Medical Image Authentication using DWT

Kulkarni Pratibha C.[1], **Bhatia S. K.**[2]

Department of Electronics& Telecommunication, JSPM"s Imperial College of Engineering & Research
Wagholi, Pune, India

Assistant Professor, Department of Electronics& Telecommunication, JSPM"s Imperial College of Engineering & Research
Wagholi, Pune, India

Abstract: ***Integrity and confidentiality of medical data is a serious issue for legal and ethical reasons because medical information are easily available in open networks due to the developments like Radiology information systems (RIS), hospital information systems (HIS), picture archiving and Communication Systems (PACS) which helps to store, access and distribute the medical data. So that integrity and authentication of medical images and data is necessary. To achieve this aim Steganography is best solution. This paper proposes "image steganography" as a means to hide this medical data inside the image without losing it. This paper focused on the medical data hiding for security and authentication of medical images. In the proposed algorithm Class Dependent Coding Scheme is used to achieve maximum capacity of medical data. This scheme is depend on the probability of the occurrence of character in the medical data. In this technique characters are divided into three classes according to the probability of occurrence. Medical image segmentation is done to protect diagnostically important part called region of interest (ROI). Text embedding is done in the rest part of an image called region of non interest (RONI). Also medical data can be embedded with LSB technique in medical image which is processed with discrete cosine transform.***

Keywords: CDCS, data hiding, medical image, ROI

1. Introduction

In recent year all the business applications are moving towards the digital era, because of great development in latest technologies such as in the area of communication, networked multimedia system, digital data storage etc. Also from the last two decades use of internet is rapidly increased towards achievement of security, effectiveness, and convenience by introducing the digitization in the business environment.

Nowadays Telemedicine application provides new ways to store, access and distribute medical data. It requires transferring the medical data along with its images over open area (network) for further diagnostic purpose.

When we share medical images along with its data in telemedicine [1], there must be protect the medical images and data. By saving the storage space cost gets reduced & speed of transmission gets increased. This can be achieved by effective embedding of medical data in corresponding medical image. In this paper medical data hiding capacity increases without affecting the medical image [2, 7].

Hiding of data is nothing but a steganography. It comes from Greek words „steganos" and „graphia", which means "covered writing". There are different methods to classify steganographic schemes, these schemes can be categorized according to the type of the covers used for the secret communication.

The two popular types are spatial domain and transform domain embedding. Example of spatial domain techniques is the Least Significant Bit (LSB) substitution. It is simple to implement & offers high data hiding capacity, and controls stego-image quality. The LSB is the direct substitution of unused or noisy LSBs bits of the cover image.

Medical images hold decisive property and are very crucial and important part of medical information which consist diagnostically important details. This part of the medical image is called as Region of Interest (ROI). The ROI is helpful in providing further diagnosis by the physician. A small bit of distortion in ROI may lead to undesirable treatment for patient. For securing medical images through text embedding, ROI should be preserved and the embedding can be applied on the remaining part of the image called as Region of Non Interest (RONI). Therefore, application of watermarking in medical images can be considered as two-step process which includes-extracting ROI form the medical images & applying watermarking on RONI [3].

The transform domain technique overcomes the robustness and imperceptibility problems found in the LSB substitution technique. The transform domains techniques are discrete cosine transform (DCT), the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). In the proposed algorithm DWT is used. In this paper a new CDCS coding scheme has been introduced. This will reduce the number of bits to represent medical data & thus increases the quality of the image [3].

2. Proposed System

Authenticate medical image algorithm consist two parts, first is image and data processing and second is embedding and extraction. The method uses following step such as acquisition of image and data, preprocessing, CDCS, ROI, segmentation, DWT, embedding, extraction.

Figure 2 Illustrates complete flow of proposed system.

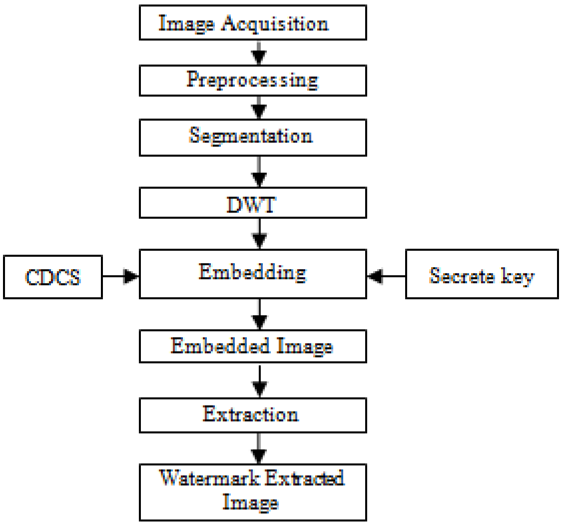

Figure 2: Block diagram of the proposed System

A. Data and Image Acquisition

Medical database is collected from different hospitals such as Eye, Dental clinic as well as from websites. Retinal images are captured from FF450 Zeiss Fundus Camera. Fundus Camera works on Optical Principal. Camera specifications Focus=7.5, field of view = 30º, Image plane size of a 1/2 CCD camera 4.8 × 6.4 mm, Resolution of retina structures smaller than 20 micrometer.

B. Preprocessing

Medical data means patients report which consists characters are converted into 6 bit binary code by using class dependent coding scheme. Images are converted into gray scale images and resizes to 512X512. Histogram equalization is applied to the grayscale image. Equations are as below:

$$S_k = T(r) \quad (1)$$

where S and r are variables denoting the intensity level of input image and processed image at any point.

And T(r) is transformation.

$$Histeq = S_k * L - 1 \quad (2)$$

where L is no of samples

C. Redundancy & Interleaving

To increase the robustness of the system for image tampering attack, redundancy and interleaving of embedded bits will be added. These bits get repeated with the Redundancy and interleaving helps to scatter these bits all over the stego image.

D. Segmentation

To select region of interest which is a important part as per diagnosis is specified by diagonal indices X1, Y1 and X2, Y2. The Valid Blocks which comes in the ROI will not be taken for the embedding. Then VBs are quantized and after the process of quantization the non-zero predefined DWT coefficients are considered for embedding the data.

E. Embedding and Extraction

If the embedded bit is logically „zero", then DCT coefficient is rounded to „even" number, else it is rounded to „odd" number. To reconstruct the embedded-image, apply inverse DWT and combining all 8 x 8 image blocks. Extract embedded data and calculate bit error rate (BER).

3. Methodology

a) Class Dependent Coding Scheme

According to the probability of the occurrence, shown in figure 4, characters are divided into 3 classes [3] as Class-A (most frequently appearing character set), Class-B (Average frequently appearing) and Class-C (Less frequently appearing characters). For class A – code is 00, Class B is 01 and for Class C is 10.

Table 1: Class Code within Each Class

Class A	Class B	Class C	4-Bit Code
Blank	M	0	0000
.	U	1	0001
E	G	2	0010
T	Y	3	0011
A	P	4	0100
O	W	5	0101
N	B	6	0110
R	V	7	0111
I	K	8	1000
S	X	9	1001
H	J	(	1010
D	Q	)	1011
L	Z	=	1100
F	,	*	1101
C	-	%	1110
:	_	+	1111

If N1, N2 and N3 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,

$$m = (2N1 + 2N2 + 2N3) + 4h \quad (3)$$

Where, $h = N_1 + N_2 + N_3$ i.e. total number of characters

Percentage Bit Saving (PBS) is given by,

$$PBS = [1 - (m \div 7h)] \times 100\% \quad (4)$$

b) Analysis of Robustness

To ensure the reliability and quality of the watermarked image, the performance of watermarking is calculated, which measured in terms of perceptibility. There are two method of calculating the performance measure_ Mean Square Error (MSE) is simplest function to measure the perceptual distance between watermarked and original image.

$$MSE = 1 \div n \sum_{i}^{n} (I' - I)^2 \quad (5)$$

Where, I is original image and I is watermarked image.
Peak Signal to Noise Ratio (PSNR) is used to measure the similarity between images before and after watermarking.

$$PSNR = 10 \log_{10} \max I^2 \div MSE \quad (6)$$

Where, max I is the peak value of original image.

4. Result

Following figures shows experimental results of different step by using MATLAB. Table 2 and 3 gives Medical images are Figure (a) shows the original retinal image for diagnosis purpose.

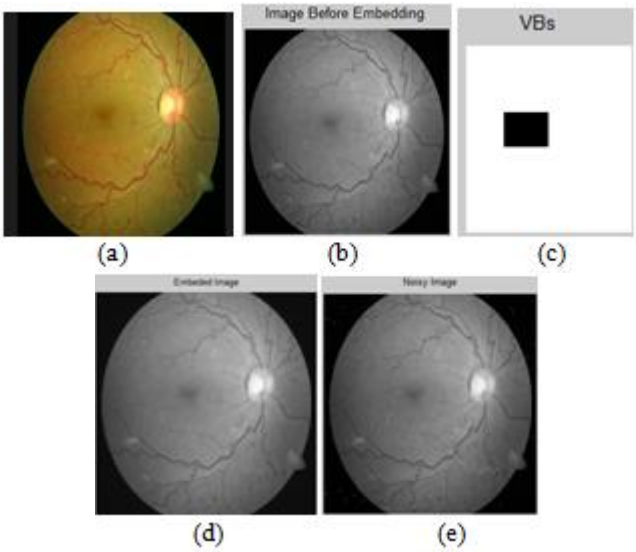

Figure 3: a) Original Image b)Grayscale Image c)Valid Block‟s d) stego Image e) Noise attack image

Table 2 illustrates capacity performance of CDCS over ASCII. Maximum number of data can be hide into an image without harming it. We can save more than 25% characters as compared to ASCII. For experimental result 50 retinal test images used, out of 50, five are listed below.

Table 2: Capacity performance of CDCS over ASCII

Image	Characters in Medical Data	ASCII bits	CDCS bits	PBS (%)
1	690	5520	4140	26.2821
2	588	4704	3528	29.3251
3	660	5280	3960	25
4	732	5856	4392	25
5	732	5856	4392	25

Table 3 shows result analysis with redundancy bit (R), interleaving bit (I), bit error rate (BER), PSNR of stego image and PSNR after attack. As the number of character increases with the increasing in redundancy and interleaving bit error rate less than 5%. PSNR value of stego image and PSNR after attack is greater than 50 dB. Due to redundancy and interleaving bits system gets more robust against tempering attack.

Table 3: Analysis of Retinal Images

Image	No. of chara.	R	I	BER	PSNR	PSNR After attack
1	690	2	2	4.637	52.5497	51.4312
2	588	2	2	4.591	52.8978	51.8162
3	660	3	3	6.969	52.0792	51.0409
4	732	4	3	4.644	51.5528	50.6838
5	732	4	4	5.191	51.1940	50.2984

Table 4 shows PSNR of Retinal image after different attacks are applied on it. With the various capacity of data is embedded and different attacks such as salt and paper, Gaussian, speckle, poisson etc. PSNR value of stego image and PSNR after attack is greater than 40 dB for salt and paper and poisson noise attack. For Gaussian & speckle noise attack PSNR is greater than 37 dB.

Table 4: PSNR of Retinal Images after attacks

Data in bits	588	660	690	732	732
Without attack psnr	50.9293	50.7607	50.3791	50.1478	49.679
Salt & paper	49.1276	48.9974	48.805	48.573	48.2613
Gaussian	39.25	39.238	39.2444	39.2266	39.2206
speckle	37.1538	37.149	37.141	37.1514	37.1393
Poisson	40.6653	40.6559	40.639	40.6537	40.6113

5. Conclusion

It is possible to transfer medical data over network with security. Hiding capacity is increases with CDCS instead of ASCII, DWT provides better quality of Stego-image. An image is segmented as ROI & RONI regions, redundancy and interleaving bits system gets more robust against various attacks.

6. Acknowledgment

We wish to express our warm thanks to Prof. A. D. Badadapure, HOD of Electronics & telecommunication Department, ICOER, Pune for his support. Also we would like to thank to Dr. Adamane, Principal, ICOER, Pune for his support.

References

[1] Gonzalo Alvarez1, Shujun Li and Luis Hernandez,"Analysis of security problems in a medical image encryption system," *Computers in Biology and Medicine*, vol. 37 (2007) 424–427.

[2] M. Fallahpour and M. H. Sedaaghi, "High capacity lossless data hiding based on histogram modification", *IEICE Electron. Express*, Vol. 4, No. 7 (2007) 205–210.

[3] S. N. Mali and R. M. 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)(2008)84–91.

[4] C. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469-474, Mar. 2004.

[5] G. S. Pavlopoulos, D.Koutsouris, "Multiple image watermarking applied to health information management", *IEEE Transactions on Information Technology in Biomedicine*, vol. 10.4 (2006) 722 – 732

[6] K. A. Navas, S. A. Thampy, and M. Sasikumar, "EPR hiding in medical images for telemedicine," *International Journal of Biomedical Sciences* Volume 3.1 (2008) 44– 47

[7] K. Solanki, N. Jacobsen, U. Madhow, B.S.Manjunath and S. Chandrashekhar, "Robust image-adaptive data hiding using erasure and error correction," *IEEE Transactions on image processing*, Volume 13,(2004)1627–1639.

[8] R.O. El Safy, H.H. Zayed and A. El Dessouki,"“An adptive stegnographic technique based on integer

wavelet transform",IEEE,Volume 978-1-4244-3778-8/09,2009.

[9] H. W. Tseng and C. C. Chnag, "High capacity data hiding in jpegcompressed images," Informatica, vol. 15, no. I, pp. 127-142, 2004.