Security Enhancement in Image Steganography for Medical Integrity Verification System

Sreekutty M S
M.Tech Student: Department of ECE
LBSITW , Poojappura
Trivandrum, India
sreekutty6635@gmail.com

Baiju P S
Assistant Professor: Department of ECE
LBSITW , Poojappura
Trivandrum, India
baijupstvm@gmail.com

***Abstract*— Nowadays image steganography has major role in confidential medical image communication. When the medical image is transmitted through insecure public network, there is a chance for tampering medical images . Therefore, it is crucial to check the integrity of medical images to prevent any unauthorized modification. To check the integrity we calculate cryptographic hash function of ROI (Region Of Interest) by using SHA algorithm. The hash value (H1) will be embedded in the RONI using discrete wavelet transform . By comparing the hash value at receiver side , we can check the integrity of medical image. If any tampering occurs, the hash function does not match. This paper proposes a new method to improve the security. The modified medical image is embedded in an ordinary looking image by spatial reversible steganography method. It helps to conceal the existence of secret medical data. It ensures that the eavesdroppers will not have any suspicion that medical image is hidden in that image. This combined approach will give enhanced security.**

Keywords—Image Steganography; Hash value; Medical Integrity;

I. INTRODUCTION

Digital image steganography[1] means hiding information within digital data. Steganography helps to conceal the existence of secret communication. Due to advancement in multi media communication technologies, a new context of easier access, manipulation, and distribution of this digital data have been established. Therefore the security of images transmitted through the public network takes lot of risk. There is a chance for the third party to access the data. It will leads to the tampering of medical image during transmission. Due to this we should provide sufficient security to the medical image to prevent unauthorized access[2]. For this we used steganographic techniques to provide sufficient authenticity and integrity[3].

By using steganographic technique , the embedded data should be invisible. It cannot be perceived by human eye vision. In medical image, integrity data embedded in the RONI(Region of non interest)[4]. RONI does not contains any valid information. So we embed secret information in RONI. It does not affect the diagnosis information.

Images can be tampered due to the introduction or the removal of lesions in image processing techniques. It may be caused by scaling, rotation etc, and lossy compression like JPEG[5]. It will lead to the loss of diagnosis information in medical image. Due to this results sometime misdiagnosis by the physician. Depending on the technique of tampering; there may be unacceptable information loss which results in a misdiagnosis by the physicians[6].

Due to this, integrity check is very important in medical image communication[7]. To avoid intentional attack we used an ordinary looking image as cover image. The modified medical image is embedded in that cover image gives more protection.

II. LITERATURE SURVEY

In early days a lot of region based techniques are proposed. ROI does not undergoes any modification. But RONI will be used for store the patient details.

Guo and Zhuang [8] have proposed region based lossless watermarking. This scheme is helps to the tamper detection. Region of embedding is selected in such a way that it does not intersect ROI. Digital signature is generated based on hash value. Watermark is generated by concatenating patient details and digital signature and then it is encrypted using Rivest Cipher 4 (RC4). Watermark is embedded using difference expansion technique in the region of embedding.

A hybrid watermarking method was proposed by Memon et al. [9] which generates a fragile watermark and a robust watermark. First the image is split into ROI and RONI region. Fragile watermark is embedded into the Least Significant Bit (LSB) of ROI and robust watermark is embedded into the embeddable blocks of RONI using integer wavelet transform. The ROI is combined with RONI to form the watermarked image. Upon reception the image is once again split into ROI and RONI. Fragile watermark is extracted from ROI and verified for tampering of image.

978-1- 5090-4967- 7/17/$31.00 © 2017 IEEE

Gouenou Coatrieu [10] present a medical image integrity verification system. It also deals to identify approximate local malevolent image alterations as well as identifying the nature of a global processing an image may have undergone (e.g., lossy compression, filtering, etc

III. PROPOSED SYTEM

The proposed system contains mainly two stages. They are protection stage and verification stage. This method is used in the centralized medical network.

A. Protection Stage

At this stage medical image is divided into ROI and RONI. ROI and RONI is separated manually by the help of a medical expert. It may be denoted by rectangular or polygonal shapes.Then calculates the cryptographic hash (H1) function of ROI using SHA -1 (Secure Hashing Algorithm) algorithm . Hash value (H1) means the condensed representation of ROI[11]. This hash value is concatenated with the vertices details of the ROI. After this the data will be embedded in the RONI [12].

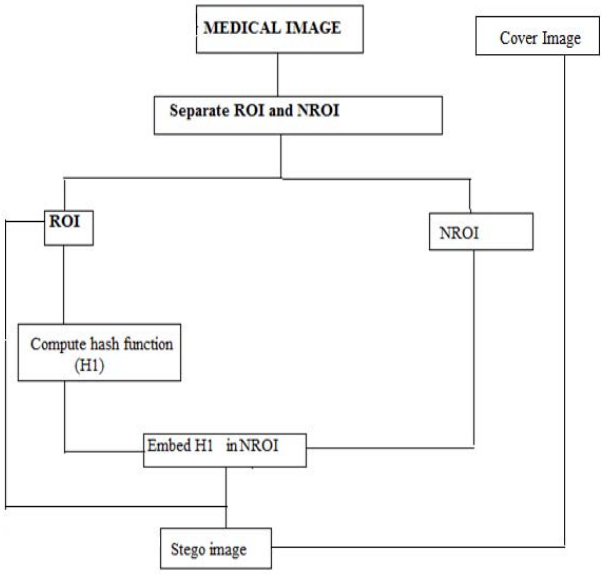

Fig. 1. : Protection Stage

This is done by the DWT steganographic method[13]. The frequency domain transform that applied in this paper is Haar DWT. For 2D Haar DWT, there are two operations: One is the horizontal and other is the vertical . In this case, the image is divided into LL,HL,LH and HH. The data is embedded in the high frequency part (HH). It contains detailed coefficient holding additional information about the image.We manipulate high frequency component to keep secret data.

After embedding the concatenated data, the modified image is embedded in the ordinary looking cover image. Modified medical image embedding will be done by reversible spatial domain technique. The embedding process steps are shown in below.

Here we consider two parameters in cover image. They are pixel position (Pp) and pixel value (Pv) . Pixel position, Pp is the position of pixel in the 2D matrix. Pp describes in odd or even according to the position value. Pixel value, Pv is the value contained in the pixel. For gray scale image pixel value is ranges 0 to 255 . Xiv* denotes pixel value of i th pixel of stego image. Xiv denotes pixel value of i th pixel of cover image. Xip* denotes position value of i th pixel of stego image. Xip denotes position value of i th pixel of cover image.

Before the embedding process, secret data will be converted into binary. It is denoted by a string of zeros and ones. This is denoted by Mi in this frame work.

Image Data embedding algorithm

- When Mi = 1

  If Xip =odd and Xiv =odd or

  If Xip =even and Xiv =even

  Xiv*= Xiv

  If Xip =odd and Xiv =even or

  If Xip =even and Xiv =odd

  Xiv*= Xiv+1

- When Mi = 0

  If Xip =odd and Xiv =odd or

  If Xip =even and Xiv =even

  Xiv*= Xiv+1

  If Xip =odd and Xiv =even or

  If Xip =even and Xiv =odd

  Xiv*= Xiv

The main parameter considered in this program is to check a number to be odd or even. Throughout this work, status of a number means whether it is odd or even. When the binary value to be embedded is 1, then if the status of pixel position and pixel value are compared. If they are same, no change is made. If they are not same, then the pixel value is incremented by 1. When the binary value to be embedded is 0, then if the status of pixel position and pixel value are compared. If they are not same, no change is made. If they are same, then the pixel value is incremented by 1.Pixel positions in cover image whose value incremented by 1 is noted and recorded as a key in a text file.

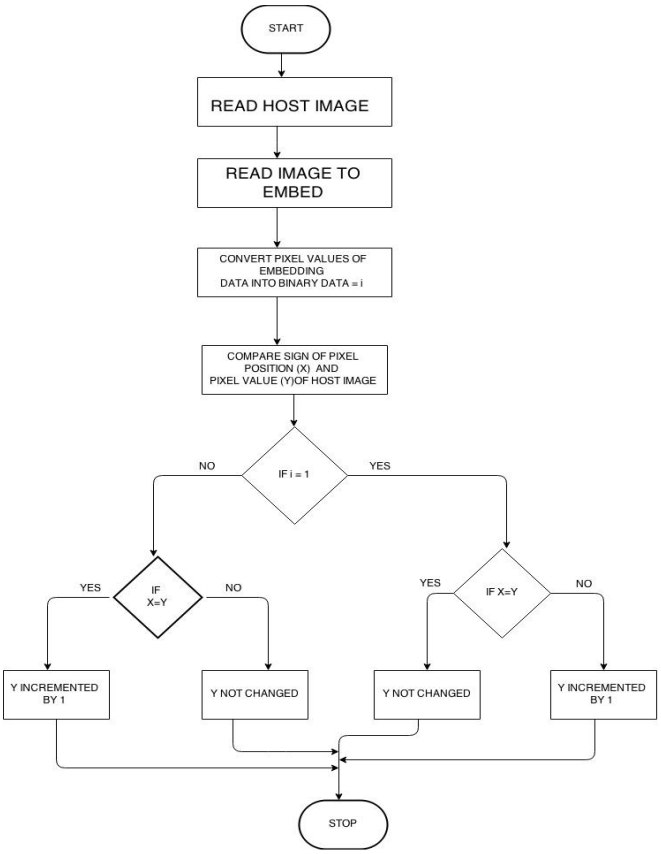

Fig 2. Image Embedding Process

By using this technique we can improve the image quality. Therefore imperceptibility of image is high.

B. Verification Stage

In verification stage we first extracted modified medical image from cover image. This steganographic method is best explained using the reverse engineering method.

A marked image (stego image) is considered. Then we check the status of a pixel position value and status of the pixel intensity value of stego image. When the status of a pixel position and status of the pixel value are equal, it is encountered as the hidden binary data is 1 when the status does not matches the hidden binary data taken as 0. After continuing this process we get set of binary values. By arranging it in proper order we get the output extracted image.

Data recovery algorithm

If Xip* =odd and Xiv *=odd or

If Xip*=even and Xiv* =even

Recovered binary value = 1

If Xip* =odd and Xiv *=even or

If Xip*=even and Xiv* =odd

Recovered binary value = 0

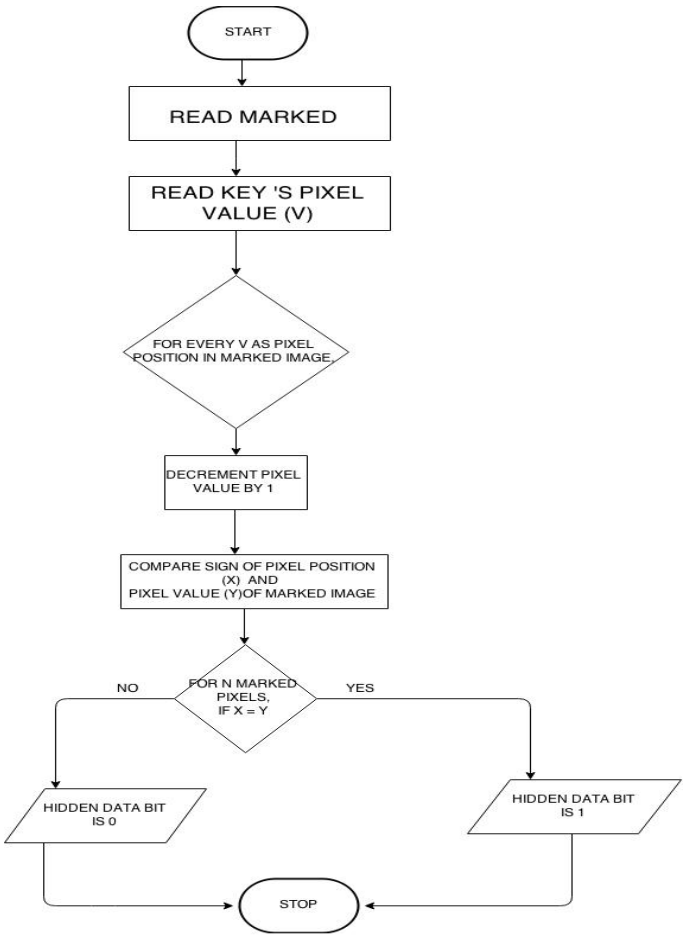

Fig. 3 : Image Extraction Process

Key is used to reconstruct the cover image from the marked image. In reconstruction, the pixel value in pixel position represented by the key image is decremented by 1.

Cover Image recovery algorithm

Xiv*-1 for every pixel in marked image specified by the key generated from marking process.

By using this technique we can hide data within the image. It has high embedding capacity. Also we can recover the original image without any loss.

From this extracted modified medical image ,we can separate ROI and RONI according to the information embedded.. Then extract the hash value (H1) from RONI . After that we compute the hash value (H2) of ROI in received medical image. If both hash functions are equal. It indicates there is no tampering takes place. If hash functions are not equal , it indicates that the image will undergoes some tampering process.

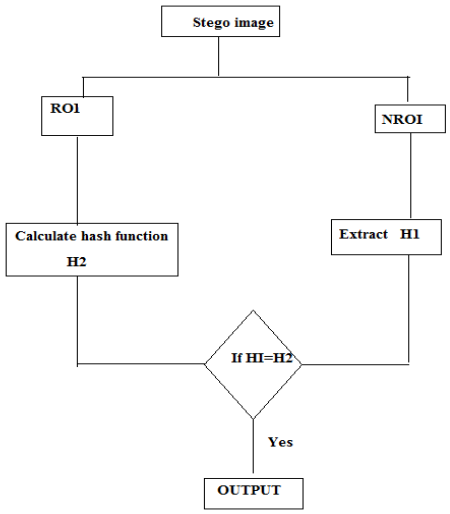

Fig. 4: Verification Stage

By using this medical integrity verification system we can check if the image undergoes any type of manipulation or not.

IV. RESULTS

In the traditional LSB algorithm applied in gray scale image, we replace the lsb of cover image into the secret information . But it is less robust. Hidden data can be easily destroyed by simple attacks. By using the new spatial steganographic method , PSNR is high . Imperceptibility is high. The results are displayed in Table I.

TABLE I. PSNR AND MSE OF PROPOSED METHOD

Proposed Method	
PSNR	***MSE***
78.8859	0.0791

Mean Square Error (MSE) is difference between the cover and stego images. For a cover image thickness and height are m and n, where I denote the cover-image and K denotes the stego-image MSE is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad \text{..... (1)}$$

The general PSNR formula is defined as the maximum value of a pixel in grayscale image is 255. A higher PSNR indicates that the quality of the stego image is better and more similar to the cover image.

$$PSNR = 10.log_{10}\left(\frac{MAX_I{}^2}{MSE}\right) \quad \text{.....(2)}$$

Fig 5 : Cover Image

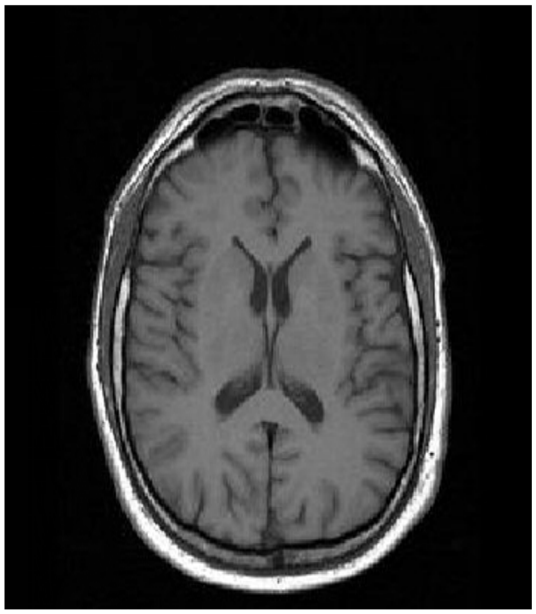

Fig 6 : Modified medical image

Fig 7 : Steganographic image

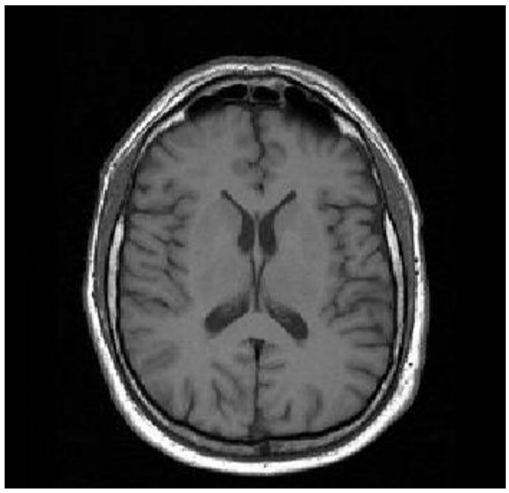

Fig 8 : Extracted Image

By using this steganography method , robustness is high . Data is embedded with minimum loss.

V. CONCLUSION

Medical integrity verification system has a major role in widely enhanced network. It certifies the medical image does not tampered by unauthorised person. Cryptographic hash functions are used to check the integrity. To increase the security, the modified medical image is embedded in a cover image. By using new spatial reversible steganographic method, we get high PSNR. It has high data embedding capacity. Imperceptibility is high. We can recover the original image by minimal loss. Image quality is high. It will help to enhance the security. This combined approach helps to achieve three goals of data hiding : capacity, integrity and security.

REFERENCES

[1] M. Awrangjeb, An Overview of Reversible Data Hiding, 6th International Conference on Computer and Information Tech- nology, pp. 75-79, December 2003

[2] R. Acharya and P. Subhanna Bhat and S. Kumar and C. Min, Transmission and storage of medical images with patient information, Journal of Computers in Biology and Medicine, Vol. 33, pp. 303-310, 2003.

[3] H. Huang, G. Coatrieux, H. Shu, L. Luo, and Ch. Roux, "Blind integrity verification of medical images, "IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 6, pp. 11221126, Nov. 2012.

[4] H.M. Chao and C.M. Hsu and S.G. Miaou, A data-hiding technique with authentication, integration, and confidentiality for electronic patient records, IEEE Trans Inf Technol Biomed, Vol. 1, pp. 46-53, March 2002.

[5] Gouenou Coatrieux, Hui Huang, Huazhong Shu, Limin Luo, and Chris- tian Roux, "A Watermarking-Based Medical Image Integrity Control System and an Image Moment Signature for Tampering Characteriza- tion, "IEEE Journal Of Biomedical and Health Informatics, VOL. 17, NO. 6, NOVEMBER 2013."

[6] Xuanwen Luo, Qiang Cheng, Joseph Tan, A Lossless Data Embedding Scheme For Medical in Application of e- Diagnosis, Proceedings of the 25th Annual International Conference of the IEEE EMBS Cancun, Mexico. September 17-21, 2003.

[7] Wu J. H. K., Chang R.-F., Chen C.-J., et al. Tamper detection and recovery for medical images using near-lossless information hiding technique. *Journal of Digital Imaging*. 2008;21(1):59–76. doi: 10.1007/s10278-007-9011-1

[8] Guo X., Zhuang T.-G. A region-based lossless watermarking scheme for enhancing security of medical data. *Journal of Digital Imaging*. 2009;22(1):53–64. doi: 10.1007/s10278-007-9043-6.

[9] . Memon N. A., Chaudhry A., Ahmad M., Keerio Z. A. Hybrid watermarking of medical images for ROI authentication and recovery. *International Journal of Computer Mathematics*. 2011;88(10):2057–2071.doi: 10.1080/00207160.2010.543677

[10] G. Coatrieux, J. Montagner, H. Huang, and C. Roux, "Mixed reversible and RONI watermarking for medical image reliability protection, "in Proc.29th Int. Conf. IEEE Eng. Med. Biol. Soc., 2007, pp. 56535656.

[11] Sharp, T.: An implementation of key-based digital signal steganography. In: Proc. Information Hiding Workshop. Volume 2137 of Springer LNCS. (2001) 13–26

[12] Joseph, Anisha, and S. S. Deepa. "An efficient watermarking based integrity control system for medical images." *2015 International Conference on Control Communication & Computing India (ICCC)*. IEEE, 2015

[13] A. Giakoumaki and S. Pavlopoulos and D. Koutsouris, A med- ical image watermarking scheme based on wavelet transform, in Proc. 25" Annual Intemational Conference of the IEEE Engineering in Medicine and Biology Society, pp. 856-859, 2003.