World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:7, 2015

Effectual Reversible Watermarking Method for Hide the Patient Details in Brain Tumor Image

K. Amudha, C. Nelson Kennedy Babu, S. Balu

Abstract**—**The security of the medical images and its related data is the major research area which is to be concentrated in today's era. Security in the medical image indicates that the physician may hide patients' related data in the medical image and transfer it safely to a defined location using reversible watermarking. Many reversible watermarking methods had proposed over the decade. This paper enhances the security level in brain tumor images to hide the patient's detail, which has to be conferred with other physician's suggestions. The details or the information will be hidden in Non-ROI area of the image by using the block cipher algorithm. The block cipher uses different keys to extract the details that are difficult for the intruder to detect all the keys and to spot the details, which are the key advantage of this method. The ROI is the tumor area and Non-ROI is the area rest of ROI. The Non-ROI should not be spoiled in any cause and the details in the Non-ROI should be extracted correctly. The reversible watermarking method proposed in this paper performs well when compared to existing methods in the process of extraction of an original image and providing information security.

Keywords**—**Brain tumor images, Block Cipher, Reversible watermarking, ROI.

I. Introduction

THE term reversible watermarking is derived from the watermarking process used for the authentication. The watermarking process authenticates by hiding the details or information in some format and extracting the details for authentication (for e.g. Barcodes in shops, colleges, companies, etc.).

Watermarking only extracts the details and does not check its originality, but reversible watermarking does both extraction and its originality. Reversible watermarking (RWM) is used in the medical field to hide the patient's detail into an image. The RWM not only authenticate but also checks whether the extracted image is bit-by-bit and pixel by pixel same as an original image.

In some situations, there is a need for the physician to consult the patient's details with another physician. In order to achieve this, RWM helps to hide those details in the image itself without degrading the image quality. The third person cannot recognize, which patient image and details were hidden in that image.

In Brain Tumor image, the Region of Interest (ROI) is the area belongs to the tumor in the image and the other area is the Non-ROI. The data can be hidden in the Non-ROI, which is the proper area to hide the information. The details cannot be hidden in ROI because it is the region that contains the tumor details.

The main use of RWM is too aspired in the fields like Medical Image Security, Electronic Patient Records, and Clinical Atlas. Many methods have been proposed already in RWM like wavelet transform method, pixel difference expansion and histogram shifting technique. The proposed methods perform well than the existing methods by extracting the embedded data correctly and retrieving the original image without degrading the quality.

II. Existing Methods

Wavelets transform based watermarking method was applied in a digital image to obtain the wavelet coefficients [1]. The wavelet coefficients were high-frequency sub bands HL, HH, LH used to embed the data. Those high-frequency integer wavelet coefficients exceed the upper and lower bound values, which cause underflow and overflow during the reverse integer wavelet transform. To avoid the histogram narrow down process that took place and the threshold value that has been set, the number of embedding rules were applied to the wavelet coefficients according to the values as higher, lower and equal to the threshold. The main drawback of this method was that, images were overwritten in ROI region of an image, which cannot be used during the diagnosis of the patient.

The most admired method in reversible watermarking was the pixel value difference expansion method which acts as the base for many forthcoming methods [2]. The reverse integer wavelet transform was used to avoid the overflow and underflow. The x, y value ranges from [0,255]. L indicates the integer average; H indicates the difference and the bit b could be embedded in the difference value H. Thus H' indicates the expandable difference. In another 'H' denotes the change in difference value under the integer L. The data embedded in the difference value H and the expandable difference H' may also be altered. To extract the data, there was a need to know the expandable and difference value. The main drawback in this method was that not all pairs were used for expansion to embed the data. Though the location map indicates which pairs were used to embed the data, it was also possible to detect the frequently paired pixel by the third person. To avoid this, the improved version of pixel value difference expansion method was proposed in which more data hiding can be achieved [2].

K. Amudha and S. Balu are with the K. S. Rangasamy College of Technology, Tiruchengode, Tamilnadu, India (e-mail: amudhak02@gmail.com, sbalu26@gmail.com).

C. Nelson Kennedy Babu is with the CMS College of Engineering, Namakkal, TamilNadu, India (e-mail: cnkbabu63@yahoo.co.in)

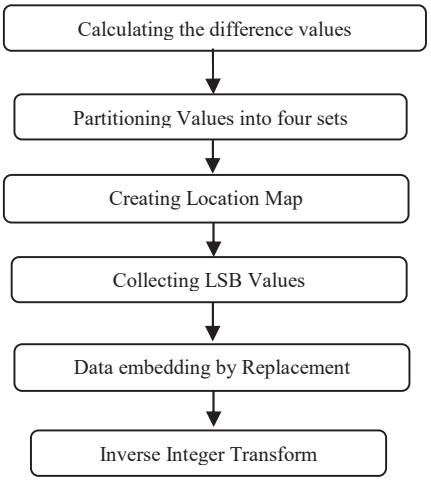

Fig. 1 Data Embedding Algorithm

The lossless reversible data hiding can be achieved by shifting the histogram and selecting the histogram peak ratio to embed the data [3]. The peak points and zero points were selected in the image histogram. The peak points were selected based on the maximum number of pixels in the grayscale value and zero points were selected based on the no pixel in the image. The number of bits to be encoded was set to be equal to the maximum number of bits associated with the peak point. After selecting the peak points and the zero points, the histogram value of the pixel above the peak point value was increased by one. As the peak point was revealed to the extractor already, it was possible to extract the original histogram and embedded data by subtracting the values before the peak point by 1. However, the main problem was the retrieval and extraction of the data, which were not being mentioned properly.

The disadvantage of the histogram modification method was eliminated by not embedding data in the peak point pixel, instead embedding it in peak point's neighboring pixel [4]. This method modified the peak point, which also results in highest PSNR ratio. The difference in the histogram modification method was proposed to reduce the distortion and to achieve highest PSNR ratio [5].

Block-based scheme examined the images interms of blocks [6]. In this method, the image was divided into blocks and the smoother areas were selected to embed the data.

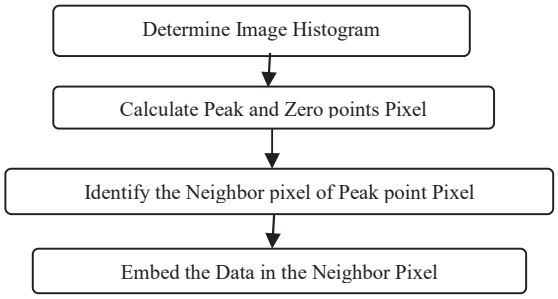

Fig. 2 Histogram Modification

Watermarking with encryption combined system was proposed for the purpose of protecting medical images [7]. This system was based on an approach combined a substitutive watermarking algorithm, quantization index modulation, with an encryption algorithm. Watermarking and encryption were conducted jointly at the protection stage. 8-bit ultrasound images and 16-bit PET images were taken for security analysis. A lossless watermarking based authentication system was proposed for the medical image integrity [8]. It gave an overview of watermarking technology by paying attention to fragile watermarking since it was the usual scheme for authentication. This technique was adapted for interleaving patient information and message authentication code with medical images in a reversible manner by used lossless compression.

A new reversible watermarking scheme was proposed to identifying parts of the image that are watermarked using two distinct modulations: Pixel Histogram Shifting and Dynamic Prediction Error Histogram Shifting [9]. It gave a very good compromise in terms of capacity and image quality preservation for both medical and natural images. A robust reversible watermarking modulation was proposed for images to the protection of relational databases [10]. It could be used for verifying database authentication as well as for traceability when identifying database origin after it had been modified. This model had the impact of the embedding process and database modifications on the probability distribution of the center of mass position.

A lossless image watermarking system was proposed which uses the lifting wavelets transform with integer to integer lifting scheme with all wavelets to host image [11]. It provided Wavelet Transform domain technique and arithmetic coding technique to improve the quality of watermarked image. An improved adaptive histogram modification based reversible data hiding technique proposed for color images [12]. Reversible or Lossless data embedding was a technique that embeds data into an image in a reversible manner. The histogram modification based reversible data hiding technique using causal window was proposed which predicts the embedding level with the help of the pixel value, edge value, just noticeable difference value. This system significantly improved the data embedding capacity along with greater visual quality.

The proposed method uses the non-ROI to embed the data to avoid the drawbacks that were mentioned in the existing methods.

III. Proposed Method

The image is segmented to identify the ROI and non-ROI in the image. After identifying the ROI and non-ROI, the image is divided into four regions. The regions belonging to the non-ROI and ROI are identified separately in order to embed the details in the non-ROI regions. The image cannot be transferred directly. Hence, the image is encrypted using an encryption algorithm.

The encryption algorithm used here is the block cipher which uses the different key for different blocks. The benefit of using the block cipher is that it is difficult to break the encryption and the intruder can't detect the keys because many keys are being used. If intruders detect any one of the key, it is difficult to detect all keys used. The algorithm used to encrypt the image is RC6 which is one of the block cipher technique. The RC6 has better features corresponds to the block cipher scheme.

Specification of RC6: - RC6-w/r/b where, w- Word size; r- Non-negative number of rounds; b- Length of the encryption key.

The base-two logarithm of w will be denoted by log w.

- a + b : integer addition modulo 2^w
- a – b : integer subtraction modulo 2^w
- a @ b : bitwise exclusive-or of w-bit words
- a * b : integer multiplication modulo 2^w
- a <<< b: rotate the w-bit word 'a' to the left by the amount given by the least significant LSB bits of 'b'
- a >>> b: rotate the w-bit word 'a' to the right by the amount given by the least significant LSB bits of 'b'

Here the keys used for encryption is three since three regions are selected to embed the details. After encryption, the regions belonging to the non-ROI is selected and the details to be hidden must be embedded into that area, as the ROI of an image should not be affected. The sender side algorithm is shown in Fig. 3.

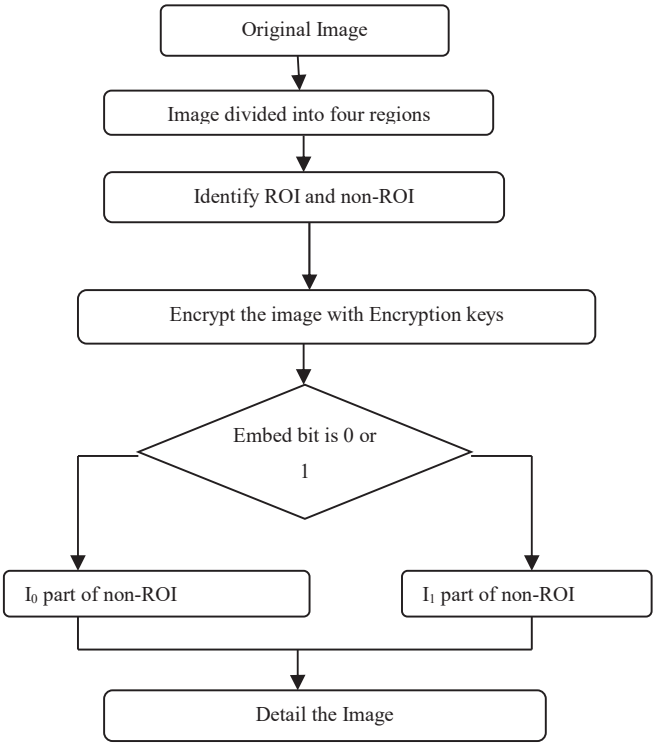

Fig. 3 Flow Diagram for Encrypted Brain Tumor Image

In order to embed the details, the embedding information should be converted into the ASCII codes. The ASCII codes are then transformed to binary codes because only the binary codes can be embedded into the non-ROI area. Each non-ROI is divided into sets I_0 and I_1 in which the pixel embedding probability is 1/2. If the pixel to be embedded is zero, then it should be done in I_0 by shifting three least significant bits (LSB's) to left. If the pixel to be embedded is one, then it should be done in the I_1 by shifting three least significant bits to left. This operation is repeated until the patient details are embedded fully.

On the receiver side, the received encrypted image is divided into regions and the decrypted. In order to identify the non-ROI and ROI, the image is divided into regions. Finally, the image is decrypted using the RC6 decryption algorithm with the help of keys. RC6 capitulate good results compared to the existing method to encrypt/decrypt images.

After decrypting the image, the LSB operation is used to find the details that are embedded in the image. Consecutively, the three LSB bits in the non-ROI are flipped (in both I_0 and I_1). The I_0 region of non-ROI contains the zeros of the embedded data whereas I_1 region contains the ones of the embedded data. This step is repeated until the patient details are completely retrieved. The receiver side algorithm is shown in Fig. 4.

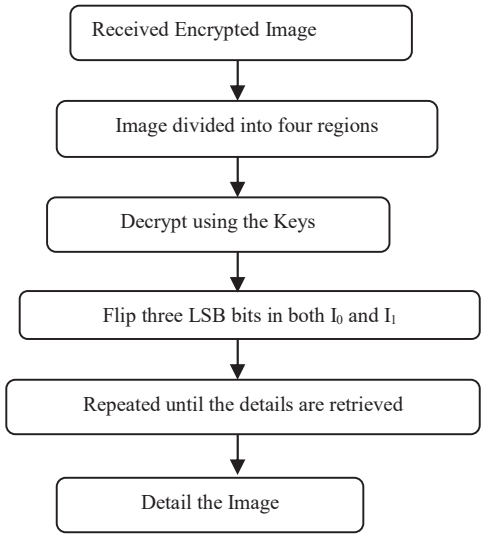

Fig. 4 Flow Diagram for Decrypted Brain Tumor Image

IV. Results and Discussion

The experimental results show that the algorithm works well compared to existing methods in all the ways. The size of the input brain tumor image is 200*200 as shown in Fig. 5. Then, the image is divided into four regions as shown in Fig. 6. The ROI and non-ROI can be easily identified to embed the data. In existing methods, the details are hidden in the image without considering the ROI and non-ROI, this causes the ROI region has modified gradually. So it should be kept original. The proposed method does well in this part and embeds the details of the patient in the non-ROI and ROI is kept original. The PSNR value is also increased when compared to the existing methods. The extracted image also has the maximum

originality of the input brain tumor image. The details that are embedded in the non-ROI are retrieved correctly. The estimation time of the proposed method is less when compared to the existing methods.

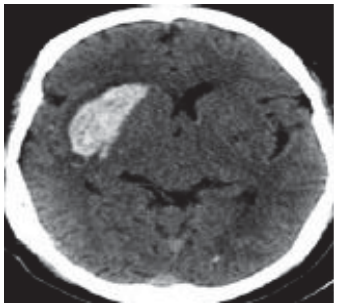

Fig. 5 Original Brain Tumor Image

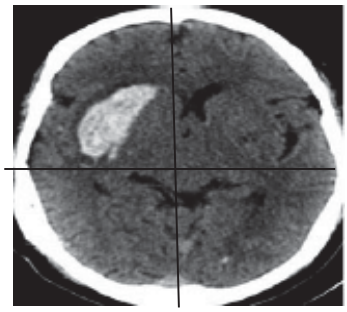

Fig. 6 Brain Tumor Image divided into Regions

The image divided into four regions numbered 1 to 4, the region 1 belongs to ROI area whereas others 2, 3, 4 belongs to non-ROI area in which the details can be embedded. The original image has been encrypted with keys using encryption algorithm is shown in Fig. 7.

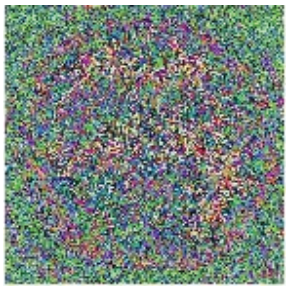

Fig. 7 Encrypted Brain Tumor Image

Patient Details
Patinet ID = 152
Patient Name = aaa
Tumor range = .05mm

Fig. 8 Sample Patient Details to be embedded

After embedding patient details, again the image is encrypted with a key which is shown in Fig. 9.

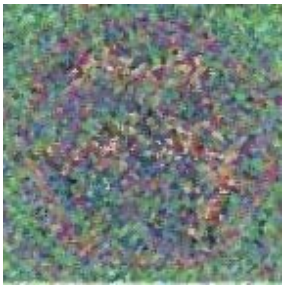

Fig. 9 Encrypted Brain Tumor Image after embedding patient details

Encrypted and watermarked image is decrypted by performing the reverse operation of RC6 encryption. The decrypted brain tumor image is shown in Fig. 10.

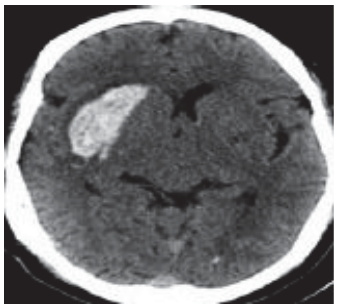

Fig. 10 Decrypted Brain Tumor Image

Patient Details
Patinet ID = 152
Patient Name = aaa
Tumor range = .05mm

Fig. 11 Retrieved Patient Details

The performance of this system is evaluated by calculating PSNR and Mean Square Error value, which is tabulated in Table I

TABLE I
PERFORMANCE EVALUATION

Parameters	Values
Time required	27.2690
PSNR	50.1782
MSE	0.09128

Pixel intensity values of the original input image are plotted in Fig. 12. Input image is encrypted by RC6 encryption algorithm after that the pixel intensity values are represented as a graph in Fig. 13.

Patient details are embedded into the encrypted image of original brain tumor image and again encrypted with security keys which histogram is shown in Fig. 14. Decrypted image is retrieved by reverse operation of RC6 encryption algorithm and its histogram is shown in Fig. 15.

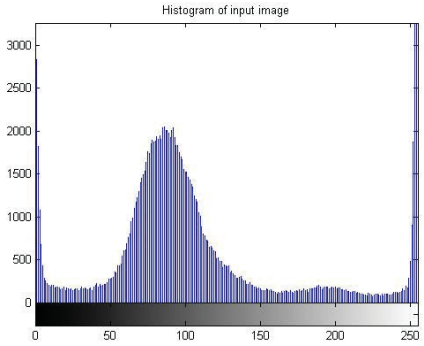

Fig. 12 Histogram of Input Image

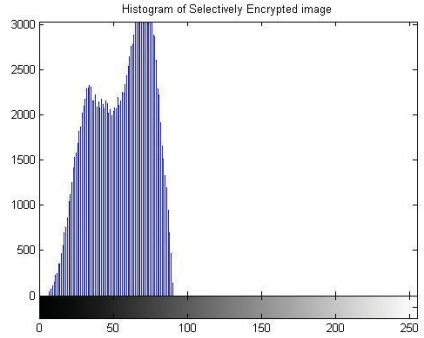

Fig. 13 Histogram of Encrypted Image

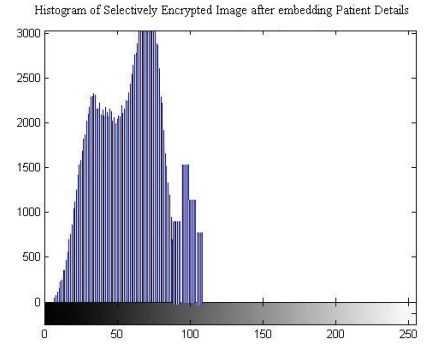

Fig. 14 Histogram of encrypted input Image after embedding patient details

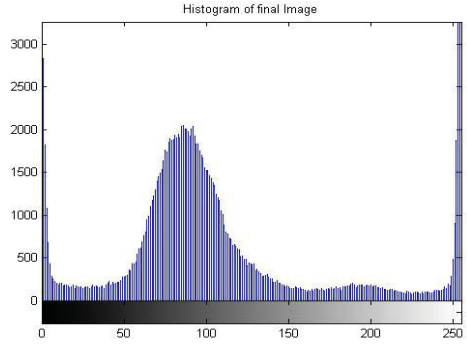

Fig. 15 Histogram of Decrypted Image

V. Conclusion

The embedding detail in the image was proposed by many methods. However, this ROI and non-ROI splitting method gives better results to embedding more information safely and retrieved that information in exact manner. This ROI and non-ROI combined with LSB shifting method is used to embed the data too securely. The patient's information is also secured using the block cipher. The reason for using the block cipher is that different keys are used to encrypt and decrypt the image. This proposed method has improved PSNR ratio, which improves the image quality and performs well in the brain tumor image and it can be used in medical applications.

References

[1] D. Giakoumaki, S. Pavlopoulos and Koutsouris, "Multiple image watermarking applied to health information management," in *IEEE Trans. Inf. Technol. Biomed*, pp. 722–732, 2006.

[2] J. Tian, "Reversible data embedding using a difference expansion," in *IEEE Trans. Circuits Syst. Video Technol*, vol.13, pp.890–896, 2003.

[3] Z. Ni, Y Q. Shi, N. Ansari and W. Su, "Reversible data hiding," in *IEEE Trans. Circuits Syst. Video Technol*, vol.16, pp. 354–362, 2006.

[4] H W. Tseng and C P. Hsieh, "Reversible data hiding based on image histogram modification," in *Imaging Sci. J,* vol.56, pp. 271–278, 2008.

[5] C. Lin, W L. Tai and C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," in *IEEE Trans. Pattern Recogn*, vol.41, pp.3582–359, 2008.

[6] H J. Kim, V. Sachnev, Y Q. Shi, J. Nam and H. G. Choo, "A novel difference expansion transform for reversible data embedding," in *IEEE Transactions on Information Forensics and Security*, vol.3, pp. 456–465, 2008.

[7] D. Bouslimi, and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echo graphic images," in *Compute Methods Programs Biomed*, pp 47-54, 2012.

[8] S Boucherkha and M Benmohamed, "A lossless watermarking based authentication system for medical images," in *international journal of signal process*, pp 278-81, 2004.

[9] W Pan, G Coatrieux, N Cuppens, F Cuppens and C Roux, "Reversible watermarking based on invariant image classification and dynamical error histogram shifting," in *Engineering in medicine and biology society*, annual international conference of the IEEE, pp. 4477–80, 2011.

[10] Javier Franco-Contreras, Mem Gouenou Coatrieux, Fréderic Cuppens, Nora Cuppens Boulahia, and Christian Roux, "Robust Lossless Watermarking of Relational Databases Based on Circular Histogram Modulation," *IEEE transactions on information forensics and security*, Vol.9, No.3, 2014.

[11] Rekha D. Patil and A. R. Nigavekar, "Reversible Image Watermarking Using Lifting Wavelet Transform and Arithmetic Coding," *International Journal of Engineering Research & Technology*, Vol. 2, Issue 2, 2013.

[12] A. Gopi Krishna and A. Mallikarjuna Prasad, "Adaptive Histogram Modification Based Reversible Data Hiding Algorithm for Color Images," *International Journal of Research in Computer and Communication Technology*, Vol. 2, Issue.8, 2013.