

Reliable Transmission and Storage of Medical Images with Patient Information using Error Control Codes

Jagadish Nayak, P Subbanna Bhat, M Sathish Kumar, Rajendra Acharya U

Abstract-- A new method for compact storage and transmission of medical images with concealed patient information in noisy environment is evinced. Digital Watermarking is the technique adapted here for interleaving patient information with medical images. The patient information, which comprises of text data and signal graph, is encrypted to prevent unauthorized access of data. The latest encryption algorithm (Rijndael) is used for encrypting the text information. Signal graphs (ECG, EEG, EMG etc.) are compressed using DPCM technique. To enhance the robustness of the embedded information, the patient information is coded by Error Correcting Codes (ECC) Reed Solomon (RS) codes. The noisy scenario is simulated by adding salt and pepper (S&P) noise to the embedded image. For different Signal to Noise Ratio (SNR) of the image, Bit Error Rate (BER) and Number of Character Altered (NOCA) for text data and percentage distortion (PDIST) for the signal graph is evaluated. It is elicited that coded systems can perform better than the uncoded systems.

Index Terms—ECC, interleaving, encryption, RS codes, SNR, PDIST, BER.

I. INTRODUCTION

Exchange of database between hospitals needs efficient and reliable transmission and storage techniques to cut down cost of health care. This exchange involves large amount of vital patient information such as bio-signals, 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 1-D signal, or text file, over digital images can combine the advantages of data security with efficient memory utilization [1]. Watermarking

Jagadish Nayak is with the department of E&C Engg., Manipal Institute of Technology, Manipal -576104 Karnataka, India. (Telephone: 91-820-2571060, e-mail: jag.nayak@mit.manipal.edu).

P Subbanna Bhat is with department of E&C Engg. National Institute of Technology Karnataka, Surathkal, India (telephone: 91 0824, e-mail: p_subbannabhat@yahoo.com).

M Sathish Kumar is with department of E&C Engg. Manipal Institute of Technology, Manipal -576104 Karnataka, India. (Telephone: 91-820-2571060, e-mail: mskuin@yahoo.com).

Rajendra Acharya U is with Department Of ECE, Ngee Ann Polytechnic, 535 Clement Road 08-03-09 Singapore 599 489

is a technique for storing copyright information. In this paper, the technique is employed to store text and graphical signals in medical images by sharing last bits of pixels. Water marking is broadly classified into two categories one is spatial domain water marking and another is frequency domain watermarking. In spatial domain lower order bits of the image pixels are replaced by the text data without losing identity of the image [2]. In frequency domain, image is first transformed into frequency domain (DFT, DCT and DWT) and then low frequency components are modified to obtain water marked images [3]. In this paper the information bit streams are interleaved in LSB of medical image. Practical transmission and storage scenarios are far from ideal due to the contamination arising from the presence of noise and other interference. Error Control Coding (ECC) techniques are proposed in this work for enhancing the reliability of transmission and storage in the presence of noise and other interference [4]. Adding Salt and Pepper (S&P) noise to the interleaved image simulates the effects of practical storage and transmission scenario. The reliability and robustness of the patient information is demonstrated using RS codes. The performance of ECC scheme is demonstrated by plotting the BER versus SNR of the S&P noise-corrupted image for both text and signal graph data. Number of characters corrupted in the text can be regarded as a measure of performance of the transmission or storage system. The quality of the signal graph is studied by evaluating percentage distortion in the signal for different values of SNR.

II. THE INTERLEAVING PROCESS

Fig.1 indicates the steps involved in interleaving an image (size: 128x128 pixels) with data file. The information to be stored is encrypted before watermarking to enhance security [5]. This encrypted patient information is coded with error control codes, which make the system robust and reliable. The coded information bit streams are swapped with the least significant bit (LSB) of the grey scale bit by bit. Each bit of the code thus replaces LSB of one pixel in the image. This cycle of interleaving coded bits in consecutive pixels is repeated to include all the bit streams. The LSB of the pixel is chosen for data interleaving because, the resulting degradation of image is minimal.

1) Encryption of the text file

The information to be stored is encrypted before watermarking to enhance the security. Highly secured algorithm called as Advanced Encryption Standard (AES),

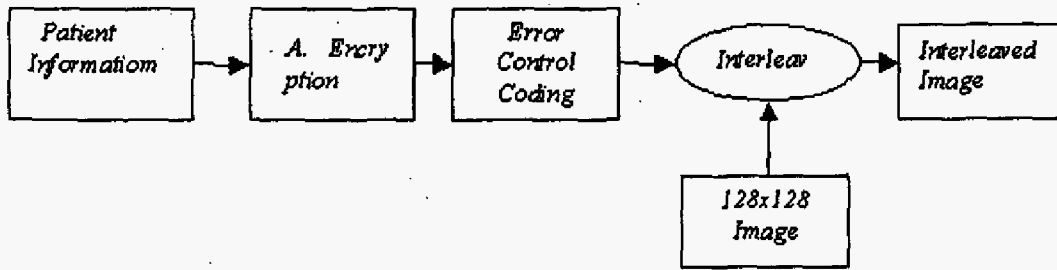


Fig. 1. Block diagram of interleaving process.

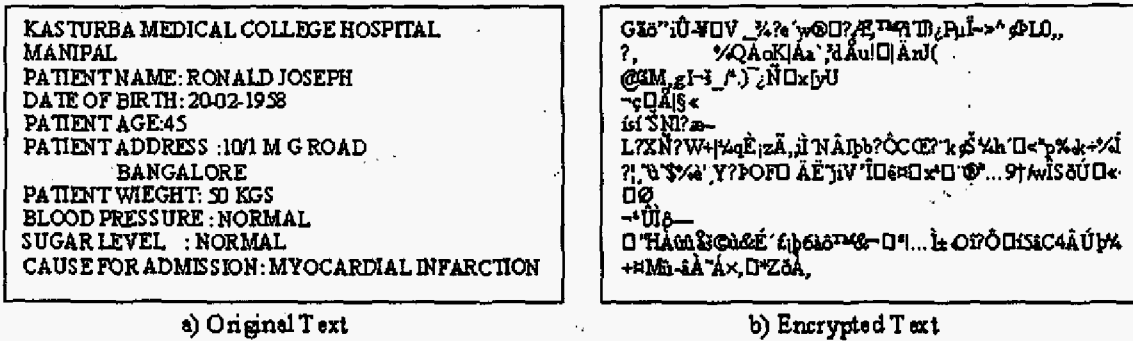


Fig. 2. Encryption Results.

this is developed by National Institute of standards and Technology, is used for the encryption of text data. This algorithm is also called as Rijndael algorithm, which is designed by John Daemen and Vincent Rijmen. Rijndael's key length is defined to be either 128, or 192 or 256 bits in accordance with the requirements of the AES. [6]. Figure 2(a) and 2(b) shows the original patient data and the encrypted data respectively.

2) Encoding of Bio-signal graph

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 ADC output. 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 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 [7] 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 .

$$x_n = px_{n-1} + e_n \quad (1)$$

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.(1)). Thus, the symbol pair (p, x_0) forms the key for the encoded ECG signal e_n . This quantized e_n is interleaved with the LSB of image. As the dynamic range of the error signal e_n is very small, it is coded with only 4 bits. Figure 3 shows the results of this process.

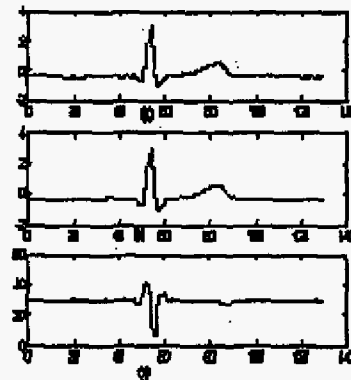


Fig. 3. Results of DPCM techniques: a) Original signal b) Reconstructed ECG signal c) Error signal



Fig. 4. MRI Image

3) ERROR CORRECTING CODES FOR PATIENT INFORMATION (REED SOLOMON (RS) CODE)

To enhance the reliability and robustness of the watermarking, patient information is coded by ECC. In this paper, we propose the use of an important class of ECC called as block code for enhancing the reliability of transmission and storage of the type of messages dealt with in this work. A comparative study of the objective parameters (BER, NOCA, and PDIST) is demonstrated for RS code.

The RS block code is organized on the basis of groups of bits. Such a group of bits are referred to as symbol. Each symbol can be considered to be non-binary symbol, which indicates that we are dealing with m bit symbol [8]. Since we deal only with symbols we must consider that if an error occurs even in a single bit of a symbol, the entire symbol is in error. RS code has following characteristics

Block length: $n=2^m-1$

Number of parity digits: $n-k = 2t$

Minimum distance: $d = 2t + 1$

This can correct combination of t or fewer errors. As it was in the case of BCH codes, such RS codes, which correct t or fewer errors, are aptly called as t -error-correcting RS code.

III. RESULTS

The patient information, which includes both text data and bio-signal graph, are encrypted using the algorithm explained above. A MRI of size 128X128 is used for the interleaving process. The encrypted patient information is broken into bit streams and coded with ECC. These code words are embedded into the image as explained in the interleaving process. As mentioned earlier, adding S&P noise of various densities simulates the noisy transmission and storage scenario. The Signal to noise ratio (SNR) is computed for the noisy image. Which is given in (2)

$$SNR = 10 \log_{10} \left[\frac{\sum_{x=1}^M \sum_{y=1}^N (f(x,y))^2}{\sum_{x=1}^M \sum_{y=1}^N [f(x,y) - f_n(x,y)]^2} \right] \text{dB} \quad (2)$$

Where $f(x,y)$ is Interleaved Image and $f_n(x,y)$ is noise corrupted image [9]. This is the quantitative measure; a class of criteria used often called the mean square criterion. Figure 4a, 4b and 4c shows original, interleaved and Noise corrupted MRI image respectively. As an objective measure for the quality of the de-interleaved or extracted text data and signal graph, BER, NOCA and PDIST is evaluated. BER gives the amount of error in the recovered patient information as compared to original information embedded in the image before transmitting or storing in noisy environment. NOCA will provide the number of text altered in recovered text data as compared to original embedded text data. The quality of the recovered bio-signal graph is evaluated using a quantitative (PDIST) measure called as percentage distortion, which will show the amount of distortion in the recovered signal as compared to the embedded signal before transmission or storage. These objective parameters are evaluated for various SNR. The robustness and reliability of the transmission and storage system is demonstrated for ECC. Depending on the error correcting capability the performance of the (15,3) and (15,5) RS codes are shown. Higher the error correcting capability better will be the performance. Figures 5.a and 5.b show the performance of ECC on text data in the form of BER and NOCA respectively against various SNR values. Similar plot for the bio-signal is shown in figures 6.a and 6.b where, BER and PDIST is plotted as a function of SNR. It is evinced that maximum tolerable noise level is 8dB, beyond which performance is unacceptably poor.

IV. CONCLUSION

A practical method based on the use of ECC for reliable and robust transmission and storage of medical images with concealed patient information is demonstrated. The patient information is coded with ECC to make it less susceptible to noise introduced during transmission or storage. A comparative study of RS code is demonstrated for various levels of S&P noise. It is seen that even though ECC will correct the errors introduced in patient information, there is limit for the error correction. Beyond some level of SNR value, the information is completely lost. Our results are encouraging enough to make investigations on more

powerful ECC techniques, to make the system more reliable and robust worth pursuing. The Convolutional codes, a different class of ECC compared to block codes could as well be used to encode the patient information. This is a future work.

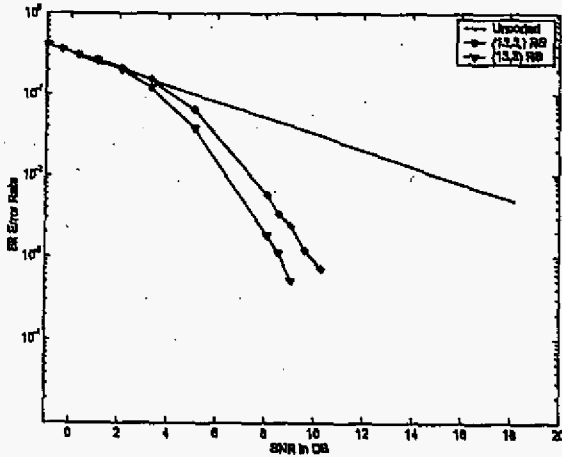


Fig.5a Plot of BER Vs SNR for Text data

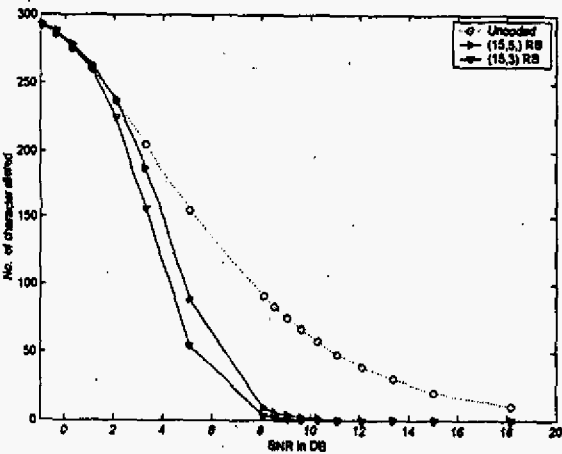


Fig.5a Plot of NOCA Vs. SNR for Text data

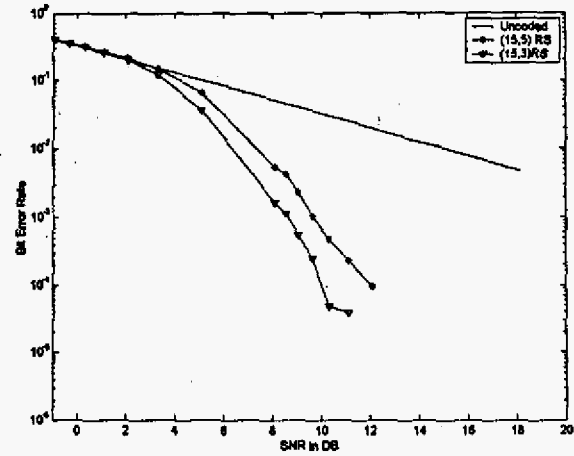


Fig. 6a. Plot of BSE Vs. SNR for Bio-signal graph

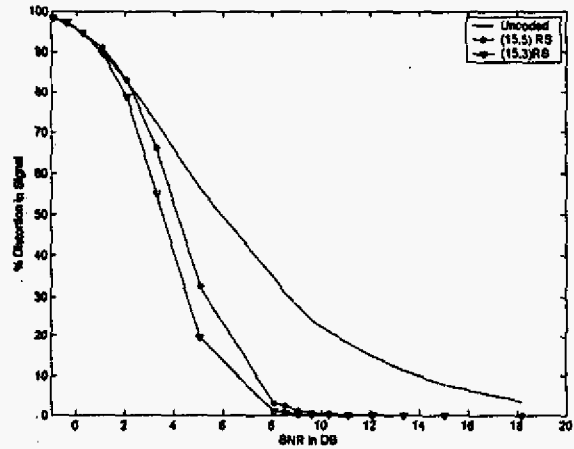


Fig. 6b. Plot of PDIST Vs. SNR for Bio-signal graph

V. REFERENCES

- [1] Hal Berghel, 'Watermarking Cyberspace', Communications of the ACM, Vol. 40., No.11, Nov 1997, pp 19-24.
- [2] Neil F. Johnson, Zoran Duric and Sushil Jajodia, 'Information Hiding: Steganography and Watermarking- Attacks and counterattacks', Kluwer Academic Publishers, 2000.
- [3] Jagadish Nayak, P Subbanna Bhat , Rajendra Acharya U, Niranjan U.C. "Simultaneous storage Of medical images in the spatial and frequency domain : A comparative study. BioMedical Engineering Online, Jun 2004. <http://www.biomedical-engineering-online.com/content/3/1/17>
- [4] Rajendra Acharya U, P Subbanna Bhat, Sathish Kumar, Lim Choo Min, " Transmission and storage of medical images with patient information" Computers in Biology and Medicine 33 (2003) 303-310.
- [5] Rajendra Acharya U, Deepthi Anand, P.Subbanna Bhat and Niranjan U.C., 'Compact Storage of Medical Images with Patient Information', IEEE transactions on Information Technology in Biomedicine, December 2001, vol.5, No.4, pp. 320-323.
- [6] Daemen and V. Rijmen, "AES Proposal Rijndael", version 2, 1999, <http://cistseer.nj.nec.com/daemen98aes.html>.
- [7] Simon Haykins, Communication systems , Wiley Eastern, 1996
- [8] Shu Lin, Daniel J. Costello, 'Error Control Coding Fundamentals and Applications ', Prentice Hall, 1983.
- [9] Anil K Jain , " Fundamentals of Digital Image Processing " PHI 20