International Journal of Engineering Applied Science and Management
ISSN (Online): 2582-6948
Vol. 3 Issue 1, January 2022

Designing a Secure Watermarking Technique using the ED-DWT for Medical Image

Nikita Malviya[1] and Nikhil Pateria[2]
Computer Science & Engineering, RGPV, Bhopal, Madhya Pradesh, India[1]
Computer Science & Engineering, RGPV, Bhopal, Madhya Pradesh, India[2]
nikitamalviya09@gmail.com[1], nik.sati29@gmail.com[2]

Abstract: The invisible watermark was once a popular way to protect medical imaging for protecting the patient data from copyright infringement. The key contribution of this paper is to accomplish the secure watermarking via ED component over the DWT coefficient and encryption. To generate multi-resolution coefficients, the medical image is deconstructed using the 2nd level DWT transform. Using edge detection on the HH wavelet band, the edge coefficients are computed. Watermark embedding takes advantage of the difference among dilation and edges intensity to provide further robustness. A random key shuffling cipher technique is used to encrypt a watermark image on medical images. The image is recreated just after decryption on receiver side. For both stages, the statistics are presented for the PSNR results and compared to those obtained at a greater level of security.

Keywords: *Image Security, Watermarking, Edge Detection, DWT, Random Key Encryption*

1. INTRODUCTION

Watermarking in the medical field has many practical applications, including tele-diagnosis, tele-conferences among clinicians, and distant learning of medical personnel [1]. Exchanging medical images between clinicians, specialists, and radiologists provides a platform for discussing and consulting diagnostic and therapeutic measures. In this case, the electronic patient report (EPR) and medical images are sent separately to the destination. Using watermarking techniques and integrating the EPR into the medical images will not only guarantee the confidentiality and security of the sent data but also the integrity of the medical images. Furthermore, authentication of watermarks and tampering detection methods can be used to identify the source of medical images and locating the tampered area, respectively.

Due to high imaging density it is essential to design the watermarking method for medical images. The goal of watermarking is to embed watermark data in the medical images without disturbing visual quality. The essential requirements [2] of the medical image watermarking methods are as follows:

1. The watermark must be invisible and must not affect image's visual quality.
2. Watermark must be robust against attacks.
3. Easily reconstructed and should be reliable.
4. Must be statistically irremovable once embedded.
5. Must provide highest level of image security.
6. The hiding capacity of watermarking must be higher.

Thus robust it is still tough task of designing the secure and watermarking method for medical imaging applications. .

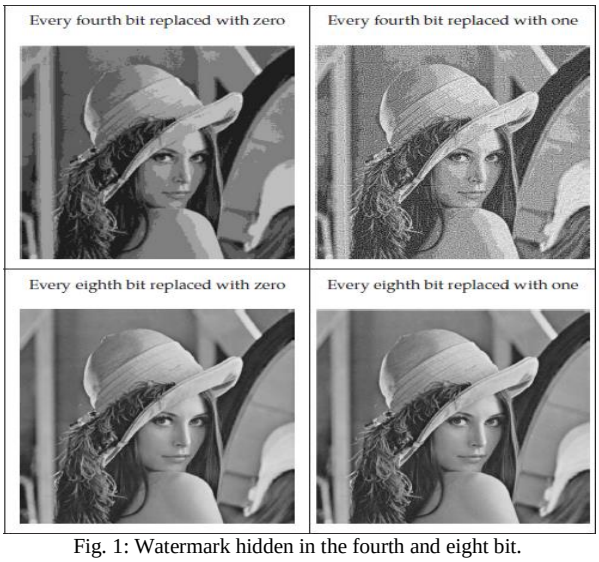


Fig. 1: Watermark hidden in the fourth and eight bit.

A watermark is embedded in the areas of an image in which the human eye is least sensitive, i.e., areas with noise in high frequency sub-bands, including areas with very high or very low brightness, textured areas, and areas near the edges. The following is an example of watermark hiding in a spatial domain. Each pixel contains eight bits, and a watermark hidden in the eighth bit is not visible to the naked eye. Figure 3.1 shows the watermark hidden in the fourth bit and eight bit.

2. CLASSIFICATIONS OF MIW

MIW can also be classified into two types (as shown in figure 2) based on its ability to resist attack; namely, robust and fragile.

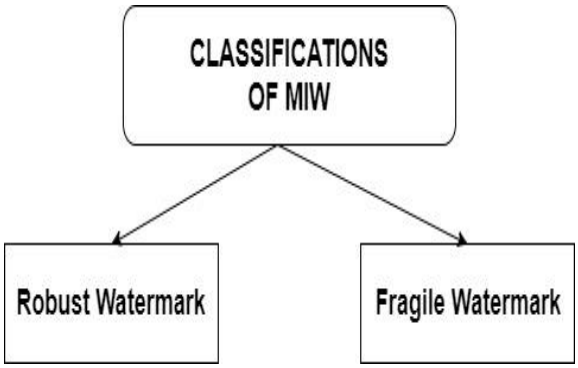


Fig. 2: Classification of MIW.

Robust Watermark- Robust watermarks are resistant to some image processing operations like, rotation, scaling, cropping etc. Robust techniques assume the transmission channel is lossless. Hence these methods embed watermark in lossless and lossy environment. As a consequence, robust watermarks can be extracted back even after intentional or unintentional attack. Based on the resilient property these watermarks are used for copy protection and copy right protection [60]. Results shows that the method is robust against attack, however the method lacks tamper detection mechanism.

Fragile Watermark- Fragile watermarks are generally used for content authentication. Fragile watermarks cannot resist attacks. It easily gets modified when host image is distorted. So, it is mainly used for integrity verification. Traditionally checksum and pseudo-random numbers are used as fragile watermarks. Latest techniques deploy cryptographic hash function for embedding. Many fragile watermarking techniques are block based technique and authentication code for each block is computed and embedded in the image. Upon reception the code is extracted for each block and compared with known code. If there is mismatch then the image is tampered.

3. PURPOSE OF MIW

The watermarks are embedded into medical image for three purposes that is shown in figure 3. One is for hiding electronic patient's record (EPR), second one is integrity verification and the last is for authentication.

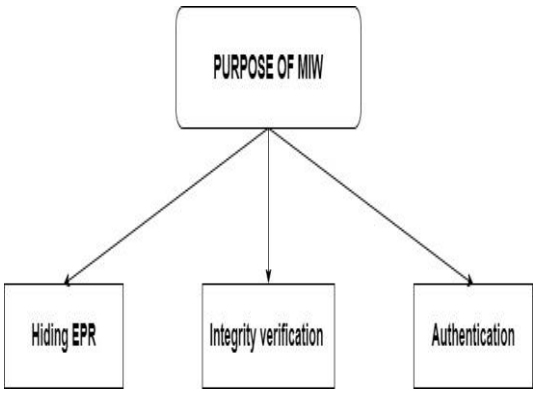


Fig. 3: Purpose of MIW.

EPR hiding watermarks- EPR hiding watermarks aim at reducing the storage space as well as to avoid detachment of image and patients data. When the patient's data and images were stored separately excessive memory is required as well as when transmitted through internet it brings transmission overheads. In order to efficiently use the memory and network bandwidth patient's data can be embedded into image. Patient's demographic data, ECG signal, patient name, ID, sex, age, physician identity etc. can be embedded as EPR into the original image.

Integrity Watermarks- Integrity ensures that the image has not been modified by unauthorized persons. Integrity verification is an analysis process which asks three main questions.

1. Is the image identical to the original image?
2. If it is not, which parts is untrustworthy?
3. And, what is the motive of tamper?

Many techniques for integrity verification have been proposed in the literature which embeds image digest, digital signatures, hash of image etc. Secure hash and signature of different parts of image is embedded as watermark. Knowledge digest is also used for integrity verification.

Authentication Watermarks- Medical images are of paramount importance for its use in diagnostic, education and research. Fragile watermarks are usually employed for authentication purpose, which identifies the source of the image. Upon reception the legitimate recipients of the marked image can verify the authenticity by checking the presence of source watermark. If the watermarked image is

tampered then the embedded watermark is undetectable and the recipient can understand that the image is not trustworthy.

4. APPLICATIONS OF MEDICAL IMAGE WATERMARKING

Medical Image watermarking has been used for different applications like copyright protection, tele-medicines, biometric authentication, data tempering, medical transcription, Compact Storage, Saving Bandwidth, avoiding as discussed below. An example of the various applications of the medical image watermarking is presented and shown in the Figure 4.

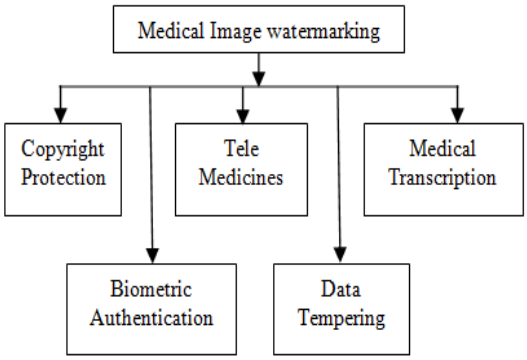


Fig. 4: Usual applications of medical image watermarking.

These applications are used for data authentication and protection purpose for medical imaging data.

Huge amount of medical images are generated every day. Generation and managing the medical data is a challenging task faced by radiologist. In many hospitals electronic patient's record (EPR) and medical images are stored separately. Requirement for memory for storage of images and patient record may increase rapidly. Hence embedding the EPR in the patient's images may save lot of memory. And also if EPR and medical images are stored separately there is a chance for disconnection of patient data and image. Isolation or misplacing of patient data may create a problem in diagnosis which may lead to loss of money as well as life. To avoid segregation of EPR and medical images, watermarking technique has been introduced to embed patient data & related information in the image itself. Transmission of multimedia data involves high bandwidth usage. Bandwidth is an important resource in network environment. Integration of EPR and the medical image saves the bandwidth requirement rather than sending EPR separately and medical image separately [74]. Hospital Information Systems (HIS) and Picture Archiving and Communication Systems (PACS) retrieve images based on querying mechanism. As the communication of medical images extends beyond private network, there is a chance for casual or malicious tampering of medical image. Hence confidentiality and security of medical data is of paramount significance in medical data management systems.

No patient likes to expose his/her medical report to public. Hence by imperceptibly embedding EPR data with advanced encryption techniques confidentiality and security may be maintained. To detect tampering, fragile watermarking techniques have been proposed. Fragile watermarking techniques embeds watermark that easily gets distorted in case on modification. Such watermarks can be used to authenticate the content. Works based on fragile watermarks even identifies the tampered regions, extent of tampering and even determines whether the data is truthful or not [27],[46].

Digital watermarks embed EPR in the image such that bandwidth and memory are utilized efficiently and effectively. It also provides a mechanism for storage of diagnostics data permanently into the image]. Access to the images is made by proper keys only. For this reason watermarking is rising as a prospective tool for access control mechanism since different keys may disclose dissimilar information.

5. EDGE DETECTION (ED)

The aim of the Digital Watermarking (DWM) in transform domain is to insert the max possible watermark signal without perceptually affecting image quality, so that the watermark must remain present as imperceptible and robust. A number of watermarking techniques exist in transform domain based on aspects of the human visual system, properties of signal transforms noise characteristics, properties of various signal processing attacks. Although issues such as visual quality, robustness, and real-time constraints can be accommodated, a single transform based watermarking is not able to satisfy diverse criteria desired for watermarking. In most cases, there is an inherent trade-off and some of the goals are achieved at the cost of others. The requirements such as imperceptibility with respect to payload capacity and robustness of watermarking system contradict each other. In order to increase the robustness, the payload should be increased which decreases the imperceptibility and fidelity of the image. The incorporation of imperceptibility and robustness simultaneously in watermarking system design is an issue that needs to be addressed. Many watermarking techniques analyze the images in order to identify the payload capacity of original image that would hold the watermark data in an imperceptible way with robustness.

The goal of these techniques is to exploit out the characteristics of the Human Visual System (HVS). They exploit the fact that HVS is less sensitive to distortion around edge and textured areas of the image compared to distortion in smooth area. The edge detection is the first step in extracting features of an image. An edge in an image is a contour across which the brightness of the image changes abruptly. In image processing, an edge is often interpreted as one class of singularities.

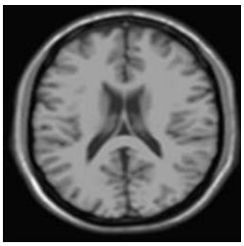


Fig. 5: Edge detections Example of CT scan image.

Fig. 6: Edge detections Example of Sobel edge detected image.

In the function, singularities can be characterized easily by the discontinuities where there gradients approaches to infinity. However, image data is discrete, thus in the discrete domain the definition of the edges in an image often is defined as the local maxima of the gradient.

Edge detection is an important task in image processing. It is a main tool in pattern recognition, image segmentation, and scene analysis. An edge detector is basically a high pass filter that can be applied to extract the edge points in an image. Edge detection refers to the process of identifying and locating sharp discontinuities in an image. The discontinuities are abrupt changes in pixel intensity which characterize boundaries of objects in a scene. Classical methods of edge detection involve convolving the image with an operator (a 2-D filter), which is constructed to be sensitive to large gradients in the image while returning values of zero in uniform regions. There are an extremely large number of edge detection operators available, each designed to be sensitive to certain types of edges. Variables involved in the selection of an edge detection operator include Edge orientation, Noise environment and Edge structure. The geometry of the operator determines a characteristic direction in which it is most sensitive to edges. Operators can be optimized to look for horizontal, vertical, or diagonal edges. Edge detection is difficult in noisy images, since both the noise and the edges contain high frequency content. Attempts to reduce the noise result in blurred and distorted edges. Operators used on noisy images are typically larger in scope, so they can average enough data to discount localized noisy pixels. This results in less accurate localization of the detected edges. Not all edges involve a step change in intensity. Effects such as refraction or poor focus can result in objects with boundaries defined by a gradual change in intensity [1]. The operator needs to be chosen to be responsive to such a gradual change in those cases. So, there are problems of false edge detection, missing true edges, edge localization, high computational time and problems due to noise etc.

There are many ways to perform edge detection. However, the majority of different methods may be grouped into two categories:

1. Gradient- The gradient method detects the edges by looking for the maximum and minimum in the first derivative of the image.
2. Laplacian- The Laplacian method searches for zero crossings in the second derivative of the image to find edges. An edge has the one-dimensional shape of a ramp and calculating the derivative of the image can highlight its location.

6. ED USING SOBEL OPERATOR

The operator consists of a pair of 3×3 convolution kernels as shown in figure 7. One kernel is simply the other rotated by 90°. These kernels are designed to respond maximally to edges running vertically and horizontally relative to the pixel grid, one kernel for each of the two perpendicular orientations. The kernels can be applied separately to the input image, to produce separate measurements of the gradient component in each orientation (call these *Gx* and *Gy*). These can then be combined together to find the absolute magnitude of the gradient at each point and the orientation of that gradient. The gradient magnitude is given by:

$$|G| = \sqrt{Gx^{2} + Gy^{2}}$$

Typically, an approximate magnitude is computed using:

$$|G| = |Gx| + |Gy|$$

This is much faster to compute.

The angle of orientation of the edge (relative to the pixel grid) giving rise to the spatial gradient is given by:

$$\theta = \arctan(Gy / Gx)$$

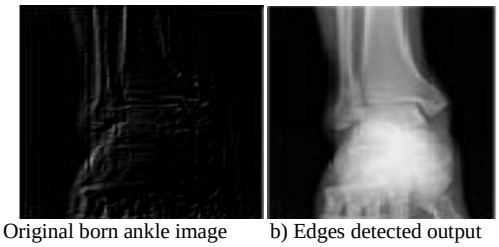
-1	0	+1
-2	0	+2
-1	0	+1

Gx

+1	+2	+1
0	0	0
-1	-2	-1

Gy

Fig. 7: Masks used by Sobel Operator.



(a) Original born ankle image b) Edges detected output

Fig. 8: Example of Sobel operator

The Sobel operator gives much sharper edges then the Prewitt operator as shown in figure 8. Thus is more prone to noise. It can be observed from the figure that the better edges are represented by the conventional Sobel edge operator but better invisibility is provided by the shift invariant operator.

7. PROPOSED METHOD

This research creates a long-lasting and secure encrypted watermarking mechanism in reference to Praveen Kumar Mannepalli et al. [22] for the basic block diagram (as shown in figure 9 and technique of ED and DWT-based watermarking technologies.

The recommended watermarking procedure is carried out in three stages. The first stage is to use an ED coefficient-based watermark embedding.

The deconstructed DWT domain is used to incorporate the watermark. The watermark is formed up of the difference between the edge component of the LL wavelet coefficient and the dilation component, according to the approach of [6].

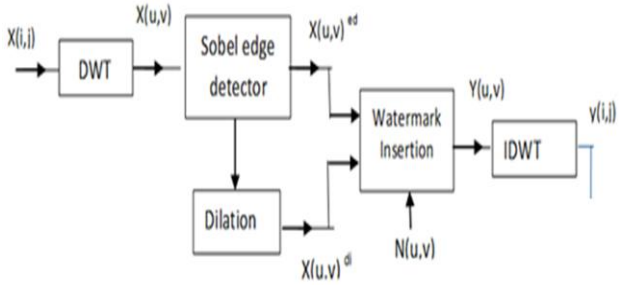


Fig. 9: Ref [6] Process of ED-based Watermark Insertion.

Before being inserted, the cover or host medical image is read and translated to 256 x256 image sizes. An external watermark logo isn't required. In the suggested method, the edge detection (ED) coefficients of the cover medical image are used as the watermark. The paper proposes extracting the low and high pass DWT coefficients from the 2nd level DWT decompositions of the cover medical image. Using the Sobel edge operator, the edge coefficient is determined over LL components. The edge coefficients are utilized to create the watermark using the watermark insertion rule.

5.2.1 Watermark Insertion Rule

In this study, the watermarking is done by following the existing watermark rule.

$$Y(u,v) = X(u,v)^{di} - X(u,v)^{ed}$$

Where X(u,v)(di) represents the dilated edge coefficient and X(u,v)(ed) represents the ED coefficient of the LL sub band of the DWT.

Use the scaling factor alpha to add the watermark features to improve the invisibility. Increasing invisibility is as simple as changing the scale factor. This is how the watermark appears:

$$W = (1-\alpha) * (Y) + \alpha N_{x,y}$$

N (x,y) represents the AWGN noise. It is proposed that the watermark be hidden in the LL sub-band of the DWT of the cover image. The watermarked image is an IDWT image of the cover image.

$$W_E = \mathrm{LL}^{\mathrm{L}}_{x,y} + \mathrm{W}(x,y)$$

This watermark is incorporated within the image and is therefore not visible in the watermarked image.. The watermark basically is extracted from the embedded images using the identical process on the receiver side.

The design of the random key generation based crypto cipher encryption method implemented over the watermarked image is a major contributor to the research. The following is the sequential process for random key based AES encryption:

1. The input for encrypting using cipher text random key is a watermarked image based on the ED-DWT technique.
2. The key generation procedure is started by scanning the size of the input image.

$$n = r * c * 8$$

This assumes that the image is 8 bits wide.

3. Create a random key in binary form as follows.

$$x_N = 1 - 2 * (bin(x_N) - 1)^2$$

4. Encode the picture by bitwise Xoring the key data and the resulting image data row by row.
5. The noise assaults are launched against the encrypted image that has been sent.
6. Decrypting the data with and without attacks is used to rebuild the image.
7. The extraction procedure for watermarks is identical to the extraction procedure.

. Using this standard procedure the image is encrypted and decrypted. The performance of the decrypted image is evaluated under the presence of the attack an example of the Encrypted ad decrypted images is shown in the Figure 10.

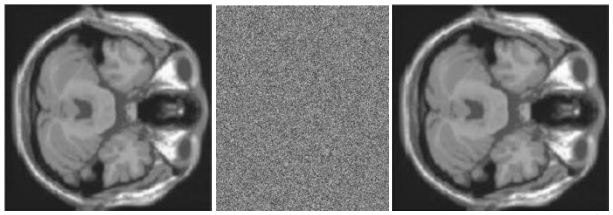
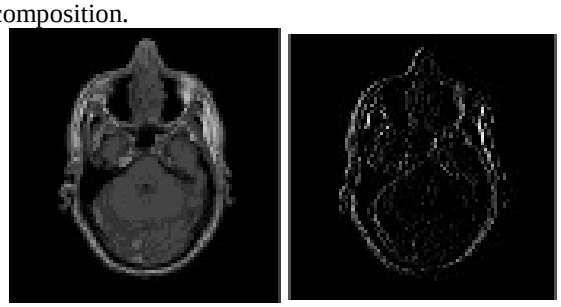


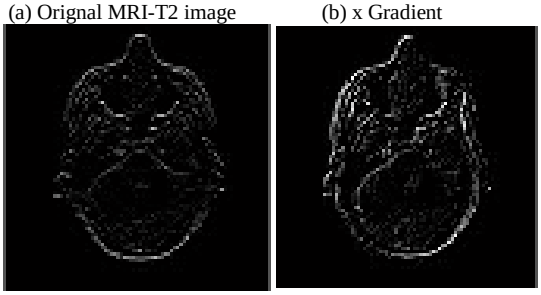
Fig. 10: An example of the image Encryption and decrypted image for MRI_1 image.

8. EXPERIMENTAL RESULTS

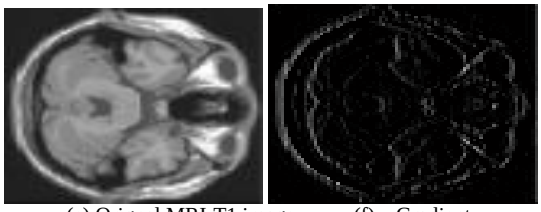
This section initially preseted the calcualted ED results aong with the 2nd level decompositions results over the input edical images. The ED is calcualted usign the Sobel and Prewitt mask as shown in the Figure 11 and 12 respectivlly. And Haar Waelet is used fhe DWT decomposition.



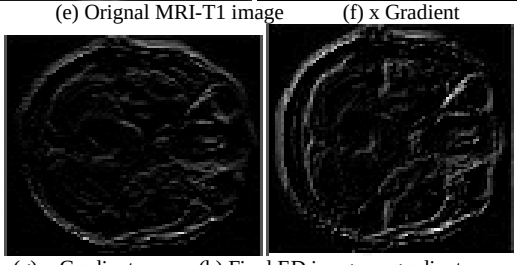
(a) Orignal MRI-T2 image (b) x Gradient



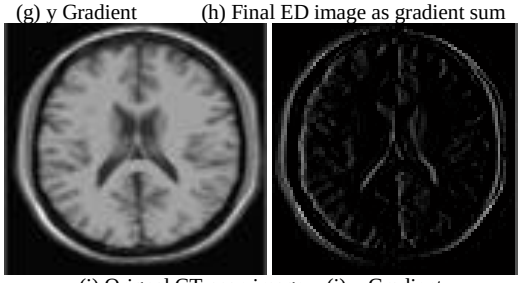
(c) y Gradient (d) Final ED image as gradient sum



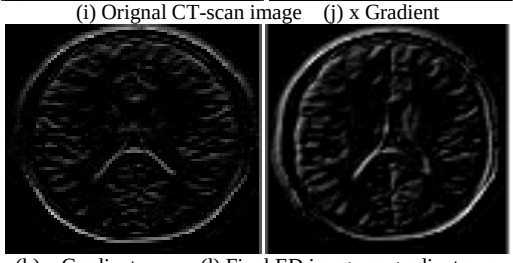
(e) Orignal MRI-T1 image (f) x Gradient



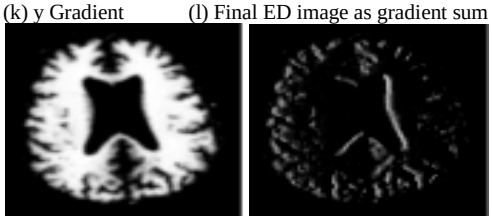
(g) y Gradient (h) Final ED image as gradient sum



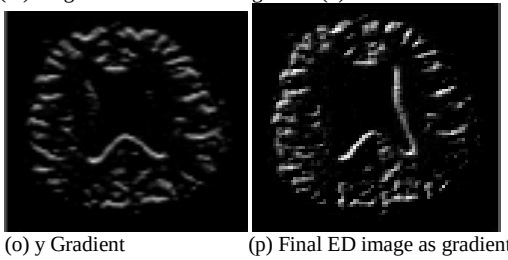
(i) Orignal CT-scan image (j) x Gradient



(k) y Gradient (l) Final ED image as gradient sum

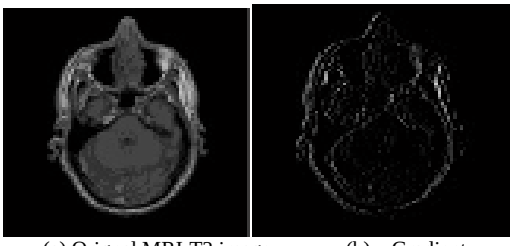


(m) Orignal Brain Tumer image (n) x Gradient

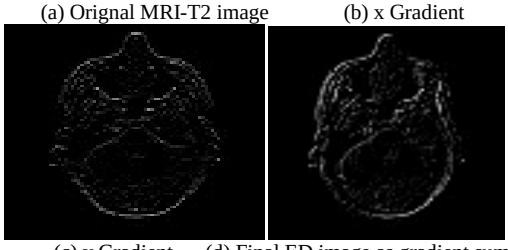


(o) y Gradient (p) Final ED image as gradient sum

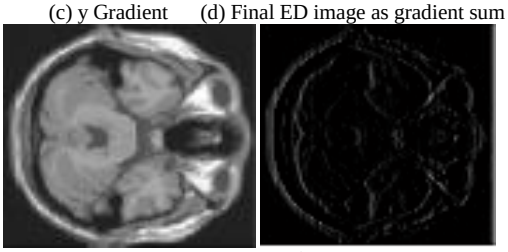
Fig. 11: Result of the Sobel based edge ddetection mask for medical images.



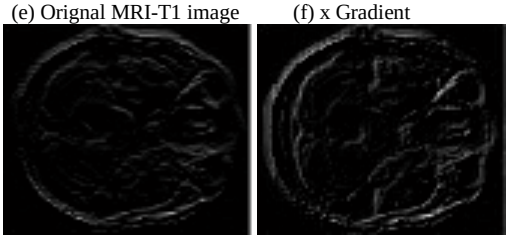
(a) Orignal MRI-T2 image (b) x Gradient



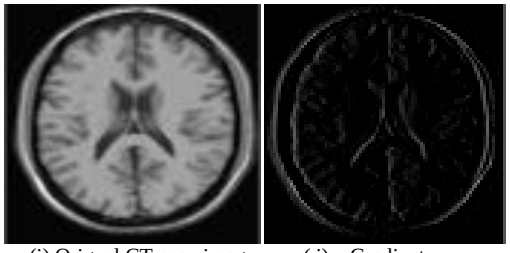
(c) y Gradient (d) Final ED image as gradient sum



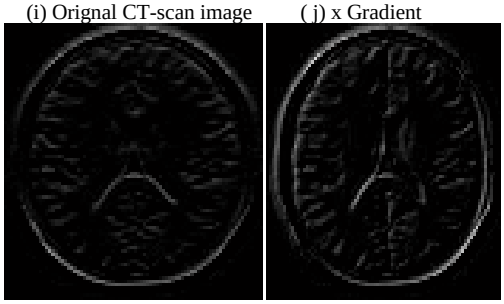
(e) Orignal MRI-T1 image (f) x Gradient



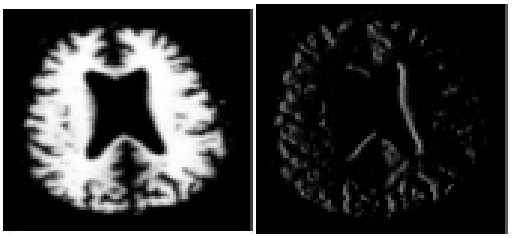
(g) y Gradient (h) Final ED image as gradient sum



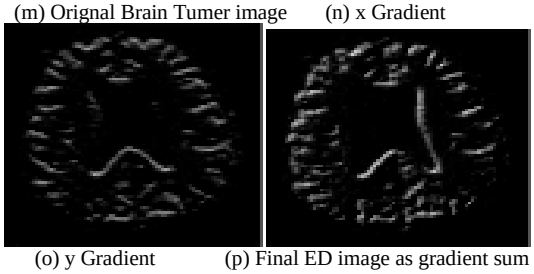
(i) Orignal CT-scan image (j) x Gradient



(k) y Gradient (l) Final ED image as gradient sum



(m) Orignal Brain Tumer image (n) x Gradient



(o) y Gradient (p) Final ED image as gradient sum

Fig. 12: Result of the Prewitt based edge ddetection mask for medical images.

Comparing the Figure 11 and Figure 12 concludes that the Sobel ED mask offers the better enhaced edge features then that of Prewitt ED operator. Thus in this dissertation it is proposed to impliment the watermarking using Sobel mask.

9. RESULTS OF THE ENCRYPTION & DECRYPTION

The results of the Image security using the encryption for the MRI_T1 image are shown in the Figure 6.7. Figure represets comparsion of cipher weights or histrograms. It can be observed from Figure 13 that encryption and decrypted weights are in proximitiy to each other without noise.

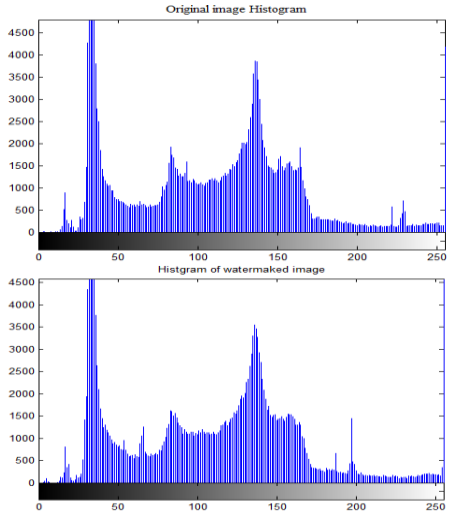


Fig. 13: comparision of cipher weights during watermarking and encryption for MRI_T1.

10. COMPARATIVE RESULT ANALYSIS

This section presents evaluation of our method under the presence of noisy attack. The Gaussian noise is added to the watermarked image and decryption performance is evaluated. The PSNR and the NC is evaluated for the parametric evaluation. The methods perform well enough. The NC without noise is nearly equal to 1 justifies the invisibility.

Table 1: Comparison of PSNR for the watermarking without attacks

Images	Watermarked	Decrypted
MRI_T1	16.6350	15.9782
MRI_T2	16.5209	15.9587
Brain Tumour	18.1007	15.9687

Table 2: Comparison of NC for the watermarking Gaussian noise attacks

Images	Without noise	With noise
MRI_T1	0.9982	0.8716
MRI_T2	0.9893	0.7947
Brain Tumour	0.9985	0.8250

11. CONCLUSION

The secure watermarking is important for protecting the images. Considering these issues, this paper has designed a fast and simple encryption method for the medical images. Paper is designed in two pass, initially in the first pass, the ED-DWT based watermarking method is validated. Then in the second pass, the random key based binary encryption methods using XOR operator is implemented. The qualitative comparison of perfromance of our encryption method and Block chain based encryption method are presented. Maximum value of the NC without noise clearly states the invisibility of watermark. The performance is evaluated under the Gaussian noise and it is found that the NC is relatively in the range of above 80% for all images even under the highly noisy attacks. But in future, it is required to improve the performance of the encryption method under noise.

REFERENCES:-

[1]. Xing Zhang, Seung-Hyun Seo, and Changda Wangm," A Lightweight Encryption Method for Privacy Protection in Surveillance Videos ", Journal of IEEE ACCESS Vol 4 2019.

[2]. Abhinav Shukla, Chandan Singh 'Medical Image Authentication Through Watermarking", International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), Vol. 2, Issue 2, Ver. 2 (April - June 2014)

[3]. Bala B. K, Kumar A. B. The Combination of Steganography and Cryptography for Medical Image Applications. Biomed Pharmacol Journal 2017;10(4)

[4]. M. Jogendra Kumar, N. Raghavendra Sai, R. Vijaya Kumar Reddy, T. Ravi Kumar and A. Pavan Kumar, "Using DWT-DCT-SVD Watermarking For Securing Medical Images," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 1127-1138,

[5]. A. Shankar and A. Kannammal, "A Hybrid Of Watermark Scheme With Encryption To Improve Security Of Medical Images," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 226-233,

[6]. A. Singh, A. Kumar and M. K. Dutta, "DWT, DCT and PBFO based Approach for Biometric Image Security," 2020 International Conference on Contemporary Computing and Applications (IC3A), 2020, pp. 298-303,

[7]. John N. Ellinas, and Panagiotis Kenterlis, "A Wavelet-Based Watermarking Method Exploiting the Contrast Sensitivity Function", World Academy of Science, Engineering and Technology 31 2007

[8]. John N. Ellinas, A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection, Journal on image processing, pp. 197-208 2008

[9]. Ramanand singh, P. Rawat Piyush Shukla, Prashant Kumar Shukla , "Invisible Medical Image Watermarking using Edge Detection And Discrete Wavelet Transform Coefficients", International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume-9 Issue-1, November 2019

[10]. Shaozhang Xiao, Zhengwei Zhang , Yue Zhang, and Changhui Yu "Multipurpose Watermarking Algorithm for Medical Images", Journal of Hindawi Scientific Programming Volume 2020,

[11]. R. Singh, P. Rawat and P. Shukla, "Robust medical image authentication using 2-D stationary wavelet transform and edge detection," 2nd IET International Conference on Biomedical Image and Signal Processing (ICBISP 2017), 2017, pp. 1-8

[12]. Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande, "Modified Advanced Encryption Standard ", International Journal of Soft Computing and Engineering 2014, PP 1-3.

[13]. Mehdi-Laurent Akkar and Christophe Giraud, "An Implementation of DES and AES, Secure against Some Attacks", Springer 2001, pp 309-318.

[14]. S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A New Image

Encryption Algorithm for Grey and Color Medical Images," in IEEE Access, vol. 9, pp. 37855-37865, 2021,

[15]. Sandipan Basu, "International Data Encryption Algorithm (Idea), A Typical Illustration", Journal of Global Research in Computer Science 2011, pp 116-118.

[16]. Raniyah Wazirali, Rami Ahmad, Ahmed Al-Amayreh, Mohammad Al-Madi and Ala' Khalifeh, "Secure Watermarking Schemes and Their Approaches in the IoT Technology: An Overview ", MDPI Journal of Electronics, 10, 1744. 2021.

[17]. Mancy L and Maria Celestin Vigila S, "A survey on protection of medical images," 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2015, pp. 503-506

[18]. G. Singh, "A review of secure medical image watermarking," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017, pp. 3105-3109,

[19]. P. Rana, U. Mittal and P. Chawla, "Medical Images Security Using Watermarking, Hashing and RGB Displacement," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020, pp. 532-536,

[20]. S. B. Sadkhan and A. O. Salman, "A survey on lightweight-cryptography status and future challenges," 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA), Wasit, 2018, pp. 105-108,

[21]. Amna Shifa, Mamoo9na N. Asghar, Martin Fleury, Nadia Kanwal, Mohammad S. Ansari, Brian Lee, Marco Herbst, And Yuansong Qiao, "MuLViS: Multi-Level Encryption Based Security System for Surveillance Videos", VOLUME 8, 2020 IEEEACCESS

[22]. Praveen Kumar Mannepalli, Vineet Richhariya, Susheel Kumar Gupta , Piyush Kumar Shukla Pushan Kumar Dutta "Block Chain based Robust Image watermarking using Edge Detection and Wavelet Transform", Research Square 2021.