RESEARCH ARTICLE OPEN ACCESS

Data Hiding In Medical Images by Preserving Integrity of ROI Using Semi-Reversible Watermarking Technique

Arshpreet Kaur*, Harvinder Singh Josan**
*(Reseach Scholar, Department of Electronics and Communication, RIMT-IET, Mandi Gobindgarh, Punjab)
**(Assistant Professor, Department of Electronics and Communication, RIMT-IET, Mandi Gobindgarh, Punjab)

ABSTRACT
Text fusion in images is an important technology for image processing. We have lots of important information related to the patient's reports and need lots of space to store and the proper position and name which relates that image with that data. In our work we are going to find out the ROI (region of interest) for the particular image and will fuse the related document in the NROI (non-region of interest) of the image, till yet we have many techniques to fuse text data in the medical images one of form them is to fuse data at the boarders of the images and build the particular and pre-defined boarder space. We have propose an algorithm in which we first find out the area of interest and after that we find noisy pixels of the image to embed data in that noisy portions of the image. We use wavelets for smoothing images and segmentation process for extracting region of interest. Coordinates of the noisy pixels have been located and data has been embedded in those pixels .The used embedding technique embed data in least significant bits, hence does not degrade the quality of the image to unacceptable limits. Results show that it gives good PSNR and MSE values which are used for measuring quality effected performance.

***Keywords* -** Data embedding, Data extraction, US/MRI images.

I. INTRODUCTION

Medical image knowledge digest consists of patient information like patient name, patient-ID , disease description, procedures with doctors information [3]. Medical image knowledge digest will be the watermark. This watermark is embedded into the image which has to be shared by using lossless watermarking technique. The data hiding scheme should have a large embedding capacity to carry more general information. The goals of this work are to protect the copyrights and can recover the embedded data. The scheme provided here for data embedding provides robustness, imperceptibility, high embedding capacity and readily retrieving capacity. Medical images can be given to the patient directly or send to the patient by online and also maintained as a soft and hard copy at the hospital for diagnosing and later in the future purposes. The problem arises here that is while sending or giving the data to the patient we have to find whether the data belongs to particular patients or not and also the privacy of the patient is a primary concern [1]. Hence authentication is required. If we consider medical images especially ultrasound and MRI, they are a confidential property of the patients or defense personals and need to be authenticated and transmitted without any vulnerable attack called tempering. However it's not possible in this hacking area, so we need to provide some security especially in the region of interest to avoid manipulations which define the defected area of the patient. A number of methods are emerging and watermarking is one of them. Some people take watermarking as steganography but there is a difference between the two. Watermarking is defined as the practice of imperceptibly altering a work to embed a message about that work. On the other hand, steganography is the practice of undetectable altering a work to embed a secret message [2]. Digital image watermarking has gained a great interest in the last twenty years among scholars who provide a number of methods. However, still we are far away from being fully or accurately successful. Therefore, more and more people are entering the field to make the watermarking idea useful and reliable for the digital world. Of these various watermarking methods, some beat others in terms of basic watermarking requirements like robustness, invisibility, processing, cost etc.

The whole system of watermarking comprises of an adder called Embedder, which embeds the mark and a detector as shown in the figure below. The Embedder's output is typically transmitted or recorded. At the detector side, the embedded image is accessed as an input to the detector. If a payload is present, detector detects and extracts the encrypted data and payload. Watermarking, like cryptography, needs secret keys to identify legal owners. The key is used to embed the watermark, and at the same time to extract or detect it. The embedded signal can be exposed only with a right key. While a single bit of information indicating that a given document is watermarked or not is sufficient sometimes, most applications demand extra information to be hidden in the original data. This information may consist of ownership identifiers, transaction dates, serial numbers, etc., that plays a key role when illegal providers are being tracked.

Reversible digital watermarking [4], [9],[10] is the technique that embeds the watermark or secret data into an original image to form a stego-image. Although the stego-image has only slight difference from the original image, in some specific images like medical, Defense, and legislature images, even the little distortion on these images cannot be accepted. For instance, in case of medical images if region of Interest found distorted, it cannot provide the correct information about the affected area of a patient. So in these circumstances, the data hiding algorithm should be able to restore the original image from the stego-image. This is the so-called reversible, lossless data hiding technique. Obviously, many data hiding techniques have been proposed but most of them are not reversible, which means that the original cover image cannot be recovered with lossless from the stego-image.In this Semi reversible technique is used.

In this paper, we propose a ROI-based watermarking scheme which is capable of hiding patient's data and verifying authenticity of ROI, in section 2, we review watermarking techniques proposed for medical images. In section 3, we present our proposed method including data embedding and extraction. In section 4, experimental results are provided to demonstrate the efficiency of the scheme. Finally, in section 5 we present our conclusion.

II. EVOLUTIONARY TECHNIQUES EMPLOYED

A general structure for the proposed work has to include many elements for hiding data in order to authenticate the medical image at various stages of the diagnosis process [5]. In order to achieve image authentication, fragile watermarking techniques with semi reversible are commonly used. Fragile authentication is more functional than the semi-fragile or robust techniques. The digital watermark must be fragile to any kind of distortion. For example, the image after lossy processing such as JPEG could be found to be authentic by robust image authentication, but it would fail fragile image authentication. For fragile, one bit error in the message leads to a totally different authenticator, however, for a “semi- fragile” image authentication, such an error does not necessarily alter the authenticator. Fragile image authentication is highly sensitive and dependent on the exact value of image pixels. Our proposed technique works in fragile environment in which we hide informatory data and authentication message in Non-region of interest of medical images. While hiding data into the image, Region of interest has been separated from NROI by using wavelets and clustering method and later increasing the brightness of the pixels of region of interest location, an embedding algorithm has been applied to hide data. Region of interest has been modified later according to the initial condition

For hiding data,firstly we need Information to be embedded for authentication purposes. For this, two types of data is needed. First to authenticate the images and second is information regarding the patient and its diagnosis report. Secondly there is a need to use a technique to embed data into an image in order to keep ROI integrated. The third main issue is to handle embedding capacity as it can be increased depending upon the diagnosis report. And finally there is a need to consider Security and integrity of the host data and how to decrypt data at receiver end and verify authentication message. There are two processes for our presented work. The first one is embedding process in which data is embedded and the second one is extraction process in which data has been extracted. Both algorithms are explained below:

The embedding process starts with the generation of watermark. Later on the watermark is embedded in NROI.

The process is described step by step as follows:

1) Read Image into MATLAB environment and convert it into gray scale if it is in other scale.
2) Separate REGION OF INTEREST and NON REGION OF INTEREST using wavelets and segmentation techniques.
3) Evaluate Message authentication code from secret message
4) Read Diagnosis report.
5) Generate the watermark by combining data generated in step 3 and 4 and concatenate it in a single line.
6) Generate an array called TABLE in order to put the integer form of Concatenated character string data .
7) Scan the host image for a value which has been chosen one at a time in a sequence from TABLE and match for minimum difference match in non-region of interest.
8) Confirm its location in secret key array, if present look for another location. Otherwise put the values of that row and column number in the secret key array.
9) Update the encrypted image array according to this newly found pixel. And update the secret key.
10) When algorithm run for all the data, watermarked signal image will be produced, if it fails in the middle, try fewer payloads.Since proposed scheme is blind so there is no need of

original image to extract the embedded watermark.

The extraction process has the following steps:

1) Load the Watermarked image in mat lab environment along with the secret key generated at the time of encryption process
2) Extract the pixels by using the secret key in the sequence provided by secret key and put in an array.
3) Decrypt the extracted watermark and MAC by converting back to characters in string form.
4) Compute the MAC code separately fromthe secret message delivered separately and compare the extracted hash to the computed hash. If both are same, received image is authentic, otherwise declare it as unauthentic.
5) Save the decoded data in a txt. File.

III. RESULTS AND DISCUSSIONS

A medical image used can be of any defected organ of a human body depending upon type of diagnosis used. There are many different techniques available in the medical profession to look closely and efficiently at the effected part. Few of them easily available are x-ray, CT scan and MRI scan. Experimental results have been taken out for images from these techniques. . Resulted outputs at various steps of algorithm are described below for a single image which is brain tumour image of a patient.

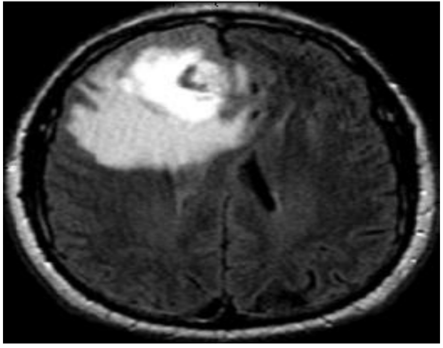

Figure 1 : Test image taken from world wide web.

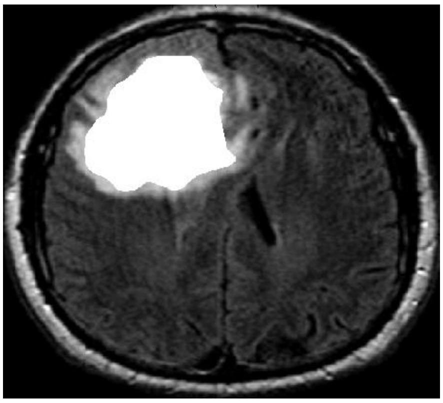

Figure 2: Marking of region of interest.

As we seen above few pixel levels have changed which results in variations b/w histograms of input image and output watermarked image. These changes cannot be seen by visual perception but can be understood from histogram bins and counts of pixels.

Perceptual similarity between the original image and the watermarked image is defined by the fidelity of a watermarking system. The fidelity measure depends on the embedding process and the transmission of the marked signal. The best method to evaluate fidelity of a watermarking system is based on examining both original and watermarked version of the work by human subjects [8], but due to high volume of test sets such an evaluation method is impractical. The most common evaluation method used in all the literature is the peak signal-to-noise ratio (PSNR) defined between the host and watermarked signals. The PSNR (PEAK SIGNAL TO NOISE RATIO) of an image is a typical measure used for evaluating image quality by considering that the few noticeable distortions are uniform in all coefficients in a specific domain, such as spectral domain, frequency domain, or some transform domain. Since PSNR is more computable and can be used to provide a generic bound for the watermarking capacity. So, we use the PSNR to analyze the watermark embedding distortions on images. We need to calculate MEAN SQUARE ERROR (MSE) in order to calculate PSNR.

- MSE measured the level of noise in encrypted image with comparison to original image and can be calculated by formula:

$$\mathrm{MSE}=\sigma_q{}^2=\frac{1}{N}\sum_j \sum_k [f(j,k)-g(j,k)^2 \quad (1)$$

Where i and j is the no. of row and column in the image.

- PSNR is used to test the change in the quality of image after applying various attacks. The mathematical formula is given by:

$$\mathrm{PSNR} = 20 * \log 10 \frac{2^n-1}{MSE} \quad (2)$$

Or

$$\mathrm{PSNR}= 20 * \log 10\ (255 /\mathrm{MSE}) \quad (3)$$

CF measures the similarity and difference between both image. It is given by:

$$\mathrm{C.F.} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} W(i,j) * W'(i,j)}{\sum_{i=1}^{N} \sum_{j=1}^{N} W^2(i,j)} \quad (4)$$

Where N×N is the size of watermark, W (i,j) and W'(i,j) represents the watermark and recovered watermark images respectively.

Tables and figures below describes PSNR and MSE data plots at different payloads.

Table 1: MSE and PSNR values at different payloads for input image

Payload in bytes	MSE	PSNR in dB	Correlation factor
8000	0.0405	62.052	0.9984
9000	0.0889	58.641	0.9998
10000	0.1896	55.351	0.9952
11000	0.3257	53.002	0.9994

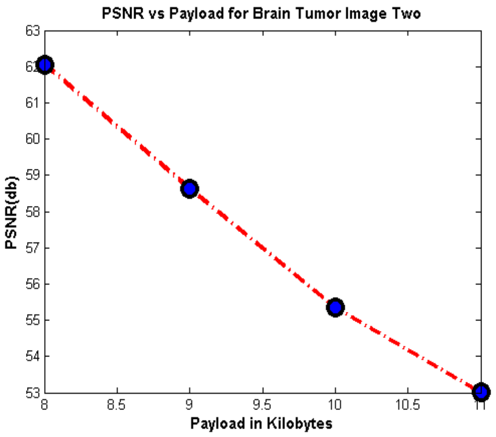

Figure 3 : Data payload vs PSNR plot graph

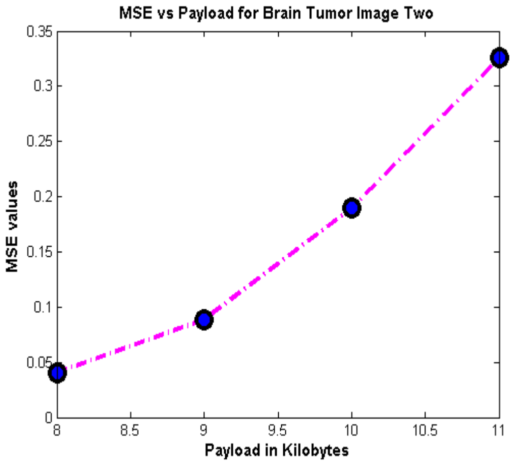

Figure 4: Data payload vs MSE plot graph

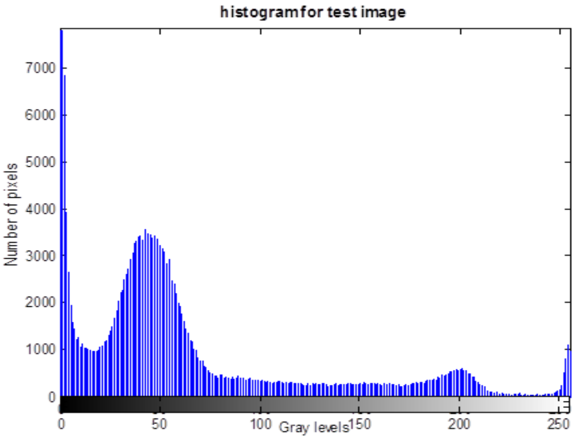

Figure 5: Histogram of input image

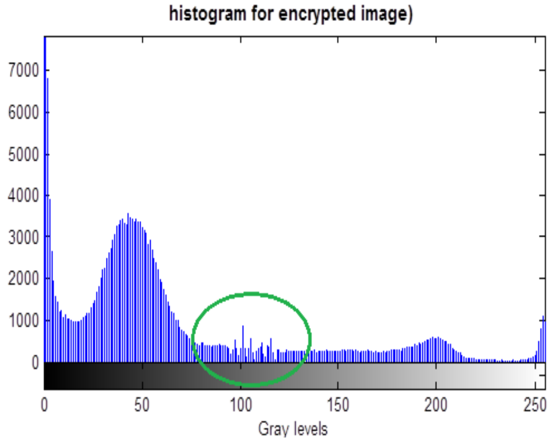

Figure 6: histogram of watermarked image

It is hard to see the difference between original image and encrypted image. But by differencing corresponding pixels of both images we can find out the changes in corresponding locations. As seen from the difference images above we can see the embedded pixels and can easily see that the embedding happens only in non-region of interest. In the histograms above for the encrypted images, an eclipse has been marked around the intensity levels which have been modified.

IV. CONCLUSION

The technique proposed is fragile data hiding technique which preserves the record of medical image by embedding the medical diagnosis report and other data. While embedding the data, ROI of medical image is avoided to ensure the integrity of ROI. This is done by first applying the wavelets in order to enhance spatial information and to reduce noise and then by applying clustering. Hence resulted in separated ROI and NROI .The scheme allows the storing and transmission of electronic patient record along with image authentication codes which can be extracted at the receiving end without the original image. In future work will be carried out to locate the ROI regions for different types of images and algorithm will be modified to increase PSNR values for better quality output.

REFERENCES

[1.] Acharya.U.R., Bhat.P.S., Kumar.S., and Lim.M.C.,” *Transmission and storage of medical images with patient information*”, *Computers in Biology and Medicine Vol 33* ,2003, pages 303–310.

[2.] Li.M., Poovendran.R., and Narayanan.S., “*Protecting patient privacy against unauthorized release of medical images in a group communication situation”, Computerized Medical Imaging and Graphics, Vol 29* ,2005, pages 367–383.

[3.] G. Coatrieux, Clarale, Guillou, J. Cauvin, L. Iocamu and Ch, Roux: "*Enhancing shared medical image fimctionalities with image knowledge digest and watermarking*", presented in the *IEEE EMBC conflnt. Technol.Appl. Biomed*. (IT AB 2006) Joannina, Greece.

[4.] Weng.S., Zhao.Y., Pan.J.S., and Ni.R., “*A novel high capacity reversible watermarking scheme,” IEEE International Conference on Multimedia and Expo (ICME 07)*, vol. 3, 2007, Page(s): 723 – 730 .

[5.] Raul, C.R. and Claudia, U.F, “Data Hiding Scheme for Medical Images” 2007 *IEEE* Page(s): 32-36.

[6.] Huang .A.H.V.C., Fang. B.W.C.and Chen.S.C. “*Privacy Protection and Authentication for Medical Images with Record-Based Watermarking*” ,*2009 IEEE* ,Page(s): 190 – 193.

[7.] Sun.X. and Bo.S., “*A Blind Digital Watermarking for Color Medical Images Based on PCA*” *2010 IEEE* Page(s): 421 – 427 .

[8.] Poonkuntran.S., R.S.Rajesh, “*A Messy Watermarking for Medical Image Authentication*” *2011 IEEE* Page(s): 418 – 422.

[9.] Khoo.B.E and Qershi.O.M, “*ROI-Based Tamper Detection And Recovery For Medical Image Using Reversible Watermarking Technique* “, *IEEE* 2010, Pages- 151-155.

[10.] Sakai.H., Kuribayashi.M., and Morii.M., ”*Adaptive reversible data hiding for JPEG images*”, *Proc. of International Symposium on Information Theory and its Applications, Auckland, New Zealand*, Dec. 7-10, 2008, pages . 870-875.