b) interleaved image.

A quantitative assessment of the method is obtained by evaluating the normalized root mean square error (NRMSE) as defined:

$$\mathrm{NRMSE}\,(\%) = \sqrt{\frac{\sum_{y=0}^{N-1}\sum_{x=0}^{M-1}[f(x,y) - f_{\mathrm{w}}(x,y)]^2}{\sum_{y=0}^{N-1}\sum_{x=0}^{M-1}[f(x,y)]^2}} \times 100 \quad (6)$$

where N is the total number of columns; M the total number of rows in the image; $f(x, y)$ the original pixel intensity; $f_{\mathrm{w}}(x, y)$ the modified (interleaved) pixel intensity.

The ASCII codes of the encrypted text shown in Fig. 3b are broken into bits and interleaved into the DCTs of Angiogram image (Fig. 6a) and magnetic resonant imaging (MRI) image (Fig. 7a). The resulting images are shown in Figs. 6b and 7b, respectively. The error signal e_n obtained from DPCM shown in Fig. 4c, is interleaved into the X-ray image (Fig. 8a). The resulting interleaved image is shown in Fig. 8b. As can be seen from these results, the process does not affect the picture quality. This is attributed to the fact that the change in LSB of a DCT changes its contribution to the picture by 1 part in 256. The text and ECG signal information are interleaved into all the pixels in the lower half of the image in the frequency domain, which contribute less to the quality of the image.

Fig. 9a and b shows the intensity histograms of the original and interleaved (with error signal of Fig. 4c Angiogram images [7]. It can be seen that the shape of the interleaved image's histogram bears resemblance to that of the original image.

The proposed technique of interleaving additional data into an image can also be used for transmission purposes, wherein patient information embedded in the medical image can be sent over communication channels, as a single data entity. In the presence of channel noise, the interleaved information embedded in the LSB is as susceptible to noise as any other bit in pulse code modulation (PCM) type of transmission. Thus, the proposed method of compact storage of patient information would be useful in telemedicine projects

(a) (b)

Fig. 8 Result of interleaving DPCM error signal in the X-ray image: (a) original image; (b) interleaved image.

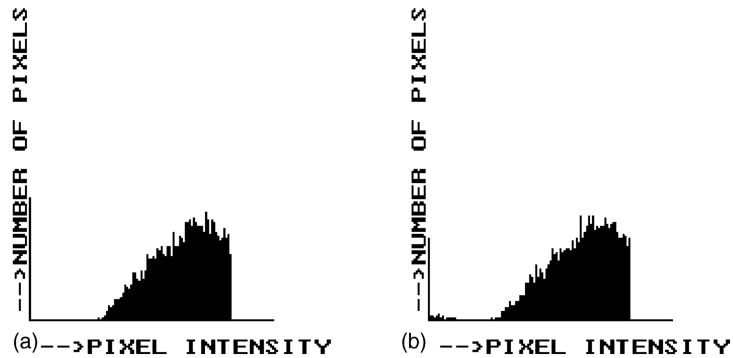


Fig. 9 Histogram of Angiogram images: (a) original image; (b) interleaved image.

Table 1 Results of interleaving data with image in the frequency domain

Image	Text (NRMSE%)	DPCM (NRMSE%)	ADM (NRMSE%)
Angiogram	3.06	3.06	3.02
MRI	4.82	4.83	4.80
X-ray	4.67	4.67	4.60

as well, which could have problems of transmitting different aspects of information related to the same patient separately. This is particularly true of remotely and poorly connected regions like most places in the III world.

The performance of such proposed scheme on medical image files is as shown in Table 1. The table shows that the NRMSE is very small and should therefore not alter the information of the original image, which is observed in practice.

In the proposed scheme, the interleaving is done after the DCT quantization (of JPEG). This helps in reconstructing the interleaved data exactly, as there are no further lossy data compression. In order to compare the proposed scheme with direct interleaving in spatial domain, the results of the latter is given in Table 2. The results in Table 1 are inferior due to lossy nature of JPEG compression. Owing to the widespread use of JPEG compression standard, the proposed method of compact storage of patient information with medical image in frequency domain may find applications in future.

Table 2 Results of interleaving data with image in the spatial domain

Image	Text (NRMSE%)	DPCM (NRMSE%)	ADM (NRMSE%)
Angiogram	0.81	0.81	0.79
MRI	0.91	0.91	0.89
X-ray	1.01	1.02	0.89

4. Hardware and software specification

The program is developed in C programming. The image used has 256 gray levels. The program involves the encryption of the text/graphical file and interleaving in the frequency domain using the DCT.

5. Mode of availability

The program is freely available (source code, executables for Windows/DOS, documentation, picture/graphic files) on request from the author.

6. Conclusions

A technique of interleaving patient information text and graphical documents is presented for efficient storage. Text files are encrypted using logarithmic technique and then interleaved in the frequency domain. The technique is tested for different images and the NRMSE was found to be less than 5%. Security of information can be further enhanced by choosing the position of the interleaved bit according to a specific plan known only to the authorized users. The performance under noisy environment or on poor quality images however needs to be explored.

References

[1] H. Berghel, Watermarking cyberspace, Commun. ACM 40 (11) (1997) 19—24.

[2] F. Neil Johnson, Z. Duric, S. Jajodia, Information Hiding: Steganography and Watermarking—Attacks and counterattacks, Kluwer Acadamic Publishers, Dordrecht, 2000.
[3] H. Berghel, L. O'Gorman, Protecting ownership rights through watermarking, IEEE Comput. (1996) 101—103.
[4] G.K. Wallance, The JPEG: still image compression standard, Commun. ACM 34 (4) (1991) 30—44.
[5] U. Rajnendra Acharya, D. Anand, P. Subbanna Bhat, U.C. Niranjan, Compact storage of medical images with patient information, IEEE Trans. Information Technol. Biomed. 5 (4) (2001) 320—323.
[6] S. Haykins, Communication Systems, Wiley Eastern, New Delhi, 1996.
[7] R.C. Gonzalez, P. Wintz, Digital Image Processing, Addison-Wesley, Reading, MA, 1987.