Communications

Compact Storage of Medical Images With Patient Information

Rajendra Acharya U, Deepthi Anand, Subbanna Bhat P, and Niranjan U. C

***Abstract*—Digital watermarking is a technique of hiding specific identification data for copyright authentication. This technique is adapted here for interleaving patient information with medical images to reduce storage and transmission overheads. The text data are encrypted before interleaving with images to ensure greater security. The graphical signals are compressed and subsequently interleaved with the image. Differential pulse-code-modulation and adaptive-delta-modulation techniques are employed for data compression, and encryption and results are tabulated for a specific example.**

***Index Terms*—Adaptive delta modulation, differential pulse code modulation, interleaving, watermarking.**

I. Introduction

The exchange of databases between hospitals require efficient transmission and storage to cut down the cost of health care. This exchange involves a large amount of vital patient information such as biosignals, word documents, and medical images. When handled separately using information media like the Internet, it results in excessive memory utilization and transmission overheads. Interleaving one form of data (such as a one-dimensional (1-D) signal or text file) over digital images can combine the advantages of data security with efficient memory utilization [1]. Watermarking is a technique for storing copyright information. In this paper, the authors adapt this technique to store text and graphical signals in medical images by sharing the last bits of pixels.

Watermarking techniques are divided into two basic categories, which are: 1) spatial-domain watermarking, in which the lower order bits of the image pixels are replaced with that of the watermark or adding some fixed intensity value to a picture and 2) frequency-domain watermarking, in which the image is first transformed to the frequency domain [discrete Fourier transform (DFT) or discrete cosine transform (DCT)], and then the low-frequency components are modified to obtain watermarked images [2].

II. Interleaving Process

Fig. 1 indicates the steps involved in interleaving an image with a data file. The information to be stored is encrypted before watermarking to enhance security [3]. The ASCII code in the text file is swapped with the least significant bit (LSB) of the grayscale bit by bit. Eight bits of each ASCII code thus replace LSBs of eight consecutive pixels of the image. (If the data file is a graphic signal having a 16-bit word, 16 consecutive pixels are used for interleaving a single word.) This cycle of interleaving an ASCII code in consecutive pixels is repeated to include all the characters in the text file. The LSB of the pixel is chosen for data interleaving because the resulting degradation of the image is minimal. Depending upon the nature of the signal, (i.e., text or graph), three different encryption algorithms are used.

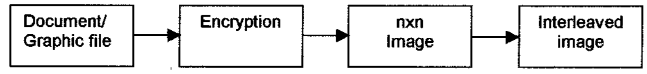
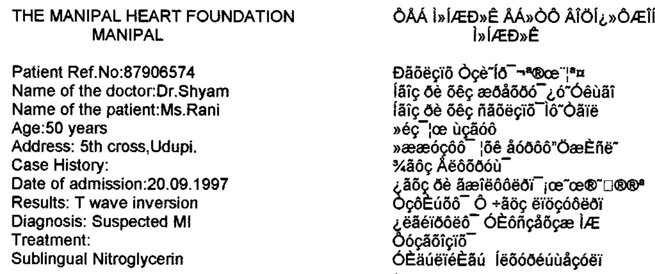


Fig. 1. Proposed scheme for storage.



(a) (b)

Fig. 2. Encryption of patient information. (a) Original patient information. (b) Encrypted patient information.

A. Encryption of the Text File

A part of the typical patient record (text file) is shown in Fig. 2(a). 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

$$T_e = \Big(\mathrm{Log}(T_o * 2) * 100\Big) - 300 \tag{1}$$

where $T_e =$ the encrypted text and $T_o =$ 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

$$T_0 = \exp\Big\{(T_e + 300)/100 - \log(2)\Big\}. \tag{2}$$

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

B. Encryption of the Heart Rate Signal Graph

An analog electrocardiogram (ECG) is usually recorded on a 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 the analog-to-digital converter (ADC) output. The interval between two successive QRS

Manuscript received December 7, 2000; revised March 21, 2001.

R. A. U is with the Electrical and Computer Engineering Department, Ngee Ann Polytechnic, Singapore 599489, on leave from the Department of Bio-Medical Engineering, Manipal Institute of Technology, Manipal 576 119, India.

D. Anand is with the Department of Electrical and Electronic Engineering, New Jersey Institute of Technology, Newark, NJ 07102 USA.

S. B. P is with the Department of Electronics and Communication Engineering, Karnataka Regional Engineering College, Surathkal 574 157, India.

N. U. C is with the Department of Bio-Medical Engineering, Manipal Institute of Technology, Manipal 576 119, India.

Publisher Item Identifier S 1089-7771(01)07411-8.

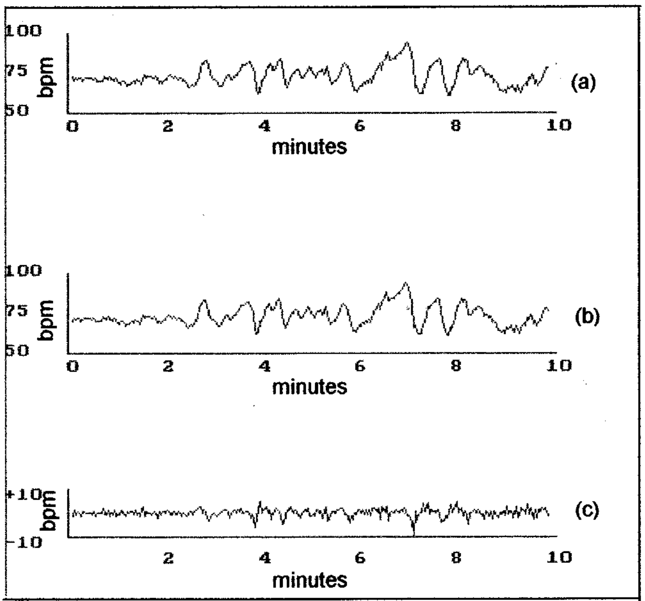


Fig. 3. Results of DPCM technique. (a) Original signal. (b) Reconstructed signal. (c) Error signal.

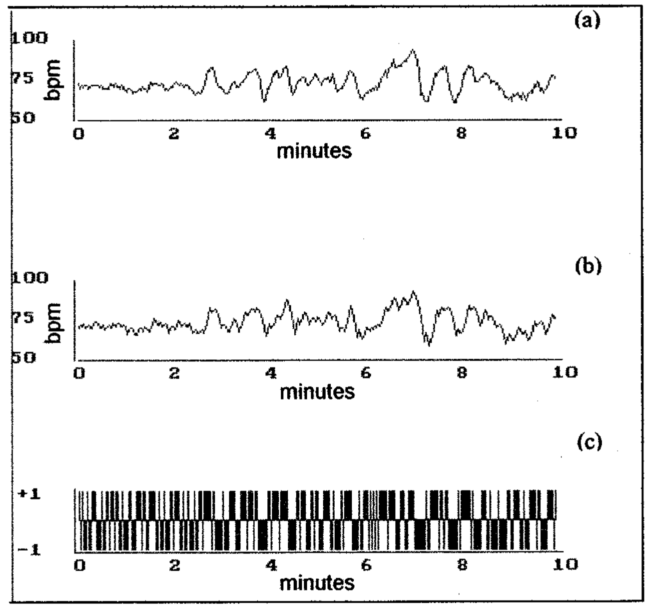


Fig. 4. Results of ADM techniques. (a) Original signal. (b) Reconstructed signal. (c) Error signal.

complexes is defined as the r–r interval (t_{r-r} seconds), which is determined by the QRS algorithm [4]. The heart rate (beats per minute) is given by the following expression:

$$\mathrm{HR} = 60/t_{r-r}. \tag{3}$$

The heart-rate signal is formed by concatenating consecutive instantaneous heart rates.

The differential pulse code modulation (DPCM) technique is extensively used to reduce the dynamic range of the signal. The DPCM is used here for encrypting the heart-rate 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 error signal e_n [5]

$$x_n = px_{n-1} + e_n. \tag{4}$$

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

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

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

Fig. 3(a) and (b) displays the original and reconstructed heart rate signals, while Fig. 3(c) 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 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 [see (5)]

$$S(n) = \Big|S(n-1)\Big|.e_n + S_0 e_{n-1}. \tag{5}$$

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

$$\hat{x}_n = \hat{x}_{n-1} + S(n). \tag{6}$$

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 estimated value $\hat{x}_n$

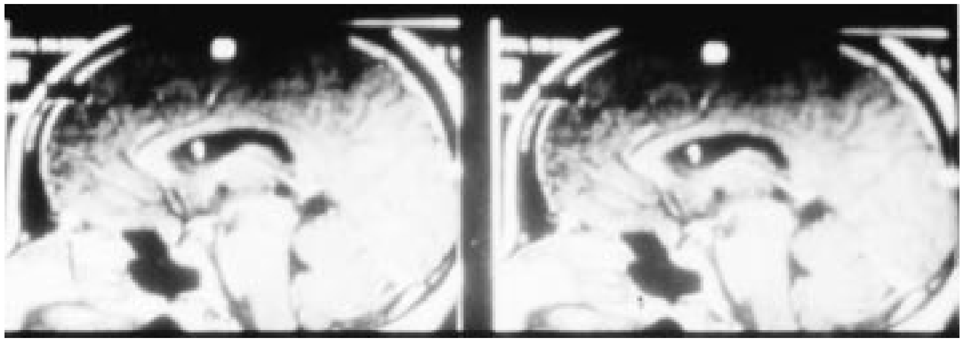
$$e_n = +1, \qquad \text{if } x_n > \hat{x}_n$$
$$e_n = -1, \qquad \text{if } x_n < \hat{x}_n.$$

Here, e_n is just 1 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. 4(a)–(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 an 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, four pixels are required to interleave one encrypted sample. The heart-rate signal is reconstructed from the error signal using regressive equations (4) or (5) and, as can be seen from Figs. 3(b) and 4(b), the reconstructed signals are good replicas of the original signals.

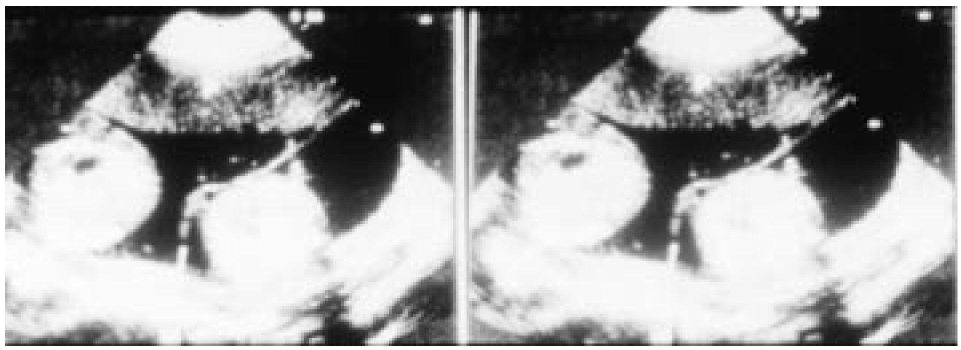
III. Result

The ASCII codes of the encrypted text shown in Fig. 2(b) are broken into bits and interleaved into the pixels of a magnetic-resonance-imaging (MRI) image [see Fig. 5(a) (size: 196 × 260 pixels)]. The resulting image is shown in Fig. 5(b). The error signals e_n obtained from DPCM and ADM, shown in Figs. 3(c) and 4(c), respectively, are interleaved into the angiogram and the ultrasound



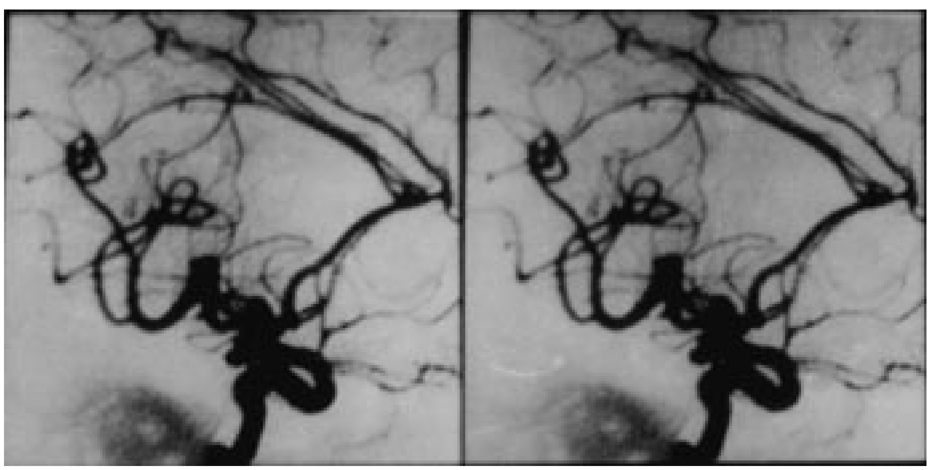
(a) (b)

Fig. 5. Result of interleaving text in the MRI image. (a) Original image. (b) Interleaved image.



(a) (b)

Fig. 6. Result of interleaving ADM error signal in the ultrasound image. (a) Original image. (b) Interleaved image.

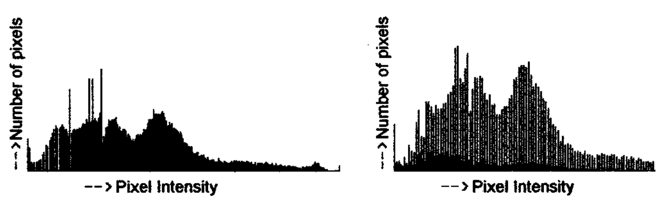


(a) (b)

Fig. 7. Result of interleaving DPCM error signal in the angiogram image. (a) Original signal. (b) Interleaved signal.

images of Figs. 6(a) (size: 200 $\times$ 265 pixels) and 7(a) (size: 270 $\times$ 229 pixels). The resulting interleaved images are shown in Figs. 6(b) and 7(b). 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 the LSB of a pixel changes its brightness by one part in 256. The text and heart-rate information are interleaved into all the pixels of the image.

Fig. 8(a) and (b) shows the intensity histograms of the original and interleaved [with error signal of Fig. 4(c)] ultrasound images. It can be seen that the shape of the histogram bears resemblance to that of the original image. The change in the population of pixels of a specific intensity is definite in nature. For example, consider two pixels with grayscale values 0 and 1. When interleaved, the "0" pixel may remain a "0" or change to "1." Similarly, the "0" pixel may remain at "1" or change to "0." Thus, there is a redistribution of pixels 0 and 1. Such a redistribution occurs among all consecutive pairs of even and odd pixels, such as "2" and "3," "4" and "5," and so on. This pairwise redistribu-



(a) (b)

Fig. 8. Histogram of ultrasound images. (a) Original image. (b) Interleaved image.

TABLE I
RESULTS OF INTERLEAVING DATA WITH IMAGE

Image	Text (NRMSE%)	DPCM (NRMSE %)	ADM (NRMSE%)	MNRMSE (%)
MRI	0.70	0.70	0.69	1.24
Ultrasound	0.53	0.54	0.52	1.43
Angiogram	0.50	0.50	0.50	0.76

tion of pixel values explains the resemblance between the original and modified histograms.

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

$$\mathrm{NRMSE}(\%) = \sqrt{\frac{\sum_{Y=0}^{N-1}\sum_{X=0}^{M-1}\left[f(x,\,y) - f_w(x,\,y)\right]^2}{\sum_{Y=0}^{N-1}\sum_{X=0}^{M-1}\left[f(x,\,y)\right]^2}} \times 100 \tag{7}$$

where $N =$ the total number of columns, $M =$ the total number of rows in the image, $f(x,\,y) =$ the original pixel intensity, and $f_w(x,\,y) =$ the modified (interleaved) pixel intensity.

From the definition of the NRMSE, it is seen that the maxima occurs when the LSB of all the pixel values are altered. The equation for maximum NRMSE then becomes

$$\mathrm{MNRMSE}(\%) = \sqrt{\frac{(N * M)}{\sum_{Y=0}^{N-1}\sum_{X=0}^{M-1}\left[F(X,\,Y)\right]^2}} \times 100. \tag{8}$$

Results of the interleaving data with image are shown in Table I.

In order to assess the effect of interleaving on reduced intensity images, the images were converted to 128 intensity levels at a coding of 7 bits/pixel and interleaving operation was carried out on them. The values of NRMSEs for these reduced intensity images doubled. This is because the denominator after the computation of the square root in both (7) and (8) get halved due to halving of image intensity levels, thereby doubling the NRMSE values.

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 a pulse-code-modulation (PCM) type of transmission. Thus, the proposed method of compact storage of patient information would be useful in telemedicine projects as well.

IV. CONCLUSION

This paper has presented a technique of interleaving patient information such as text documents and physiological signals with medical images for efficient storage. Text files are encrypted using a logarithmic technique, and heart-rate signals are encrypted by DPCM and ADM techniques prior to interleaving. The technique is tested for different images, and the NRMSE was found to be less than 0.71% for 8-bit encoded pixel intensity. 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.

REFERENCES

[1] H. Berghel, "Watermarking cyberspace," *Commun. ACM*, vol. 40, no. 11, pp. 19–24, Nov. 1997.
[2] H. Berghel and L. O'Grossman, "Protecting ownership rights through digital watermarking," *IEEE Computer*, vol. 29, pp. 101–103, July 1996.
[3] S. Haykins, *Communication Systems*. New York: Wiley, 1996.
[4] J. Pan and W. J. Thompkins, "A real time QRS detector algorithm," *IEEE Trans. Biomed. Eng.*, vol. BME-32, pp. 230–236, Mar. 1985.
[5] R. C. Gonzalez and P. Wintz, *Digital Image Processing*. Reading, MA: Addison-Wesley, 1987.