Text fusion watermarking in Medical image with Semi-reversible for Secure transfer and Authentication

P.Viswanathan*
Assistant Professor, SCS
VIT University
pviswanathan@vit.ac.in

Dr.P.Venkata Krishna**
Associate professor, SCS
VIT University
pvenkatakrishna@vit.ac.in

***Abstract*-Nowadays, the transmission of digitized medical information has become very convenient due to the generality of Internet. Internet has created the biggest benefit to achieve the transmission of patient information efficiently. However, it is easier that the hackers can grab or duplicate the digitized information on the Internet. This will cause the following problems of medical security and copyright protection. In order to fulfil the security and convenience issues of the patients following goals like the prevention of medical fault, the real-time detection of abnormal event, the support of clinical decision and developing of medical service based on patient has to be achieved. For this purpose this paper proposes the technique called binary embedding technique. It uses the binary information of the text embedded with semi reversible properties in the image are called binary embedding. This technique prevents the distortion of embedded information in the original image due to addition of noise. The concept of semi reversible property is used retains the original information, image quality before and after the process of watermarking is presented as a statistical analysis.**

***Keywords*— Data hiding, Semi Reversible, data embedding, digital watermarking, binary data, text data, coefficient variation, multimedia security.**

I. INTRODUCTION

In today's world the 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 in the hospital for diagnosing and later in the future purpose [1]. The problem rises here that is while sending or giving the data to the patient we have to find whether the data belongs to particular patient or not and also the privacy of the patient is needed [2]. Hence authentication is required.

The traditional methods used for authentication is by enquiring the patient directly, dispatching the information either directly or sending the information to their mail [3]. In this method some duplication will be performed and information will wrongly deliver in false acceptance of result.

To avoid this type of problem, we used the latest technique called watermarking for authentication of the medical image [4]. Medical image watermarking means embedding the patient information in the medical image. Why have we chosen the watermarking for medical image to authenticate is, because it increases the storage compatibility and avoids storing of multiple information, etc [5].

In this paper we proposed Text fusion Image watermarking technique with semi-reversible property having higher order embedding capacity which is an improved model of this method. Here we used the binary information so that the complexity will be reduced. By using watermarking technique the memory needed to store the patient information is minimised and better authentication of the patient is performed.

A. Related Works

Frequencies domains watermarking such as DCT, FFT, DWT are used in which the image is initially transformed to the frequency domain then the low frequency components are modified containing the authentication [6]. Spatial domains watermarking is the values of the chosen frequencies are altered from the original containing the watermark [7]. There are some semi-reversible watermarking algorithm are used based on robust Fourier domain embedding technique for securing medical informatics but here the distortion occurs due to round of errors, here the robustness depends upon the size of the bit plane [8]. There is another method also used called difference expansion applied for multilayer embedding but the visual quality of the embedded image will be drastically degraded and also there must be underflow or overflow problem and having less hiding capacity [9]. These are some of the related works done.

B. Problem Definition

This specification document describes the capability that provides the software application "text fusion watermarking with semi-reversible properties in medical image for authentication" overcomes the problems which rises like medical image distortion, attack of watermarking medical images, etc.

C. Goals and Objectives

Goals

- To provide authentication for the patient by encapsulate the patient information in the medical image.
- To extract the patient information from the watermarked medical image and if authenticated then the medical image is recovered from the distortion which enables to get back the original medical image.

978-0-7695-3845-7/09 $26.00 © 2009 IEEE
DOI 10.1109/ARTCom.2009.18

- ➢ At the end, the original image, watermarked image and the reconstructed image is to be compared by using coefficient variation.

Objectives

- To provide the patient information to be hidden in the medical image component.
- To provide lower computational complexity and higher embedding capacity.

Medical image Processing:

The steganography concept is very useful in secret transfer and better authentication for medical images [10].

II. ANALYSIS

A. *Feasibility Study*

The Feasibility Study is made according to two major considerations [11].

Operational feasibility

- The proposed paper is beneficial to the authorized users. It prevents their information from reaching to hackers.
- All patients can access to their information easily from their medical image by extracting the information with the given key.

Technical feasibility:

- Technology needed for present project is already available.
- The latest techniques are incorporated so as to achieve the best of this new development of the system.
- This new technology guarantees imperceptibility, ease of accuracy and reliability.
- The system is fully developed and generalized, so that any future expansion will not be a hindrance.
- Security is provided in the form of data hiding technique called watermarking with the key. Hence unauthorized users cannot access the information in the system.

Thus we conclude that the Text Fusion watermarking with semi-reversible properties for Medical image authentication is not only operationally viable, with the right behavioural pattern, but also economically viable, with the required technical feasibility.

III. ARCHITECTURE OF PROPOSED SYSTEM

A. *System Architecture*

The image authentication is one of the critical processes where the copyright of the owner must be secured while transmitting the image in the network. So, we concentrate on the security of the owner information. For this we choose an invisible data hiding technique known as watermarking which is performed in the medical image for copy protection and authentication for medical images. The architecture is shown in fig 1

Let us see the advantages and disadvantages of this method.

Advantages:

- It is a semi- reversible data hiding technique with high-capacity and low-distortion characteristic by utilizing different expansion of the pixel pairs.
- It improves trustworthiness of signal tracing and maintaining the visual perception.

Disadvantages:

- The process of adjusting the watermark intensity for a given image is difficult.
- To prevent the reduction of the image quality, the processed pixel values which are greater than 255 will be abandoned. This will cause the reduction of the embedding capacity.
- Pseudo random bit sequence generation should be done before embedding the information for modifying the intensity values.

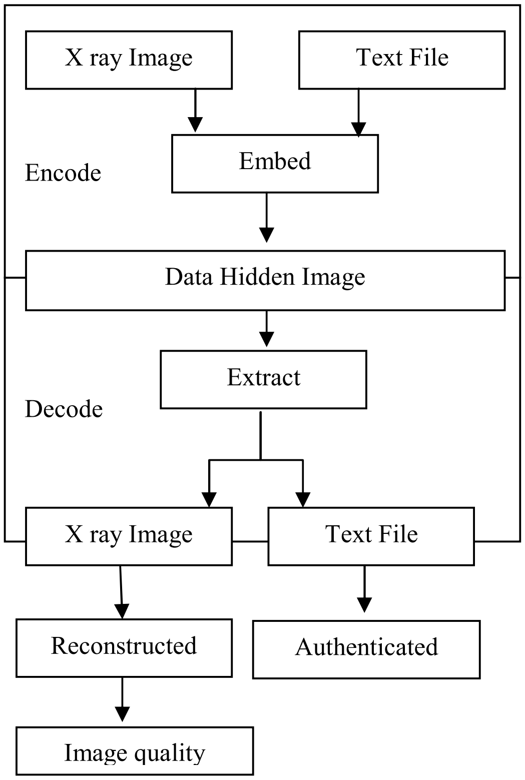


Fig1. Architecture of Watermarking

B. Proposed Method

We used the text fusion watermarking technique for better authentication of the medical image. In this case the detector uses a threshold value is the number of characters as the key provided to extract the data from the medical image. It also proposes the concept of semi reversible properties in the image for data-hiding and to get back the medical image without any distortion during watermarking. We demonstrate how the proposed approach reduces the probability of false negative detection without increasing the false positive detection rate. The coefficient variance of original medical image, watermarked image and reconstructed image is compared.

The proposed method is divided into ***five modules*** 1.Encoding, 2. Decoding, 3. Authentication,4. Reconstruction, 5. Correlation.

1) Encoding

The watermarking data is the text data having the patient information stored in the text file which is to be fused in the medical image.

Grey scale Image:

Our proposed method uses an X-ray image which is an intensity (grey scale) image where it takes an 8-bit value i.e. (0,255).

Watermark Embedding:

The embedding process is to mix the text data in the medical image. Firstly the text file having the patient information is read and then it was converted to the binary data using the equation (1).

$$B\ (t\ ) = \frac{\left((text\ (\ i\ )\&\ 2^7) \ll 1\right)}{2^7} \qquad (1)$$

Where, *1* $\leq$ *i* $\leq$ *count, 1* $\leq$ *t* $\leq$ *8* and *B* is binary data, count is the no of characters and *text ()* is the text data in the file. In order to have the semi reversible that is higher order function is performed using the equation (2).

$$I\ (x, y)\ =\ I(x, y)\ \&\ (2^8 - 2) \qquad (2)$$

Where *t* $\leq$ *i* $\leq$ *count *8* and *I(x, y)* is the source image.

Finally the binary content of the text data is embedded in the medical image using the equation (3)

$$W(x, y) = I(x, y) \oplus B\ (t) \qquad (3)$$

Where, W(x, y) represent the watermarked image. Now, the text data which has the patient information is hidden in the medical image with semi reversible property by bit by bit encoding of higher order sequence.

2) Decoding

During the decoding process the data encapsulated in the watermarked medical image is extracted for the authentication process.

Watermarked Image:

Our method uses an X-ray image which is intensity (grey scale) image where it takes an 8-bit value i.e. (0,255) embedded with the text data.

Watermark Extraction:

In our method the binary data of the text information embedded in the medical image is extracted. During extraction, the number of characters embedded is given as the key to decode the binary data and the medical watermarked image is performed using the equation (4).

$$B\ (t) = W(x, y)\ \&\ 1 \qquad (4)$$

After the extraction the binary data is converted to the text data using the equation (5) for the authentication.

$$\text{Text} = B(t) \times 2^{(8-t)} \qquad (5)$$

Where, *8*$\leq$ *t* $\geq$*I, 1* $\leq$ *i* $\leq$*count.*

3) Authentication

It is the process to determine the ownership of the information or image provided [11]. Here the multiple authentication is performed, once the user didn't give the correct key the extraction will not be performed and if the key is given correct, the extraction is performed and the text data is stored in the text file to compare with the information of the patient, if the data is correlated with the patient information then the image is authenticated else the image is not authenticated. Thus the authentication is performed

4) Reconstruction

Once the image is the medical image it must not be affected due to watermarking and if even though it is affected we ought to recover the affected area, to obtain the original medical image from the watermarked image so the image must be reconstructed [12]. This process follows only when the image is authenticated. After the image is authenticated then the watermarked image is reconstructed to recover the originality of medical image by using the semi reversible property followed using the equation (6)

$$I(x, y) = W(x, y) \oplus B\ (t) \qquad (6)$$

The reconstruction process is same as encoding process but the parameter is watermarked image and the binary data of the text obtained from the extracted resultant text data, finally the original image is obtained.

5) Image variance

Finally our attention is to the check the variance of the image before watermarking, after watermarking and after the reconstruction of image. Here we used the coefficient variation to detect the variation or changes in the image after the various modules like encoding, decoding and reconstruction. The variation is plotted in the graph relation in decibels (dB) using the equation (7), (8) and(9).

$$Mean = \frac{1}{N} \sum_{i=1}^{N} x_i \qquad (7)$$

$$SD = \sqrt{\frac{\sum_{i=1}^{N} (x_i - \mu)^2}{N}} \qquad (8)$$

$$Variation = \frac{Mean}{SD} \qquad (9)$$

IV. IMPLEMENTATION

A. Experimental Results

The medical image of size 256*256 grey level images is used to demonstrate the effectiveness of the text fusion watermarking method. Initially the text having the information of the patient in the notepad shown in *fig 5* is taken as a watermark. This text information is converted to binary data and transformed into the 128 bit of an original image shown in *fig 2* by exclusive operation resulted in watermarked image shown in *fig 3*. The watermarked image is further tested for the authentication by extracting the text information shown in *fig 6*.

The binary data is extracted and converted to text is done and stored in notepad. After extraction, the watermarked image is removed by reverse operation of exclusive with the resultant binary information of the text, which results removal of distortion and original medical image is recovered shown in fig 4. All the operation are performed using binary information resulted in less distortion watermarked image and the time taken for embedding, extracting and recovering are also very less.

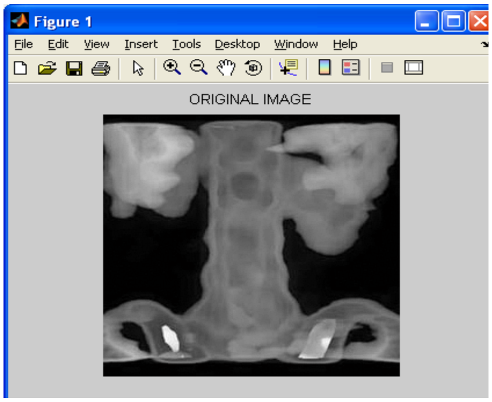


Fig2. Original Image

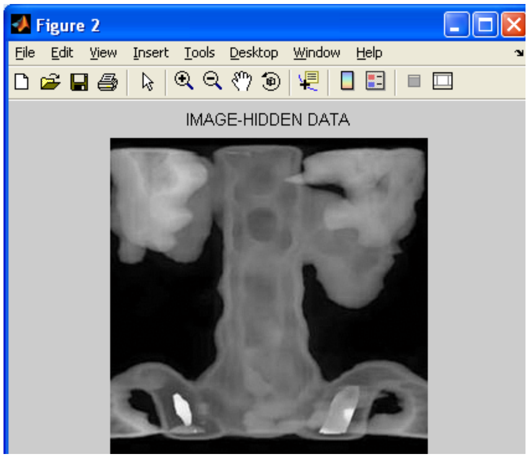


Fig3. Watermarked Image

The each resultant image obtained is compared with the original image using coefficient variation to test the level of distortion. The compared result is shown in fig 7 where there is less variance between the original image and watermarked image and there is no variance between the original image and recovered image. Finally the quality of the image is improved by the frequency domain technique by DWT.

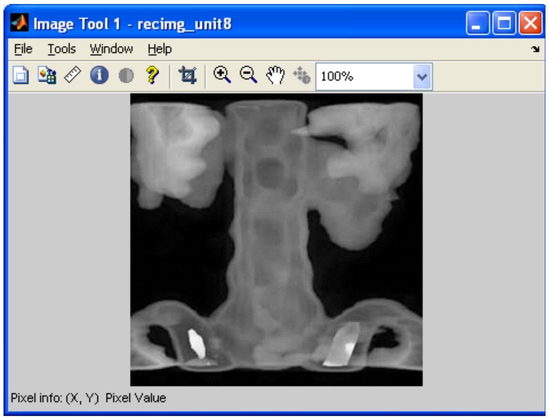
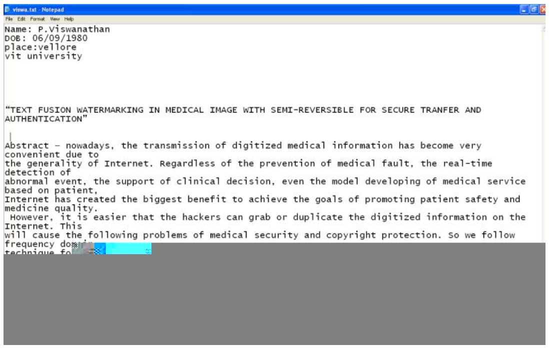


Fig4. Recovered Image



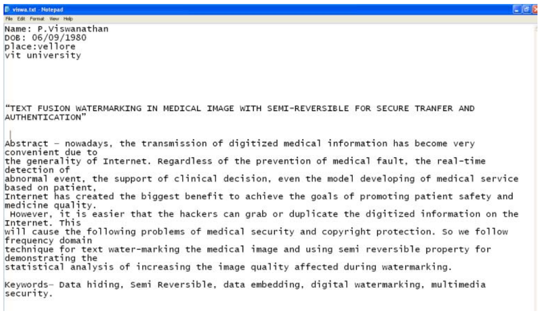
```
Name: P.Viswanathan
DOB: 06/09/1980
place:vellore
vit university



"TEXT FUSION WATERMARKING IN MEDICAL IMAGE WITH SEMI-REVERSIBLE FOR SECURE TRANFER AND
AUTHENTICATION"


Abstract – nowadays, the transmission of digitized medical information has become very
convenient due to
the generality of Internet. Regardless of the prevention of medical fault, the real-time
detection of
abnormal event, the support of clinical decision, even the model developing of medical service
based on patient,
Internet has created the biggest benefit to achieve the goals of promoting patient safety and
medicine quality.
 However, it is easier that the hackers can grab or duplicate the digitized information on the
Internet. This
will cause the following problems of medical security and copyright protection. So we follow
frequency do
technique fo
```

Fig5. Embedded Text



```
Name: P.Viswanathan
DOB: 06/09/1980
place:vellore
vit university



"TEXT FUSION WATERMARKING IN MEDICAL IMAGE WITH SEMI-REVERSIBLE FOR SECURE TRANFER AND
AUTHENTICATION"


Abstract – nowadays, the transmission of digitized medical information has become very
convenient due to
the generality of Internet. Regardless of the prevention of medical fault, the real-time
detection of
abnormal event, the support of clinical decision, even the model developing of medical service
based on patient,
Internet has created the biggest benefit to achieve the goals of promoting patient safety and
medicine quality.
 However, it is easier that the hackers can grab or duplicate the digitized information on the
Internet. This
will cause the following problems of medical security and copyright protection. So we follow
frequency domain
technique for text water-marking the medical image and using semi reversible property for
demonstrating the
statistical analysis of increasing the image quality affected during watermarking.

Keywords– Data hiding, Semi Reversible, data embedding, digital watermarking, multimedia
security.
```

Fig6. Extracted text

V. CONCLUSION

This paper presents a watermarking of the patient information in the form of text data which is embedded in medical image using the semi-reversible properties in order to get back the original medical image. Exploring space patterning of a text document used digital watermarking.

Digital watermarking in the frequency domain for general gray scale picture is useful for the desired quality of the watermarked image. It enables high-capacity applications for reversible data extraction in protecting medical images and data hiding. Thus the complete model with hiding the patient information in addition to the authentication information is performed

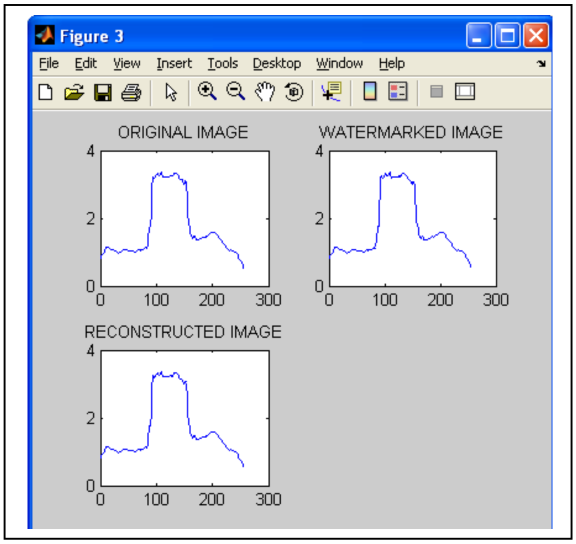


Fig 7. Coefficient Graph of original

VI. ACKNOWLEDGEMENT

The success accomplished in doing such a real life project such as this would not have been possible without the timely help rendered by many people to whom we feel obliged We express my gratitude to Dr P.Venkata krishna Associate Professor VIT University, for the valuable suggestions and timely feedback during the course of project. and grateful. We also thank staff and friends for their invaluable guidance and for constant support and encouragement.

VII. REFERENCES

[1] 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.

[2] Mingyan Li, Radha Poovendran, Sreeram Narayanan, Protecting patient privacy against unauthorized release of medical images in a group communication situation, Computerized Medical Imaging and Graphics 29 (2005) 367–383.

[3] L. Brinkmann T, A. Klein, T.Ganslandt, F. U¨ckert, Implementing a data safety and protection concept for a web-based exchange of variable medical image data, International Congress Series 1281 (2005) 191– 195.

[4] Ingemar Cox, Jeffrey Bloom, and Matthew Miller. *Digital Watermarking:Principles & Practice*. Morgan Kauffman Publishers, 2001.

[5] A. Ferreira et. al. Integrity for electronic patient record reports. In *Proc. 17th IEEE Symposium on Computer-based Medical Systems*. IEEE, 2004.

[6] Rajendra Acharya U, U.C. Niranjan, S.S. Iyengar, N. Kannathal, Lim Choo Min,Simultaneous storage of patient information with medical images in the frequency domain, Computer Methods and Programs in Biomedicine (2004) 76, 13—19

[7] Farid Ahmed and Ira S. Moskowitz. "A Semi-Reversible Watermark for Medical Image Authentication" *Proceedings of the 1st Distributed Diagnosis and Home Healthcare (D2H2) Conference Arlington, Virginia, USA*, April 2-4, 2006

[8] Jasni M. Zain, Abdul R.M. Fauzi, "Evaluation of Medical Image Watermarking with Tamper Detection and Recovery (AW-TDR)" *Proceedings of the 29th Annual InternationalConference of the IEEE EMBS Cité Internationale, Lyon, France* August 23-26, 2007.

[9] J. Tian, Reversible watermarking by difference expansion, Proceedings of Workshop on Multimedia and Security: Authentication, Secrecy, and Steganalysis, Dec.2002, pp. 19–22.

[10] William Stallings. *Cryptography and Network Security- Principles and Practices*. Prentice-Hall, 2003.

[11] Multimedia security laboratory. The Catholic University of America.

[12] J. L. Horner and J. R. Leger. Pattern recognition with binary phaseonly filters. *Applied Optics*, 24:609–611, 1985.

[13] Farid Ahmed and Ira S. Moskowitz. Correlation-based watermarking method for image authentication applications. *Optical Engineering*, 43(08):1833–1838, August 2004.

[14] Dom Osborne, Derek Rogers, Matthew Sorell, and Derek Abbott. Multiple medical image ROI authentication using watermarking. In *Proc. SPIE vol. 5651, Biomedical Applications of Micro- and Nanoengineering II*, pages 221–231. SPIE, 2005.

[15] Jessica Fridrich, Miroslav Goljan, and Rui Du. Lossless data embedding new paradigm in digital watermarking. *EURASIP Journal onApplied Signal Processing—Special Issue on Emerging Applications of Multimedia Data Hiding*, 2002.