International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 8 (September 2014) www.ijirae.com

Data Hiding Technique for Secure Transmission of Medical Images

Simranjeet Kau r*
ECE,PTU Jalandhar

Sukhjinder Kaur
ECE, PTU Jalandhar

Birdevinder Singh
Mechanical Engg, PTU Jalandhar

Abstract— ***With sloping emergence of communication and computer networks technologies, exchange of medical images has become a usual practice these days. These images can be modified easily and imperceptibly with malicious intentions. It has been proposed to use digital watermarking technology to hide the patient's data and then retrieve back the same data at the receiving end by using certain secret key. The objective of the watermarking method is to check the integrity and preservation of the confidentiality of the patient data in a network sharing. In the proposed method, we used reversible data hiding technique for authentication and data hiding which selects the NROI for embedding the watermark in order to assure the integrity of ROI. Performance evaluation of this proposed scheme for data hiding is carried out and end comparison is made. Experimental results demonstrate that the watermark embedding is invisible and has a good peak signal-to-noise ratio (PSNR) if the embedding factor is low. Scheme is good at authentication as well as the capacity has been increased up to 13k of payload information***

Keywords— watermarking, authentication, encryption, data hiding, decryption, embedding

I. INTRODUCTION

The Internet has become the most important information provider, and offers many mediums to deliver and to interchange information. Digital images can be easily shared via the Internet and conveniently processed for queries in databases. With some powerful image processing tools, one can modify some features in a picture easily without any detectable trace. These kinds of operations are regarded as tamper. The validity of the image is of most importance such as images for military, medical, and judicative use [1]. The production of ownership and prevention of unauthorized manipulation of digital images are becoming an important issue [2]. So some effective ways are needed to guarantee integrity of the image. 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 tampering. However it's not possible in this hacking era, so we need to provide some security especially to the region of interest to avoid manipulations, which defines the defected area of the patient. A number of methods are emerging and watermarking is one of them.

II. RELATIVE WORK

There are many developed techniques, which work in spatial as well as frequency domains. It's difficult to embed large amounts of data in frequency transform domain as compare to spatial domains.

Vargas et al. [3] proposes a reversible data-hiding algorithm. It provides good capacity by exploiting the interconnection between neighboring pixels. Nagarju et al. [4] proposes a digital watermarking technique, which is a class of fragile reversible watermarking that constitutes and finds an application in authentication of medical and military imagery. Reversible watermarking techniques ensures that after watermark extraction, the original cover image can be recovered from the watermarked image pixel-by-pixel. Umamageswari et al. [5] proposes a reversible watermarking technique to embed information into medical images. Reversible watermarking techniques ensures that after watermark extraction, the original cover image can be recovered from the watermarked image pixel-by-pixel. In this paper Region of interest (ROI) and Region of non interest (RONI) is defined. ROI is protected and effort is made to embed data in RONI. Zain et al. [6,7] proposed an LSB- based scheme for ultrasound images, where the original image can be recovered completely. Tian et al. [8] proposes an important category of high-capacity reversible data-embedding algorithms called the expansion-embedding approaches.

In our work, we proposed a semi-reversible scheme, which is capable of hiding patient's data and verifying authenticity of image, to achieve image authentication, fragile watermarking techniques is used.

III. METHODOLOGY

The sketch of proposed scheme is given in Fig. 1. The embedding process starts with the generation of watermark. So first we describe the procedure for generation of watermark. Later on the watermark is embedded in NROI.

A. Steps to generate watermark

In order to generate the watermark, following steps are implemented:

1. Generate a fixed hexadecimal number message by using a HASH function for a particular message defined by the sender. The combination of all the fixed hexadecimal numbers called Message Authentication Code (MAC) is then put into a file in the sequence according to secret message
2. Read the text file containing the patient information; convert character data into integer values.

3. Now concatenate the data and MAC into a single line array having length say's', such that Table= (i) which is element of [0,1], $1 \leq i \leq t$}.
4. Convert above data into corresponding binary code and form the vector which may have length of M bits such that vector = {w2(i)|w2(i) $\in$[0, 1], $1 \leq i \leq M$ }.

B. Steps for embedding the watermark in NROI

The following steps are used for embedding the watermark in NROI:

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 cropping tool.
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.

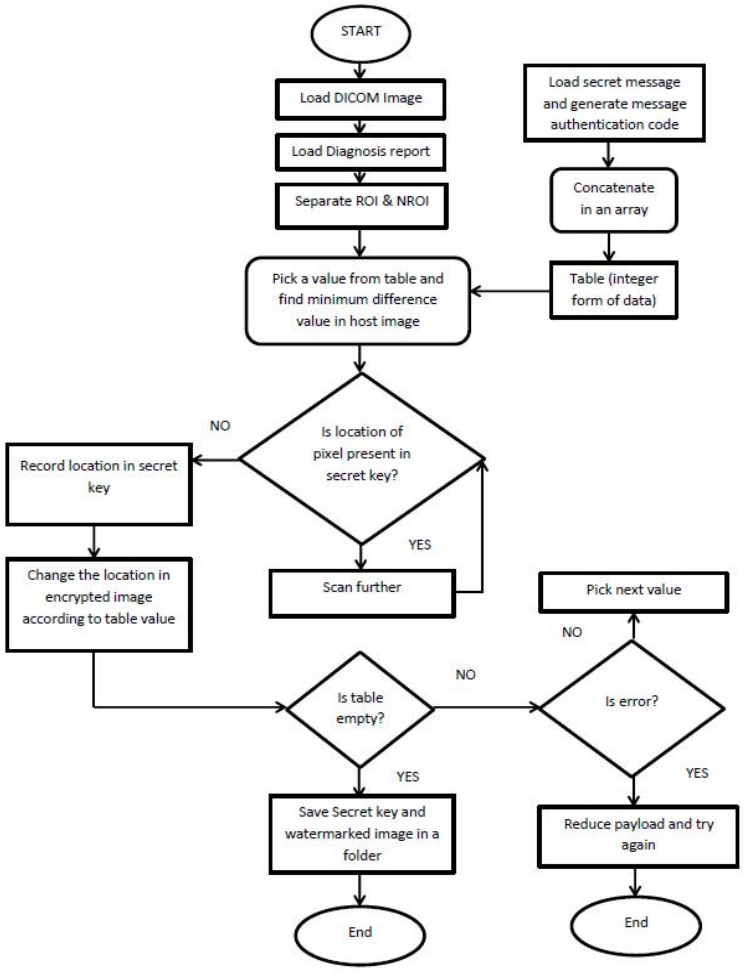

Fig.1 Encryption Algo-flowchart

C. Steps for extraction process

Since proposed scheme is blind so there is no need of original image to extract the embedded watermark. The sketch for decryption of watermarked image is given in Fig. 2.

The extraction process has the following steps:

1. Load the Watermarked image in matlab 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 from the 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. Save the decoded data in a txt. File.

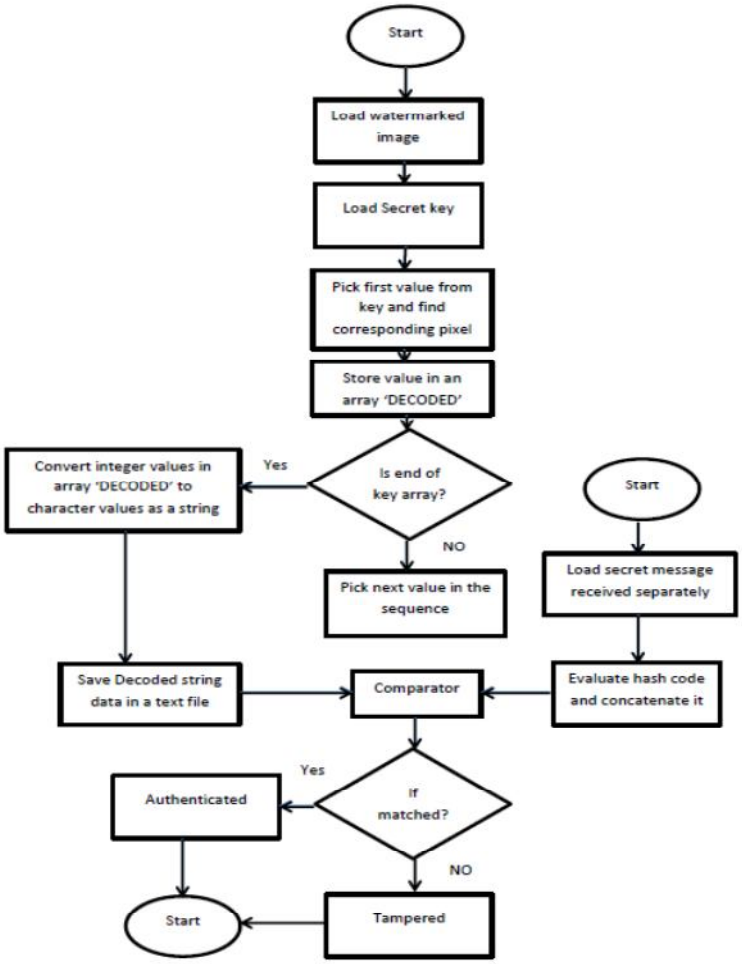

Fig. 2 Decryption Algo-flowchart

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section we show the experimental results of our proposed scheme. To evaluate the performance of the proposed scheme DICOM image of brain of patient were used as shown in Fig. 3. Seperation of ROI (Region of interest) and NROI(Non region of interest) shown in Fig. 4.

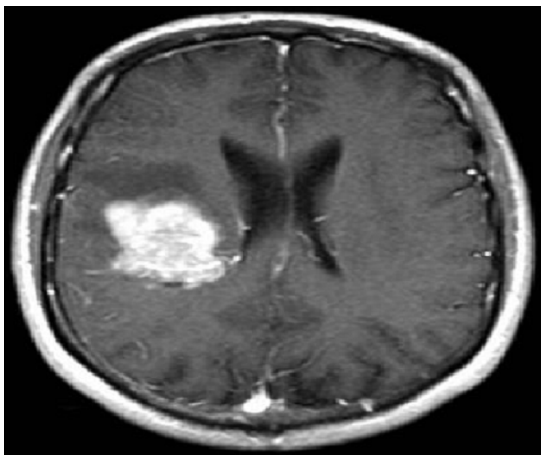

Fig. 3 Brain DICOM Image with effected portion

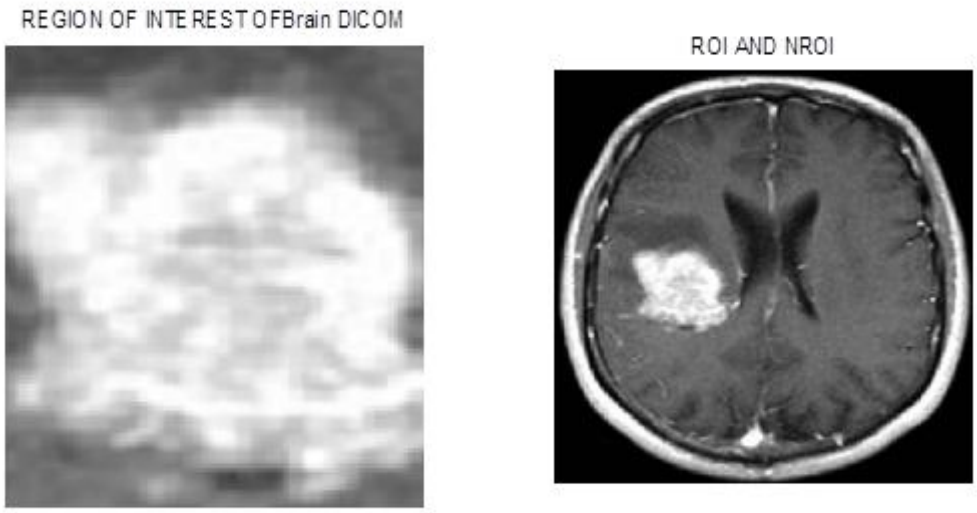

Fig . 4 Separated ROI and NROI of Brain DICOM Image in Matlab

The proposed algorithm can embed up to one byte per pixel. However we are not using all pixels here as we used only the co-ordinates of the matched pixels which results in almost negligible amount of change in perceptual appearance in histograms of encrypted images. We can see this negligible change in histogram of dicom image in the Fig 5.

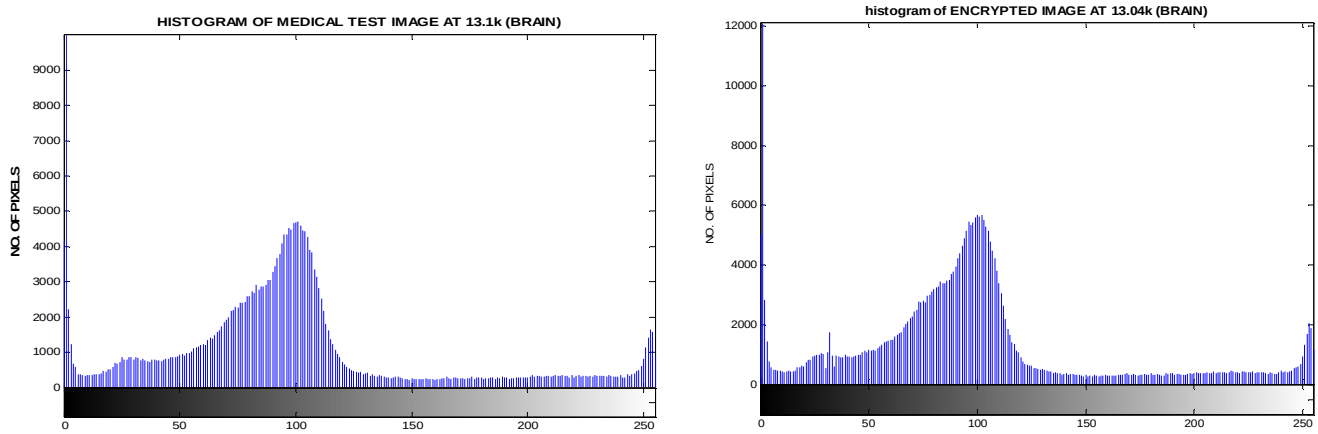

Fig 5. Histogram of original brain image and modified brain image

The proposed technique is tested on the image with different payload and the scaling factor as shown in the table. The watermarked image shows high embedding capacity upto 13K and good visual quality in terms of PSNR.

Table I
X-RAY IMAGE of BRAIN at CONSTANT SCALING FACTOR

Test Image	Payload (bytes)	MSE	PSNR (dB)	Correlation factor	Scaling factor	Elapsed time (sec)
Brain DICOM IMAGE	8k	0.0036	73.1254	1	0%	90.16
	10k	0.0070	70.3795	0.9998	0%	150.16
	12k	0.0097	69.2245	0.9997	0%	265.66
	13k	0.0123	66.9874	0.9996	0%	286.76

Table II
X-RAY IMAGE of BRAIN at CONSTANT PAYLOAD BYTES

Test Image	Payload (bytes)	MSE	PSNR (dB)	Correlation factor	Scaling factor	Elapsed time (sec)
BRAINDICOM IMAGE	13k	0.0158	66.4536	0.9995	-10%	278.03
	13k	0.01222	67.5944	0.9997	0%	279.78
	13k	0.00694	69.4274	0.9998	+10%	298.12
	13k	0.00476	71.2925	0.9999	+20%	307.13
	13k	0.00285	73.5023	1.0000	+30%	308.46

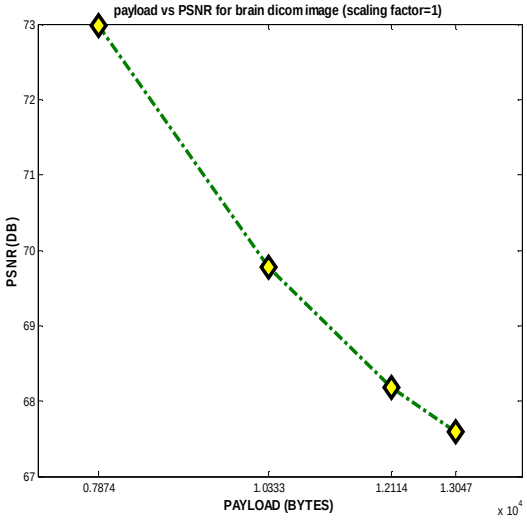

Fig 6. Line graph of Payload v/s PSNR

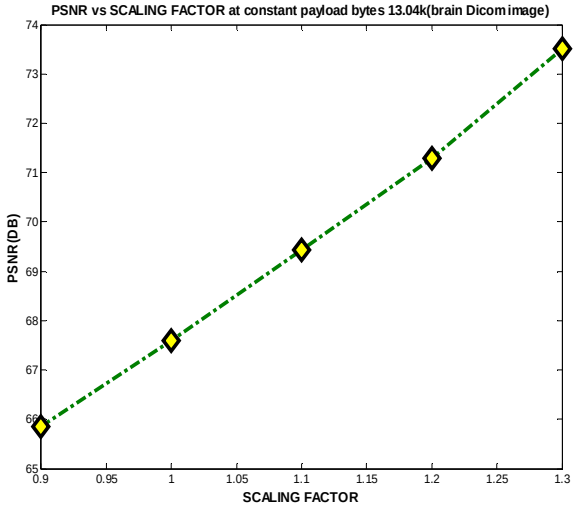

Fig 7. Line graph of Payload V/s Scaling Factor

As we can see from the tables above and the plots between PSNR and Payload, when we increase the payload above 12000 bytes there is change in the correlation factor which decides the mismatching from the original image. Also embedding capacity can be increased of the images by scaling it to higher factors but there is degradation in the required signal due to the degradation in the quality of the image. By increasing the scaling factor we can increase the embedding capacity of informatory data. From the above calculations it is clear that, the proposed scheme achieves the more embedding capacity as compared to the algorithms discussed in literature review. Perceptual similarity between the original image and the watermarked image is defined by the fidelity of a watermarking system. 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. So, we use the PSNR to analyze the watermark embedding distortions on images. In order to calculate Mean Square Error (MSE) in order to calculate PSNR.

The mathematical representation of the PSNR is as follows:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

where the MSE (Mean Squared Error) is:

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

g represents the matrix data of our degraded image in question
m represents the numbers of rows of pixels of the images and **i** represents the index of that row
n represents the number of columns of pixels of the image and **j** represents the index of that column

V. CONCLUSIONS

In experimental results, it has been shown that the watermark embedding is invisible and has a good PSNR if the embedding factor is low. So the quality of the image will not be affected by the watermarking embedding. The watermark embedding is very sensible to any distortion. Since the watermark generation is a flexible scheme that generates a completely different watermark only when the image content is modified. 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.

The scheme allows the storing and transmission of electronic patient record along with image authentication codes, which can be extracted at the receiving while the original image can be recovered perfectly. Scheme is good at authentication as well as the capacity has been increased up to 13k of payload information.

ACKNOWLEDGMENT

I sincerely express innate gratitude to my diligent and significant advisors, family, and friends, who were always the source of inspiration for me and motivated throughout this period of work. The present work would not have been possible without all of them.

REFERENCES

[1] Y. Liu, W. Gao, H.Yao and S. Liu, "*A Texture-based Tamper Detection Scheme by Fragile Watermarking*", Computer Science and Technology Department of Harbin Institute of Technology, 2004 IEEE.

[2] M.E. Yalçin and J. Vanderwalle, "*Fragile Watermarking and Unkeyed Hash Function Implementation for Image Authentication on CNN-UM*", Katholicke Universite it Leuven, Department of Electrical Engineering (ESAT), April 2002.

[3] L. M. Vargas and E. Vera, "*An Implementation of Reversible Watermarking for Still Images*" IEEE volume 11, feb 2013.

[4] Pasunuri Nagarju, Ruchira Naskar and Rajat SubhraChakraborty, "*Improved Histogram Bin Shifting based Reversible Watermarking*", International Conference of Intelligence systems & Signal processing (ISSP).IEEE 2013 .

[5] A.Umamageswari, G.R.Suresh, " *Security in Medical Image Communication with Arnold's Cat map method and Reversible Watermarking*" International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013].

[6] J. M. Zain, L. P. Baldwin, and M. Clarke, *"Reversible watermarking for authentication of DICOM Images,"* Proceedings of the 26th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2004, pp. 3237 - 3240.

[7] J.M. Zain and M. Clarke *"Reversible Region of Non-Interest (RONI) Watermarking for Authentication of DICOM Images,"* International Journal of Computer Science and Network Security, vol. 7, pp. 19-28, 2007.

[8] J. Tian, "*Reversible watermarking using a difference expansion*," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug.2003.

