EPR Hiding in Medical Images with CDCS and Energy Thresholding

Rajesh Barapate   Dr. Suresh Mali   Dr. Dinesh Yadav

***Abstract*— Confidentiality of patient's data is important in telemedicine applications, which involves transferring of medical images along with the corresponding Electronic Patient's Report (EPR) data in inter or intra hospital network for diagnosis. Embedding EPR in medical images has advantages like less memory requirement, removal of mapping between images and corresponding EPR data. However, as the size of EPR increases, security and robustness of the embedded information becomes major issue to monitor. This paper proposes high capacity, robust blind data hiding technique in Discrete Cosine Transform (DCT) domain. A new coding technique called Class Dependent Coding Scheme (CDCS) is used to increase the embedding capacity. High imperceptibility is achieved by selecting efficient DCT blocks for embedding. Experimental results show that the proposed scheme exhibits high imperceptibility as well as low perceptual variations in Stego-images. The embedding scheme also takes care of sensitive part of the medical image responsible for accurate diagnosis called Region of Interest (ROI). Security and robustness have been tested against various image manipulation attacks**

***Index Terms*— EPR, Medical-image, Steganography, Stego-image, CDCS, DCT, ROI, Compression, Tampering, Resizing, Attacks**

Introduction

Medical image sharing along with corresponding confidential *EPR* data through a computer network is essential in telemedicine. Three important goals while sharing medical images and *EPR* in telemedicine [1] are to safeguard the confidentiality of *EPR* data; to save as much space as possible, to reduce the cost of storage and increase the speed of transmission; and to protect the diagnostically sensitive area (*ROI*) from being embedded. Traditionally, doctors keep two separate data bases (image and text) and preserve the mapping between them. Proposed system of embedding *EPR* text in corresponding medical image does not require two separate data bases and the mapping. However, during the process of embedding the requirements to make the system robust and secured for additional increase in *EPR* are:

1. *EPR* text information embedded must be as high as possible without degradation [2] of images.
2. *ROI* [3] of medical image should not be degraded which is responsible for diagnosis [4, 5, 6].
3. Retrieval of *EPR* text information must be robust [7, 8, 9] against various attacks.
4. Minimize the side information [10, 11] to be given.

In blind information hiding the receiver does not have access to the original host image [12, 13]. A new *CDCS* code have been proposed in this paper in which data is embedded in the low and mid frequency *DCT* coefficients [7, 8], however, special mechanism is used to find higher energy image blocks which will give higher degree perceptual quality of medical Stego-image. While performing all the embedding steps at transmitting end the proposed scheme inherently gives multiple levels of security.

I. Proposed System

Figure 1 shows the proposed embedding scheme consisting of text processing phase (*TPP*) and image processing phase (*IPP*). The *EPR* encoded bits are embedded and medical image is reconstructed to give Stego-medical image. At the time of execution of these phases the embedding parameters (r, n, $\hat{w}$, *seed*, *QF*, x_1, y_1, x_2, y_2) are provided as an input to the respective phases which gets reflected in embedding key.

a) CDCS

Proposed system assigns fixed codes in *CDCS* to each character by considering their probability of frequency of occurrences [13]. The *EPR* characters are then categorized in three different non overlapping special classes as *Class-A (most frequently appearing character set), Class-B (Average frequently appearing) and Class-C (Less frequently appearing characters).* Any character in each Class will then be represented by only 4 bits prefixed by class code (1-bit or 2-bit). Therefore, Class Code along with character code can distinguish 48 different characters which are sufficient to represent any *EPR* data. The proposed *CDCS* combines the advantages of both fixed length and variable length coding to get less number of bits to represent same information which provides ***security levels 1*** as shown in *Figure 2.*

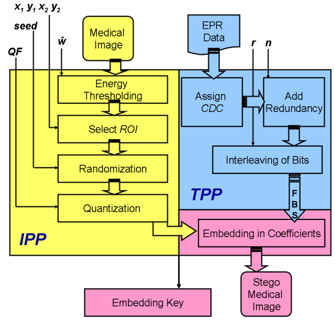


Fig. 1 A Proposed Embedding Scheme: Text Processing and Image Processing Phases with necessary inputs

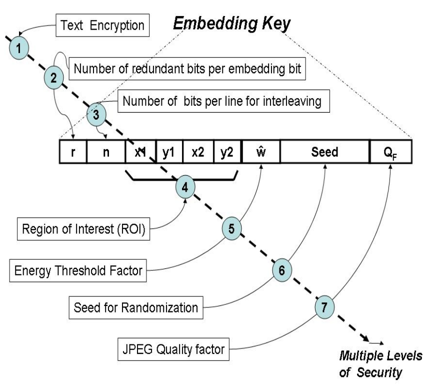


Fig. 2 Embedding Key

If N_1, N_2 and N_3 are the total number of characters belonging to *Class-A*, *Class-B* and *Class-C* respectively, Total number of bits to be embedded is given by,

$$m = (N_1 + 2N_2 + 2N_3) + 4h \qquad (1)$$

where, $h = N_1 + N_2 + N_3$, number of *EPR* characters.

For example, a message "*telemedicine*" needs only of 61 bits with *CDCS* as compared to 84 bits with *ASCII* leading to saving of 23 bits (27.38 % saving). This saving can further be increased with increase in message length and number of *Class-A* characters. Percentage Bit Saving (PBS) is given by,

$$PBS = \left[1 - \left(\frac{m}{7h}\right)\right] \times 100\ \% \qquad (2)$$

Robustness against various attacks such as image compression, resizing and tampering can be achieved by adding redundancy for each bit prior to embedding [7, 8]. The bits are then read as a *Final Bit Stream* (*FBS*) in a particular way called *interleaving* of bits. This *interleaving* of bits will disperse subsequent bits from each other throughout the image. The number of redundancy to be added and number of interleaved bits has to be specified (input) as the embedding parameters. *CDCS* along with specified number of redundancy bits added (***r***) and number of interleaving bits (***n***) provides two ***security levels 2* and *security levels 3*** as shown in **Figure 2.**

The specified *ROI* indices are also becoming the embedding parameters and gives ***security level 4***.

b) **Energy Thresholding**

The blocks having energy greater than the threshold energy will only be considered for embedding. Energy threshold (E_t) is calculated as,

$$E_t = \hat{w} \cdot MVE \qquad (3)$$

where, ŵ = Energy threshold factor which gives ***security level 5*** and *MVE* = Mean Value of Energy given by,

$$MVE = \frac{1}{z}\sum_{k=1}^{z} E_k \qquad (4)$$

where, z = Number of 8 x 8 non-overlapping blocks of the image and E_k = Energy of k^{th} block which is given by,

$$E_k = \sum_{i=1}^{7}\sum_{j=1}^{7} \left\| C_{ij} \right\|^2 \qquad (5)$$

where C_{ij} = Two dimensional *DCT* coefficients.

DC-coefficient ($i = j = 0$) is neither used for calculation of energy nor for embedding as it degrades the quality of entire block heavily. The blocks having more energy can embed information bits with minimal distortion [7]. Therefore, block having energy more than E_t will only be considered for embedding and treated as *Valid Blocks* (*VBs*).

Security level 6 is achieved by randomly selecting the *VBs* and Quantization gives robustness against natural *JPEG* compression attacks. The given *QF* is also acting as another embedding parameter and gives ***security level 7***.

The embedding is carried out by suitably modifying the DCT coefficients of the blocks finally selected after the process of quantization. According to logical value of a bit to be embedded the rounded value of DCT coefficient gets modulated. If the bit is logically 'zero', the coefficient is rounded to 'even' number, otherwise to 'odd' number.

The final stage of the embedding process is the reconstruction of a Stego-image. The experimentation shows that after embedding the *EPR* bits of information, the Stego-images gives *PSNR* value more than 40dB.

II. Experimental Results

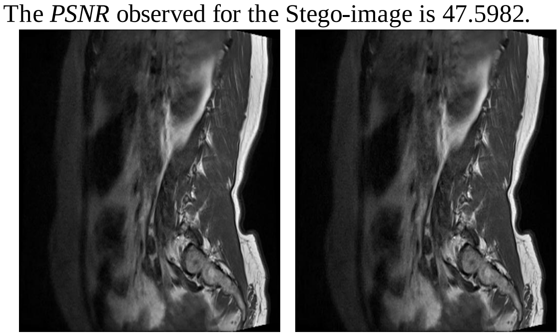
The images used for the experiments are standard greyscale radiological medical image files (*BMP and JPEG*). Various sets of experimentation are carried out to see the effect of *CDCS*, *r*, *n*, *ŵ*, *seed*, *QF*, x_1, y_1, x_2, y_2 on *PSNR*. Along with *PSNR* the Stego-images are also tested for various statistical properties such as *Average Absolute Difference (AAD), Histogram Similarity (HS), Normalized Cross Correlation (NCC) and Correlation Quality (CQ)*. Robustness of the scheme under various attacks such as Stego-image compression, resizing and image tampering is also tested.

Table 1 shows comparison of *CDCS* and *ASCII* codes for various number of *EPR* characters. The average *PBS* for all the 114 different medical images tested with the proposed system while embedding up to 500 EPR characters is more than 20 with respect to fixed *DCT ASCII* mechanism as shown in **Table 1**.

Table (I) CDCS Result

***EPR* characters**	***Number of bits to represent EPR***		
	ASCII With fixed DCT method	***CDCS with proposed IPP***	***PBS (%)***
078	0546	0428	21.61
253	1771	1407	20.55
506	3542	2814	20.55
584	4088	3244	20.65

Figure 3(a) and **Figure 3(b)** shows 512 x 512 '*L-Spine*' original (Cover) image and Stego-image respectively. While embedding 270 *EPR* characters with '*QF* =70', 'ŵ =0.5'. The *PSNR* observed for the Stego-image is 47.5982.



(a) **(b)**

Fig. 3

Table (II) PSNR Variations

Medical Image under test	*PSNR* (*dB*)	
	with *ASCII &* Fixed *DCT* coefficient method	with *proposed TPP and IPP*
L-Spine (m1)	42.20	42.96
MRI head (m2)	34.01	35.54
Abdomen (m3)	36.01	37.24
Shoulder (m4)	43.74	44.96

Four different types of images '*L-Spine (m1)*', '*MRI head (m2)*', '*Abdomen (m3)*' and '*Shoulder (m4)*' are observed after embedding *EPR*. The resultant Stego-images are observed for two methods – first without adopting energy thresholding mechanism with *ASCII* and second with proposed *IPP* and *TPP*. *PSNR* of the resultant Stego-images are as shown in **Table** *II*.

Quality metrics used in visual information processing belong to the group of difference distortion measures [16] are *AAD*, *HS*, *NCC* and *CQ*. The histogram variations for '*L-Spine*' image using *ASCII* without energy thresholding (E-1) and proposed *CDCS* with energy thresholding scheme (E-2) is as shown **Figure 4**. It is observed the histogram variations are very low in case of proposed system. **Table** *III* shows improvement in all pixel based quality metrics with proposed *CDCS* and energy thresholding.

Table (III) Pixel Based Metrics

Measure	**E-1**	**E-2**
AAD	0.9436	0.5912
PSNR	43.90	47.60
HS	11658	6532
NCC	0.9993	1.0000
CQ	26831	26852

Energy threshold factor (ŵ) plays an important role in deciding *PSNR* of a Stego-image. Figure 5 shows variation in *PSNR* with respect ŵ for various values of *QF*.

As given value *QF* increases, the capacity of embedded EPR information also increases. However, robustness against JPEG attack reduces with *QF*. Addition of redundancy in *EPR* text information before embedding into images is necessary to increase robustness of information at the receiving end. **Table** *IV* shows the results of *JPEG* compression attack with added redundancy for '*L-Spine'* image with 'ŵ =0.5'.

Table (IV) Performance Under JPEG Compression Attack

Q F	**With r=1**		**With r=3**	
	Comp. Attack (bpp)	**No of bits embedded**	**Comp. Attack (bpp)**	**No of bits embedded**
25	0.5	91	0.42	32
50	0.72	143	0.61	46
75	1.3	187	1.15	63

TABLE (V) PERFORMANCE UNDER RESIZING ATTACK

Resizing	**Bits embedded**	**'r'**
10 %	476	1/3
15 %	476	1/3
20 %	476	1/3
25%	275	1/5

Various interpolation methods are used for '*L-Spine'* image resizing. The most popular ones are bilinear, bicubic and nearest neighbour interpolations. **Table** *V* shows the results of resizing attack using Bicubic method. Table VI shows resizing attack using nearest Neighbor and Bilinear Interpolation. It can be seen from **Table** *V* and **Table** *VI* that increase in percentage of resizing needs more redundancy for faithful reproduction at the cost of payload.

Table (VI) Performance Under Resizing Attack

Percentage Resizing	**Nearest Neighbour interpolation**	**Bilinear Interpolation**

	Number of Bits	**'r'**	**Number of Bits**	**'r'**
2 %	2840	1/5	1544	1/9
5 %	2840	1/5	1158	1/12
10 %	2008	1/7	1158	1/12

In spite of malicious tampering of the 'L-Spine' image all the embedded bits were recovered successfully after the attack. **Table** *VII* shows that increase in percentage of tampering needs increases in the redundancy for faithful reproduction *EPR* information.

Table (VII) Performance Under Tampering Attack

Image Tampering (%)	**Number of bits Recovered**	**'r'**
10	413	1/3
20	256	1/5
30	256	1/5
50	147	1/9

III. CONCLUSION

Proposed *CDCS* can be used as effective coding scheme for *EPR* data hiding in medical images which increases the embedding capacity and provides better perceptual quality of Stego-image. Energy thresholding and JPEG quantization reduces the possibility of loss of information drastically. Effective use of redundancy and interleaving enhances the robustness of the scheme against various attacks like *JPEG* compression, image tampering and image manipulation. Six layered security achieved due to redundancy, interleaving, energy thresholding, randomization, *ROI* and quantization makes the proposed system most secured. Thus the proposed system can effectively be used for high volume of *EPR* data hiding in medical images with higher values of robustness and security.

REFERENCES

[1] G. Alvarez1, S. Li, and L. Hernandez, *Analysis of security problems in a medical image encryption system*, Computers in Biology and Medicine, Vol. 37, pp. 424–427, 2007.

[2] M. Fallahpour and M. Sedaaghi, *High capacity lossless data hiding based on histogram modification*, IEICE Electron. Express, Vol. 4, pp. 205–210, 2007.

[3] J. Zain, and M. Clarke, *Security in Telemedicine: Issues in Watermarking Medical Images*, 3rd International Conference : Science of Electronic, Technologies of Information and Telecommunications, 2005.

[4] B. Planitz and A. Maeder, *Medical Image Watermarking: A Study on Image Degradation*, Proc. Australian Pattern Recognition Society Workshop on Digital Image Computing, WDIC, Brisbane, Australia, 2005.

[5] S. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, *Multiple Image Watermarking Applied to Health Information Management*, IEEE Trans. on IT in Biomedicine, Vol. 10, pp. 722 – 732, 2006.

[6] K. Navas, S. Thampy, and M. Sasikumar, *EPR Hiding in medical images for telemedicine*, Biomedical Sciences Vol. 3, pp. 44– 47, 2008

[7] K. Solanki, N. Jacobsen, U. Madhow, B. Manjunath, and S. Chandrashekhar, *Robust Image-Adaptive Data hiding using Erasure and Error Correction*, IEEE Transactions on image processing, Vol. 3, pp. 1627–1639, 2004.

[8] S. Mali and R. Jalnekar, *Imperceptible and Robust Data Hiding using Steganography Against Image Manipulation*, International Journal of Emerging Technologies and Applications in Engineering, Technology and Sciences, (IJ-ETA-ETS), pp. 84–91, 2008.

[9] G. Simmons, *The prisoners' problem and the subliminal channel, in Advances in Cryptology*, Proceedings of Crypto 83 (D. Chaum, ed.), Plenum Press, pp. 51–67., 1984.

[10] N. Johnson and S. Jajodia, *Exploring Steganography. Seeing the Unseen*, IEEE Computer, Vol. 31, pp. 26-34, 1998.

[11] M. Wu, *Joint Security and Robustness Enhancement for Quantization Embedding*, IEEE Transactions 0-7803-7750-8/03, pp. 483-486, 2003.

[12] J. Zollner, H. Federrath, H. Klimant, A. P¯tzman, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, *Modeling the security of Steganographic systems*, 2nd Information Hiding Workshop, pp. 345-355, 1998.

H. Munch, U. Engelmann, A. Schroter, H.P. Meinzer, *The Integration of Medical Images with the Electronic Patient Record and their Web- Based Distribution*, Academic Radiology, Vol. 11.6, pp. 661-668, 2004.

[13] C. Cachin, *An information-theoretic model for Steganography*, Information and Computation Journal, Vol. 192, pp. 41-56, 2004.

[14] H. Stern, *Compression Techniques for Mobile Data Terminal Communication*, IEEE Transaction, pp 429-432, 1991.

M. Kutter and F. Petitcolas, *A fair benchmark for image watermarking systems*, Electronic Imaging . Security and Watermarking of Multimedia Contents, Vol. 3657, Sans Jose, CA, USA, 25, 1999.

AUTHOR'S PROFILE

Mr. Rajesh Barapate has completed his Masters in Electronics and Telecommunication from Reginal Engineering College, Jaipur. Presently he is pursuing his Ph. D. from J. J. T. U., Rajsthan. He is author of 15 Engineering books. His areas mainly include Image Processing, Information Hiding and Security.

Dr. Suresh Mali has completed his PhD from Bharati Vidyapeeth Pune, presently he is working as Principal in Sinhgad Institute of Technology & Science, Narhe, Pune. He is author of 4 books and having more than 34 international and national publications. He is also working as BOS member for Computer Engineering at University of Pune. His areas mainly include Image Processing, Information Hiding and Security.

Dr. Dinesh Yadav has completed his PhD from Bharati Vidyapeeth Pune, presently he is working as B. S. C. O. E.,Wagholi, Pune. He is having more than 25 international and national publications in the field of Image Processing. His areas of Research is mainly include Image Processing.