International Journal of u- and e- Service, Science and Technology
Vol.9, No. 7 (2016), pp.121-130
http://dx.doi.org/10.14257/ijunesst.2016.9.7.12

Enhancing Information Capacity and Security Level Based on Reversible Watermarking Technique in Medical Images

K. Amudha[1], C. Nelson Kennady Babu[2] and S. Balu[3]

[1]*Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, India*
[2]*Computer Science and Engineering, CMS College of Engineering, India*
[3]*Computer Science and Engineering, K.S.Rangasamy College of Technology, India*
[1]*amudhak02@gmail.com*, [2]*cnkbabu63@yahoo.co.in*, [3]*sbalu26@gmail.com*

Abstract

This paper proposes a new technique based on reversible watermarking to improve information embedding capacity and security level in medical images. This technique uses two methods namely Image compression and image partitioning techniques. Original image is converted into R-S Vector interms of ones and zeros and it is compressed to provide space for embedding more information. Hash value is calculated from original image to analyze security level. Image partitioning technique divides the image into two parts then secret information is embedded into LSB bits. This image compression and partitioning technique improves the information embedding capacity level and hash output confirms the image integrity level.

Keywords: *Image security, loss less compression, image partitioning, encryption, data hiding*

1. Introduction

In recent days, hospital data base systems store the patient data and medical images in a computer network. Those medical images and patient data are converted and stored as a digital data in computer network. The patient data is exchanged from one hospital to another hospital significantly. So it is necessary to protect the patient data from an illegal use, because sharing of patient data may lead to some security issues like confidentiality, image reliability and authentication. These security levels are confirmed by a technique called reversible watermarking technique. Watermarking is a method of modulating or modifying the gray level values of image pixels for inserting a message. The watermarking technique consists of two main process namely embedding process and extraction process. In the embedding process, secret information is embedded into the original image. In the extraction process, the original information is retrieved from the encrypted image with the help of same secret keys. The reversible watermarking technique is used to check the uniqueness of the patient information and input image. In this paper, a new security technique is proposed which is used to enhance security levels and information embedding capacity. This technique uses R-S vector formation, compression and image partitioning technique. R-S vector is formed by flipping and discriminating function which is used to convert each group of pixels interms of ones and zeros. Loss less compression algorithm compresses the RS vector output to provide space for embedding more information. Image partitioning technique divides the image into part A and part B and information is embedded into LSB bits of part A.

ISSN: 2005-4246 IJUNESST

2. Existing Methods

A region-based tampering detection and recovering method was proposed based on reversible watermarking and quad-tree decomposition [1]. Quad-tree decomposition was used to divide the input image and linear interpolation process was used to calculate a recovery feature. This technique used invertible integer transformation to embed all recovery features. Double Watermarking of DICOM Medical Images was proposed based on Wavelet Decomposition Technique [2]. The first embedded information was Electrocardiograph and second embedded information was Patient's demographic text ID. This method used Wavelet Decomposition Technique which was used to embed double watermark. Watermarking technique was proposed based on frequency domain which was used to improve the deficiency of the JPEG quantification [3]. This result was achieved by reducing the bit error rate of the recovered watermark**.** Frequency domain techniques improved the quality of retrieved image in order to reduce the bit error rate and adjust the value of transform coefficients. Blind assessment of image quality was improved based on fragile and robust watermarking techniques [4]. Transmitted image degradation was measured by fragile watermark. Robust watermark was used to construct a reference watermark from the received image in order to measure the amount of degradation of the fragile watermark.

Authentication and data hiding was proposed based on ROI watermarking scheme for DICOM images [5]. The original image was divided into ROI and RONI and then hash value of ROI was calculated. This hash value and patient's information was embedded into ROI. This watermarked ROI was embedded into RONI by Discrete Wavelet Transform technique. Hybrid watermarking was proposed for medical images based on ROI and RONI technique [6]. In this method secret information was embedded into least significant bits of ROI. This watermarked ROI was embedded into RONI using integer wavelet transform. Two dimensional chaotic maps and improved algorithm was proposed for security analysis of image encryption [7]. This technique used chaotic algorithm to improve the security level. The original image pixel position was changed based on the chaotic key. After encryption and decryption, the original image was retrieved with respect to chaotic key. Lossless information hiding technique was proposed for tamper detection and recovery of medical images [8]. It was worked based on region of interest and region of non interest. This technique used hash algorithm to calculate the hash value of ROI which improved image integrity level. Secret information was embedded into ROI and this embedded ROI was combined into RONI. In this receiver side the extracted image hash value was equal to the hash value of the original image.

Chaotic Watermarking Scheme was proposed for Authentication of JPEG Images [9]. Discrete Cosine Transform was applied to find DCT coefficients. After entropy decoding, the quantized DCT coefficients were mapped to the initial values of the chaotic system. Chaotic iteration was embedded into the JPEG compressed domain to generate watermark information. Re-Quantization could not invalidate tamper detection because DCT coefficients were modified directly after quantization. So this technique performed extraction process in the compression domain. Resistance of the double random phase encryption technique was proposed against various attacks [10]. This technique demonstrated various attacks on computer generated ciphered images. This method was shown to be resistant against brute force attacks but it is danger to select the known plaintext attacks. Reversible watermarking technique was proposed for tamper detection and recovery of medical images [11]. Original image was divided into ROI and RONI. The least significant bits of ROI were taken and compressed by Run Length encoding and then embedded into RONI. Image Encryption Algorithm was proposed based on Chaotic Mapping to protect the confidentiality, integrity and authenticity of original images [12]. This technique used alternative symmetric key

encryption algorithm to secure medical images. This symmetric key encryption algorithm was to secure image encryption which was based on chaos. It comprised of horizontal and vertical transformation function, shift function and gray scale function. Wavelet Based Watermarking Method was proposed for Digital Images using the Human Visual System [13]. In this technique the number of watermark elements was proportional to the energy contained in each wavelet transform bands. The ratio of changing rate of a sinusoidal pattern to subtended visual angle in cycles per degree was calculated to estimate the characteristic of the image. Adaptive Image Watermarking Scheme was proposed based on Visual masking [14]. This technique considered brightness sensitivity and texture sensitivity which was adaptive in the strength of watermarks. DC components in the discrete cosine transform were used to estimate the brightness sensitivity. DCT coefficients were quantized by JPEG quantization table which was used to estimate texture sensitivity.

From this literature survey, existing methods used only one technique to embed secret information. Even if, double watermark was used in existing technique which means double time information was embedded into it but it used single technique to provide space for double time embedding information. Compared to existing methods proposed method uses two techniques to provide space for embedding information. So that it provide more space to double watermark. Similarly it uses double encryption technique to achieve high security level.

3. Proposed Method

Loss less image compression and image partitioning technique enhances the security level and improves the information capacity. This algorithm achieves image integrity, authentication and confidentiality. The sender side algorithm is given below:

3.1. Sender Side Algorithm

Step 1: Extract groups from original image

Step 2: Calculate R-S vector

Step 3: Compress R-S vector

Step 4: Determine the MD5 hash value of original image

Step 5: Append the MD5 hash value, compressed R-S vector and patient information

Step 6: Encrypt the output of step 5 and embed into the original image

Step 7: This step 6 output is again divided into Part A and Part B

Step 8: Embed LSB bits of part A into Part B

Step 9: Embed secret information into Part A

Step 10: Append Part A and Part B

Step 11: Encrypt the output of step10 by AES algorithm.

3.1.1. Group Extraction: Original input image is partitioned into groups and each group contains four pixels. The pixel value is represented interms of 1s or 0s. This single valued 1s or 0s are determined by discriminating and flipping function.

3.1.2. Flipping Function: Flipping function modifies the pixel value by changing least significant bit. If the LSB bit is '1' it is changed to '0' or if the LSB bit is '0' it is changed to '1'. For example, if the value of a pixel is 144 which is represented in the binary system as 10010000. On applying flipping function, the LSB bit is flipped to be '1' instead of '0', then the pixel value is changed from 144 to 145. The values of four pixels are 156, 157, 158 and 156 which is represented in the binary system as 10011100, 10011101, 10011110 and 10011100. On applying discrimination function to this group of pixels, the value is calculated by the following equation,

Discrimination value $=\sum|P_{i+1}-P_i|$

$D_{Before} = \sum(|156-157)|+(|157-158|)+(|158-156|)$

$=\sum (1+1+2)$

$D_{Before} =4$

The value of each pixel of that group is modified by flipping function. After using flipping function the values of four pixels are 157, 156, 159 and 157 which is represented in the binary value as 10011101, 10011101, 10011111 and 10011101. On applying discrimination function to this group of pixels, the value is

$D_{After} = \sum (|157-156)|+ (|156-159|) + (|159-157|)$

$=\sum (1+3+2)$

$D_{After} =6$

3.1.3. Discrimination Function: Discrimination function defines the state of the group as regular group or singular group based on its discrimination value. The discrimination value is calculated for each group before using the flipping function and after using the flipping function. The condition for determining the state of the group is as follows,

- $D_{after} > D_{before} \longrightarrow$ Regular group
- $D_{after} > D_{before} \longrightarrow$ Singular group
- $D_{after} = D_{before} \longrightarrow$ Unused group

So the state of the above example is Regular group, because D_{after} (6) > D_{before} (4)

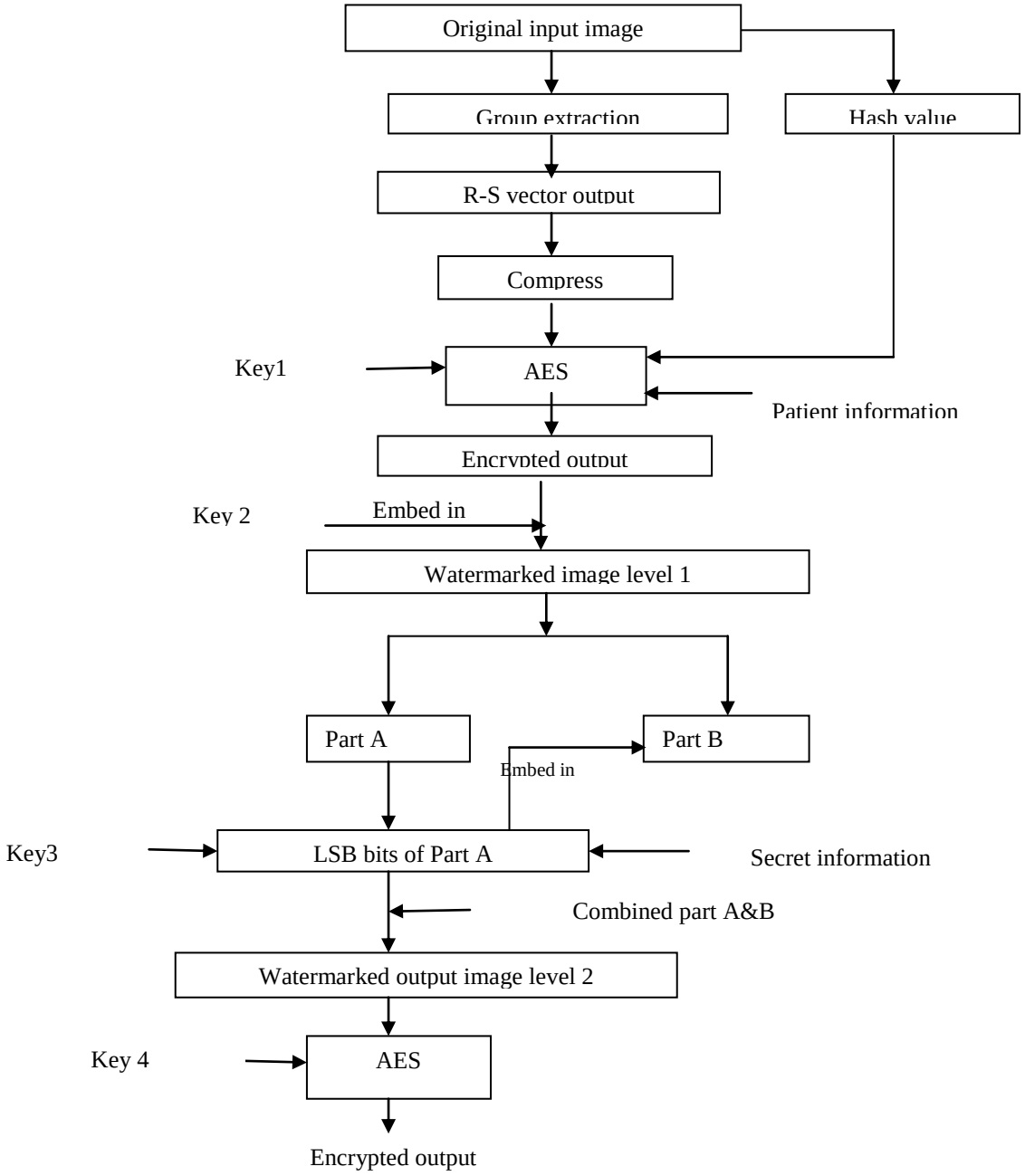


Figure 1. Sender Side Algorithm

3.1.4. R-S Vector: The pixels of each group have a single value. Regular group is assigned as 1 and singular group as 0 and unused group as -1. The unused groups are not considered because they are not affected by the flipping function. So the R-S vector contains a stream of bits ones and zeros which comes under either in singular group or regular group.

3.1.5. Compression: R- S vector is compressed by loss less compression algorithm which is used to provide free space for hiding the information. By using loss less compression Huffman's algorithm, the original R-S vector can be restored without any loss and it provides

good compression ratio. Here, this compressed R-S vector output; patient information and hash value of the original image are embedded in original image. The embedding capacity can be calculated as

Information capacity $I_C = R_N+S_N+L$

Where,

- R_N = Number of regular group
- S_N = Number of singular group
- L = length of the compressed R-S vector

3.1.6. MD5 Hash Value: MD5 hash algorithm produces 128 bits, which is expressed in 32 digit hexadecimal number. MD5 hash function is used to verify the image integrity which shows that the received image is same as the original image.

3.1.7. Watermarking Process: MD5 hash value, patient information and loss less compressed R-S vector output are combined and encrypted using advanced encryption standard algorithm with the help of secret keys. Then the encrypted output is embedded in original image which is called as watermarked image.

3.1.8. Image Partitioning Technique: Image partitioning divides an image into two parts, part A and part B to embed more information into that image. Least significant bits of part A are embed into least significant bits of part B to provide free space for embedding information into part A. Then secret information is embedded into least significant bits of part A. In this paper, R-S vector compressed output, patient information, hash value of original image are integrated, encrypted and embedded into original image. This watermarked image is divided into part A and part B. Then least significant bits of part A is embedded into part B and again secret information is embedded into part A. First, the amount of information is embedded with R-S vector output, and then amount of information is embedded into LSB bits of part A after image partitioning. Here, information is embedded twice with the help of secret keys so that more amounts of data can be embedded into an image.

3.2. Receiver Side Algorithm

Step 1: Decrypt the encrypted output by AES to get watermarked output image

Step 2: Divide the watermarked output image into part A and part B

Step 3: Extract secret information from part A

Step 4: Embed LSB bits of part B into part A

Step 5: Using secret key recover the encrypted output

Step 6: Extract patient information, hash value and R-S vector by AES with secret key

Step 7: Decompress the R-S vector and recover the image

Step 8: Calculate the hash value of the recovered image

Step 9: Compare hash value of recovered image to the extracted hash value

Step 10: If both are equal recovered image is original image otherwise image is discarded.

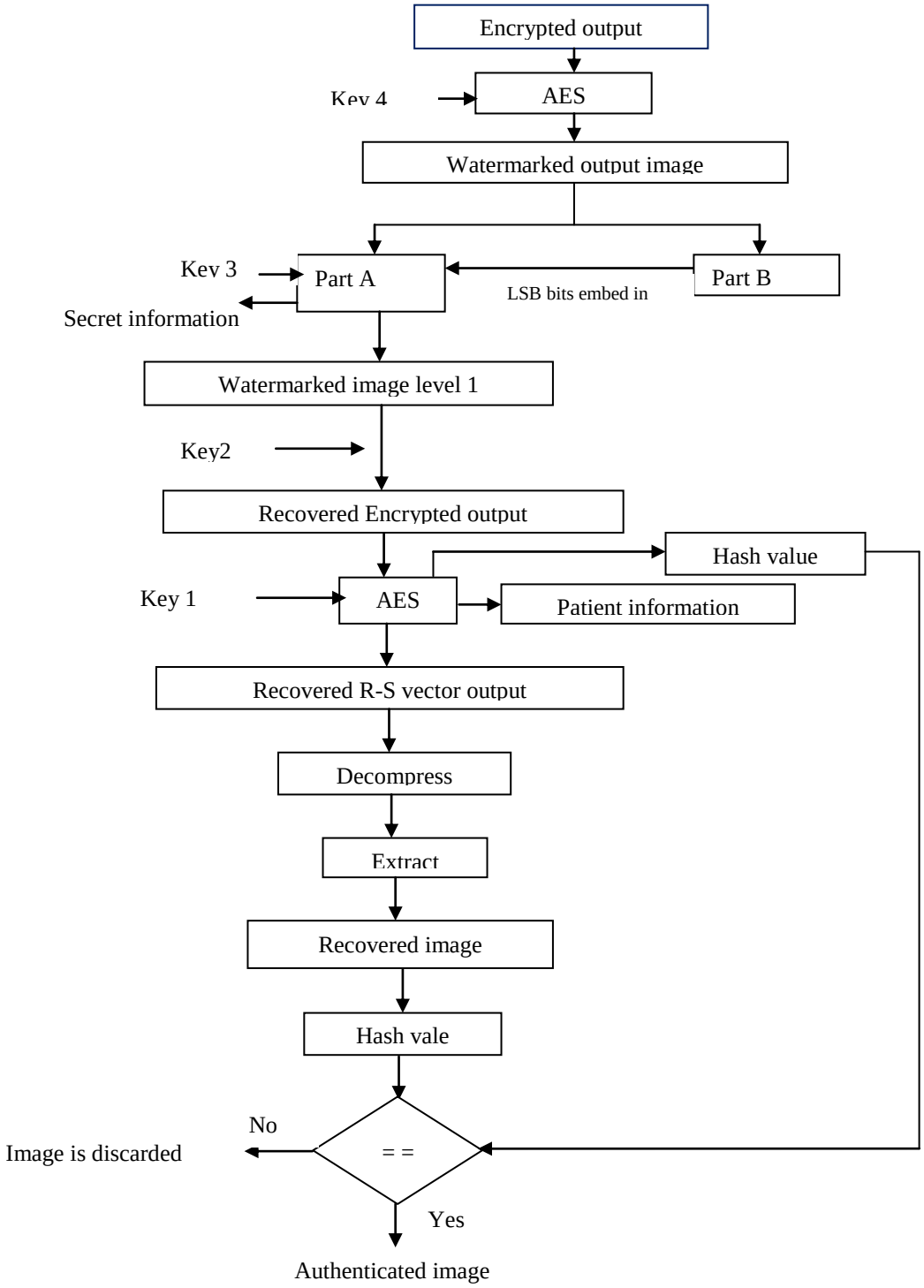


Figure 2. Receiver Side Algorithm

4. Results and Discussion

The size of input image is 200x200 as shown in the Figure 3. The image is divided into groups and each group consists of four pixels which is shown in the Figure 4. The R–S Vector

consists of a stream of bits (zeros and ones), and each bit represents the state of a group of pixels in the image which is shown in Figure 5. Flipping function is used to modify the pixel value by flipping least significant bit which is shown in Figure6. Compressed R-S vector is shown in Figure 7. The MD5 hash value, the compressed R–S Vector of the original image and patient information are combined and encrypted using AES encryption technique with help of secret keys and embedded into the original image which is the watermarked image is shown in Figure 8.

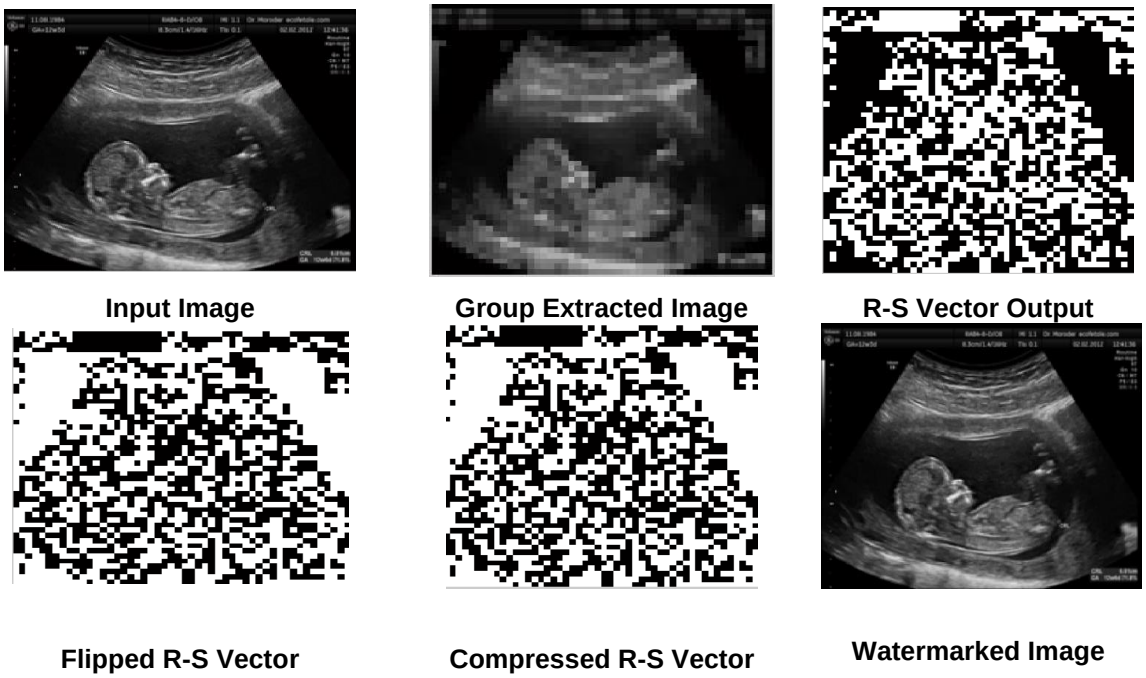
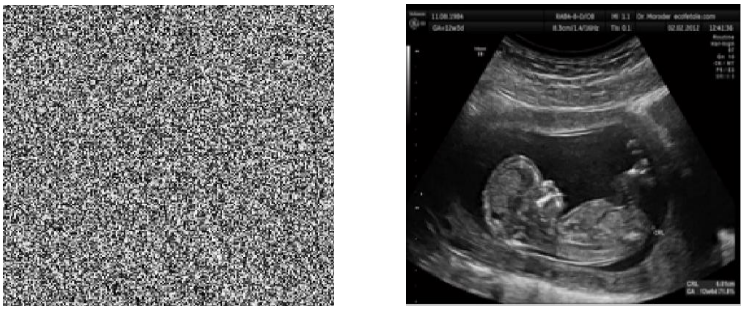


Figure 3. Watermarked Image Using R-S Vector

The watermarked image is divided into Part A and Part B. LSB bits of Part A is embedded into LSB bits of Part B and secret information is embedded into LSB bits of Part A is shown in Figure 9 and Figure 10. Then, Part A and Part B are combined to get a watermarked image is shown in Figure 11. Watermarked medical image is encrypted with help of key using AES (Advanced Encryption Standard) encryption algorithm which is shown in Figure 12. Encrypted and watermarked image is decrypted by performing the reverse operation to get the original image which is shown in Figure 13.



Encrypted image using AES **Decrypted image**

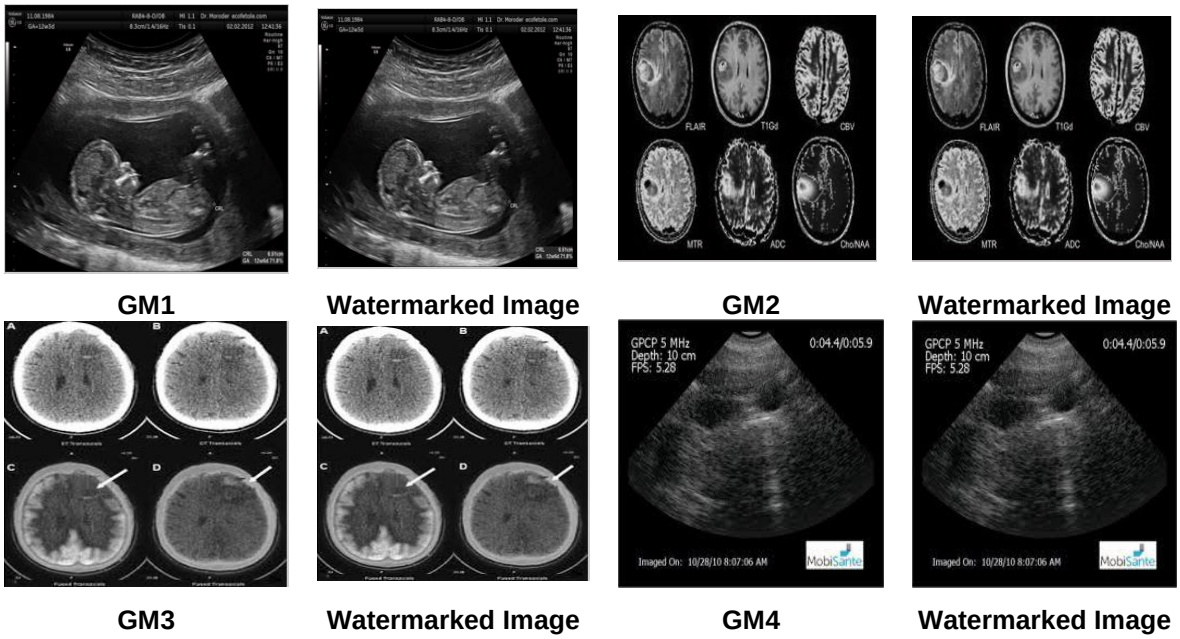
Figure 4. Watermarked Image Using Partitioning Technique

The performance of this system is evaluated by calculating PSNR and Mean Square Error value, which is tabulated in Table 1

Table 1. Performance Evaluation

Parameters	Reversible watermarking technique
PSNR	51.8825
MSE	0.4211

The experimental results take different gray scale images as shown in Figure14 and they are performed using R-S Vector with loss less compression and image partitioning technique which gives performance results as shown in Table 2.



GM1 **Watermarked Image** **GM2** **Watermarked Image**

GM3 **Watermarked Image** **GM4** **Watermarked Image**

Figure 5. Sample for Original and Authenticated Gray Scale Medical Images

Table 2.Performance Evaluation

Sample Images	PSNR	MSE
GM1	51.88	0.421
GM2	46.21	1.011
GM3	47.01	0.952
GM4	51.22	0.502

5. Conclusion

In this work, MD5 hash value is calculated from original image and it has 128 bits. It confirms the image integrity which shows that the received image is same as the original image. This technique provides two times to embed secret information; it improves the information embedding capacity which means that double watermark is used. Similarly it uses two times AES algorithm to encrypt the image which provides more security level. So that this method provides more capability to embed large amount of data since lossless image compression and image partitioning techniques has been used. This technique provides high PSNR ratio up to 51.8865 which improves the image quality.

References

[1] X. Deng, Z. Chen, F. Zeng, Y. Zhang and Y. Mao, "Authentication and recovery of medical diagnostic image using dual reversible digital watermarking", Journal of Nanoscience and Nanotechnology, vol. 13, no. 3, **(2013)**, pp. 2099-2107.
[2] K. Kannammal, S. Pavithra and S. Rani, "Double Watermarking of DICOM Medical Images using Wavelet Decomposition Technique", European Journal of Scientific Research, vol. 70, no. 1,**(2012)**, pp. 46-55.
[3] H. C. Chen, Y. W. Chang and R. C. Hwang, "A Watermarking Technique based on the Frequency Domain", Journal of Multimedia, vol. 7, no. 1, **(2012)**, pp. 82-89.
[4] A. Bhattacharya, S. Palit, N. Chatterjee and G. Roy, "Blind assessment of image quality employing fragile watermarking", Senevnth International Conference on Image and Signal Processing and Analysis, Dubrovnik, Croatia, **(2011)**, pp. 431-436.
[5] O. M. A. Qershi and B. E. Khoo, "Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images", Journal of Digital Imaging, vol. 24, no. 1,**(2011)**, pp. 114-125.
[6] N. A. Memon, C. Asmatullah and M. Ahmad, "Hybrid watermarking of medical images for ROI authentication and recovery", International Journal of Computer Mathematics, vol. 88, no. 10, **(2011)**, pp. 2057- 2071.
[7] F. Huang and Y. Feng, "Security analysis of image encryption based on two dimensional chaotic maps and improved algorithm", in Higher Education Press and Springer-Verlag, **(2009)**.
[8] J. H. K. Wu, R. F. Chang, C. J. Chen, C. L. Wang, T. H. Kuo, W. K. Moon and D. R. Chen, "Tamper detection and recovery for medical images using near-lossless information hiding technique", Journal of Digital Imaging, vol. 21, **(2008)**, pp. 59-76.
[9] H.Wang, K. Ding and C. Liao, "Chaotic Watermarking Scheme for Authentication of JPEG Images", in international conference on Biometrics and Security Technologies, **(2008)**, pp. 1-4.
[10] Y. Frauel, A.Castro, T. J. Naughton and B. Javidi, "Resistance of the double random phase encryption against various attacks", Optical Society of America, **(2007)**.
[11] S. C. Liew and J. M. Zain, "Reversible medical image watermarking for tamper detection and recovery", in 3rd IEEE International Conference on Computer Science and Information Technology, **(2010)**, pp. 417-420.
[12] S. Mazleena, S. Ibrahim, F. Ismail and Isnin, "Image Encryption Algorithm Based on Chaotic Mapping,**"** Jurnal Teknologi, **(2003)**, pp. 1–12.
[13] Y. S. Kim, O. H. Kwon and R. H. Park "Wavelet Based Watermarking Method for Digital Images Using The Human Visual System," in IEEE Electronics Letters, vol. 35, no. 6, **(1999)**, pp. 466-468.
[14] J. Huang and Y. Q. Shi, "Adaptive Image Watermarking Scheme Based on Visual masking," IEEE Electronics Letters, vol. 34, no. 8, **(1998)**, pp. 748-750.

