Turkish Journal of Computer and Mathematics Education Vol.12 No.13 (2021), 1855-1862

Research Article

Secure And Fragile Watermarking Of Medical Images With Fingerprint Based Biometric Data Using Matlab

Geetha Priya S[1], Harini B[2], Harini Priya R[3], Resmi R Nair[4]

[1]UG Scholar, Department of Electronics and Communication Engineering Easwari Engineering College, Chennai, India
[2]UG Scholar, Department of Electronics and Communication Engineering Easwari Engineering College, Chennai, India
[3]UG Scholar, Department of Electronics and Communication Engineering Easwari Engineering College, Chennai, India
[4]Associate Professor, Department of Electronics and Communication Engineering Easwari Engineering College, Chennai, India.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract

In the modern era, the Internet has turn out to be the primary hub for exchanging information among users. At the same time, data attacks and threats may override the safety of these digital information. Many techniques like watermarking and digital signature are employed to protect these types of information in the field of data processing. Watermarking strategies are carried out in various fields that allows you to guard the content material from unauthorized user. It also assures the user on fact integrity and authenticity, patent evidence and content ownership.Robust watermarking strategies intent to show the patent and the proprietor issues. These strategies have the cap potential to withstand against malware issues like image compression, noise, and change in dimension, etc. However, semi-fragile watermarking, which is also called as soft authenticate, tries to exhibit only the integrity and accuracy of thematerial. This method cannot withstand against the malware attacks.

Keywords: Robust watermarking, Discrete wavelet transform, Minutiae fingerprint extraction

I.Introduction

Some ultra-modern binary image steganographic techniques focus to generate pictures with desirable visible standard. Meanwhile, others cognizance extra at the statistical protection of the anti-steg analysis [1].A binary stenographic technique is described in this paper. A concept of flipped pixels is used in order to improve the image. Initially, a fused distortion measurement is proposed, which combines the two data-carrying pixel position methods while still taking advantage of the advantages of flipping distortion measurement. The edge adaptive grid approach and the "Connectivity Preserving" criterion are the two data-carrying pixel location methods.

The Flipping Distortion measurement (FDM) determines the distortion rating through statistical functions and obtains excessive statistical protection, where the Edge Adaptive Grid (EAG) and Connectivity Preserving Criteria (CPC) analyses the local textures and then selects the pixel. Then, to remove the interference introduced through the flipping of adjoining pixels, an optimization method is suggested to discover higher pixel tossing locations in addition to enhance the steganography performance.Research prove that the steganography technique can produce more potent statistical protection with higher visible standard without reducing the embedding ability [2] – [5].

Steganography is the unique method of communicating confidential information under virtual media in common channels. The process of the uprooting of secret data from the media can be done only by the sender and receiver [9].Images like caricature, signature which comes under binary images have extensive utilisation in our day-to-day life. Steganography in binary images turn out to be highly significant as it is widely being used in facsimile communication. Moreover, 1 and 0 are the only possible two values in a binary image [6] – [7].
In the existing system, an effective watermarking process for greyscale image is put forward. It is implemented with the help of sub-band fusion using stationary wavelet transform algorithm and singular value decomposition algorithm. The purpose of this system is to protect the confidential image information. Since both original image and watermark image has to be visible, decomposition of both the images into sub-bands are done with the help of SWT [3], [8]. Later the concatenation of both bands is computed. On applying Inverse SWT, the resultant computerized image is the remaining cover image of sub-bands.

II.ROBUSTWATERMARKING USING DWT

In proposed system, we will implement task using discrete wavelet transform.The purpose of using DWT is that the watermark is a randomly generated bit. In the second level of DWT decomposition, the watermark is developed into 3 bits and inserted in the low-frequency sub-bands of DWT. The process of embedding is done by combining extended bit multi-scale quantization technique. Using Inverse Discrete Wavelet Transform the image is divided into 3×3 size to find the generated watermark bit matrix in the receiver side. After extracting the watermark, PSNR between the original and the extracted watermarks are calculated. The PSNR is calculated to measure the similarity of image quality.

III. WATERMARK EMBEDDING PROCESS

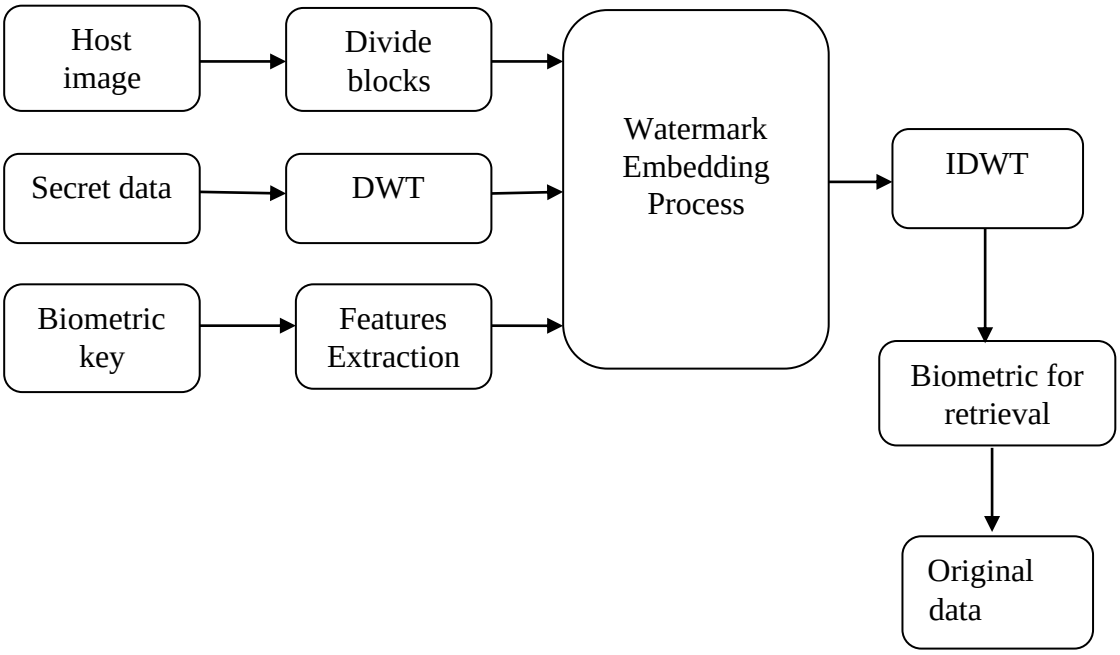

Fig. 1: Watermark Embedding Process

IMAGE ACQUISITION:

The primary phase of any vision framework is the image acquiring stage. Computerized imaging or computerized image acquisition is the formation of a numerically encoded illustration of the visual attributes of an article, like an outline scene or the detailed design of an item. The process of computerized image acquisition includes pre-processing, reduction of pixel size, storing, and displaying the image.After acquiring the image, numerous techniques of processing may be implemented to the image to carry out the various exclusive imaginative and prescient day-to-day optical activities [7].In spite of some useful resource of image enhancement, if the image has now no longer been obtained satisfactorily, then the desired tasks might not be achieved.The use of a digital image is highly advantageous over analog image. This is because, digital image has the capacity to make digital copies indefinitely without degrading the image quality.

DISCRETE WAVELET TRANSFORM:

The mathematical tool for hierarchical decomposition of an image is known as Discrete Wavelet Transform (DWT). The non-stationary signals are processed using DWT in which the keystone is small waves and wavelets that are of varying frequency and limited duration. In this process, temporal information is retained. The translations and dilation of a fixed function are formed by mother wavelet. The suitability of DWT for image watermarking is analysed by this section. Horizontal, vertical and diagonal are the three spatial directions in which the image is decomposed into. Therefore, the anisotropic properties of the HVS are reflected more unequivocally.

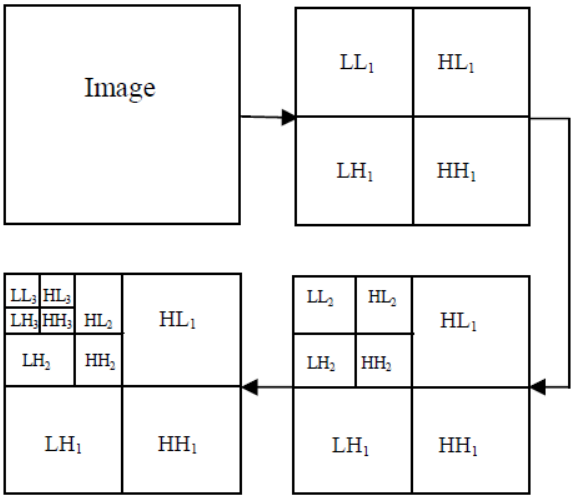

Fig.2: Three level DWT image decomposition

It is efficient in ciphering. It is performed by simple filter convolution. At more than oneresolution level, the image can be reproduced, by adopting multi-resolution analysis. The wavelets enable the image to be represented in terms of coarse overall shape and data ranging from wide to narrow. At minimal band, the magnitude of Discrete WaveletTransform coefficients is large. The higher the value of the coefficient, the more important it is.Watermark detection at lower resolutions is computationally efficient since each successive resolution level involves a smaller number of frequency bands. It's simple to find edge and texture patterns in a photograph using high resolution sub bands.

MINUTIAE BASED FINGERPRINT EXTRACTION:

Minutiae algorithm is extensively used method of fingerprint extraction and its layout has unique characteristics. This technique is considered to be the foundation for various fingerprint recognition systems. In this algorithm, two fingerprints are said to be matched, if their minutiae details match. The minutiae-based fingerprint representation has more advantage over other correlation-based systems, as the former system is predominately accurate and has smaller template size. As a result of the above characteristics, it becomes impossible to retrieve the original from the minutiae details.

In comparison to other algorithm, the minutia point details having corresponding dimensional maps are unique enough to differentiate among fingerprints effectively. This technique also reduces the challenging problem of fingerprint matching to point pattern recognition.The minutiae fingerprint representation systems are also utilized to remove insecurity issues and the point details are sufficient enough to provide finger uniqueness. With respect to image quality and complete distortion, the minutiae-based fingerprint recognition is more effective and efficient when compared to other fingerprint recognition systems.

IMAGE QUALITY ASSESSMENT:

Image quality measurement is essential for most of the image processing applications. Quality of a processed image can be found by comparing the similarities and differences between the original image and the processed image. Qualitative and quantitative analysis can be made to find the quality of the processed image. The distinction between subjective and objective evaluation is that subjective evaluation cannot be integrated into an automated real-time system. Objective tests, on the other hand, are automated and mathematically defined measurements.Also, time consuming andexpensive becomes the added disadvantage to the use of subjective evaluation. Hence, in recent years objective methods have attracted more attention. The two widely usedperformance metrics for quantitative analysis of image quality are the Mean Squared Error (MSE) and the Peak signal-to-noise ratio (PSNR). They both are very easy and simple to implement.

Because of inherent physical limitations, the quality of photographs and videos may degrade clearly from the point where they are filmed to the point where they are displayed, image quality measurement is a critical phase in image processing systems.The systematic design of coding, communication, and imaging systems can be improved or tailored to the desired level of service at a minimal cost by identifying those who have the highest sensitivity to these distortions.

Mean Squared Error (MSE):

The evident method of measuring the closeness among the host image and modified image is to evaluate a difference signal which is the square of the difference between the modified signal to that of the original signal, and then determine the mean value of the error signal. TheMSE is extensively used and easiest method for comparing the image quality.

This standard is commonly deployed in signal processing and the equation is as follows:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j) - y(i,j))^2$$

x(i, j) denotes the original image signal; y(i, j) denotes the processed image signal; pixel dimension of the M×N image is given as i and j. If x(i, j) = y(i, j), then MSE=0.

Peak Signal to Noise Ratio (PSNR):

The value of PSNR is usually expressed in terms of Decibels. The PSNR quantity varies inversely as Mean Squared Error.

The formula for determining the PSNR is given as follows:

$$PSNR = 10\log_{10}\frac{(2^n - 1)^2}{\sqrt{MSE}}$$

IV. RESULTS AND DISCUSSION:

A constructive watermarking method is described by way of producing the watermark over the host image. The DWT based frequency analysis approach is implemented to conceal the data. The MATLAB environment- user friendly is employed to implement the work. The received outcomes show the effective data storage and retrieval. The evaluation of work here is achieved under MSE and PSNR values. The benefit of using MATLAB simulations is that it simplifies the complexity of pre-processing and improves the accuracy of the characteristic extraction.

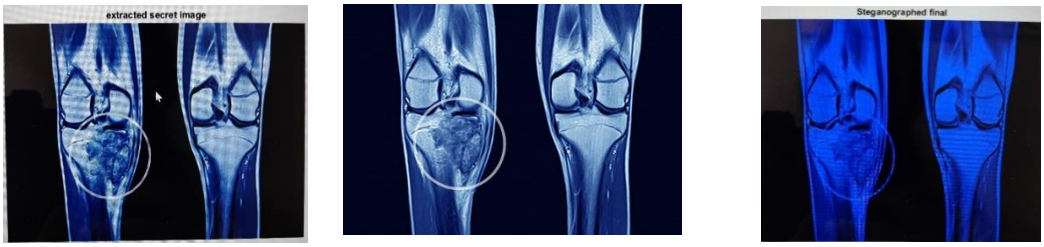

Fig3(a) Host Image **Fig3(b) Watermarked Image** **Fig3(c) Recovered Image**

Fig .3: Experimental results of watermarking on X-Ray images

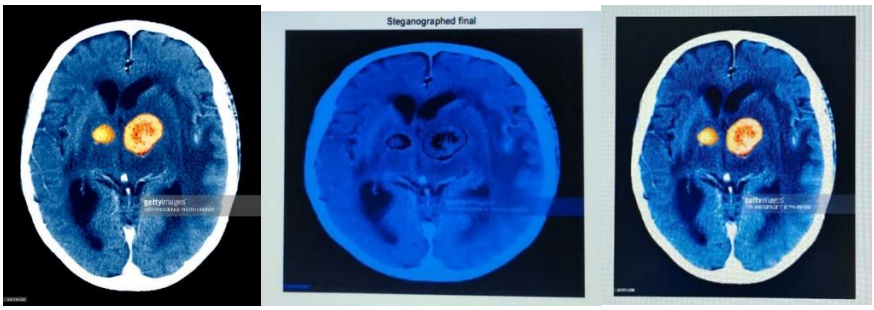

Fig.4(a): Host Image **Fig.4(b): Watermarked Image** **Fig. 4(c): Recovered Image**

Fig. 4: Experimental results of watermarking on MRI Brain Scan images

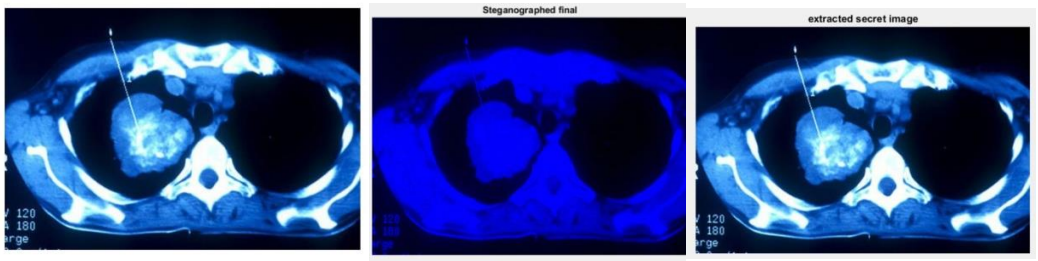

Fig5(a): Host Image Fig5(b): Watermarked Image Fig5(c): Recovered Image

Fig.5: Experimental results of watermarking on lung cancer diagnostic image.

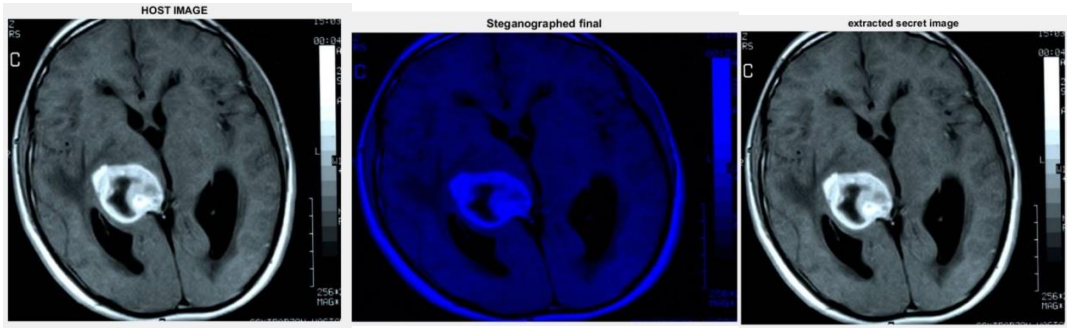

Fig6(a): Host Image Fig6(b): Watermarked Image Fig6.(c): Recovered Image

Fig6: Experimental results of watermarking on right Thalamic glioma MRI image

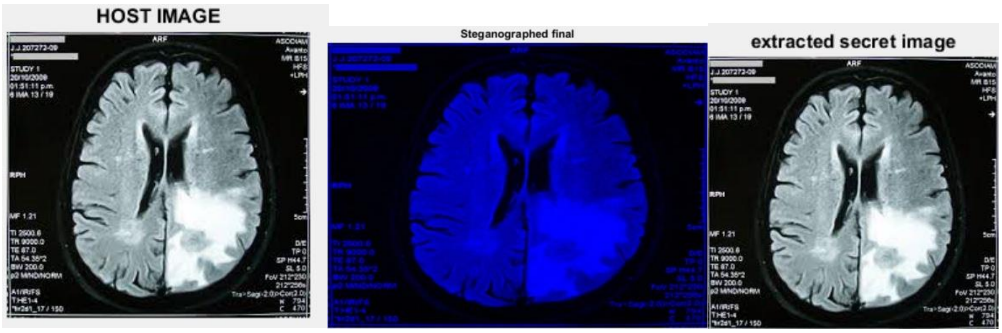

Fig7(a): Host Image Fig7(b): Watermarked Image Fig7(c): Recovered Image

Fig7: Experimental results of watermarking on brain tumor diagnostic image

Table I: PSNR & MSE values of recovered medical images.

Image	**3Level DWT MSE**	**3Level DWT PSNR**
Knee X-Ray image	0.0582	14.022
MRI Brain Scan image	0.0833	12.730
Lung cancer diagnostic image	0.0236	16.032
Right Thalamic glioma MRI image	0.0267	15.759
Brain tumor diagnostic image	0.0127	19.035

Table I gives the PSNR and MSE values of recovered images obtained after de-watermarking. The image quality of the processed image is assessed by determining the PSNR of the image.

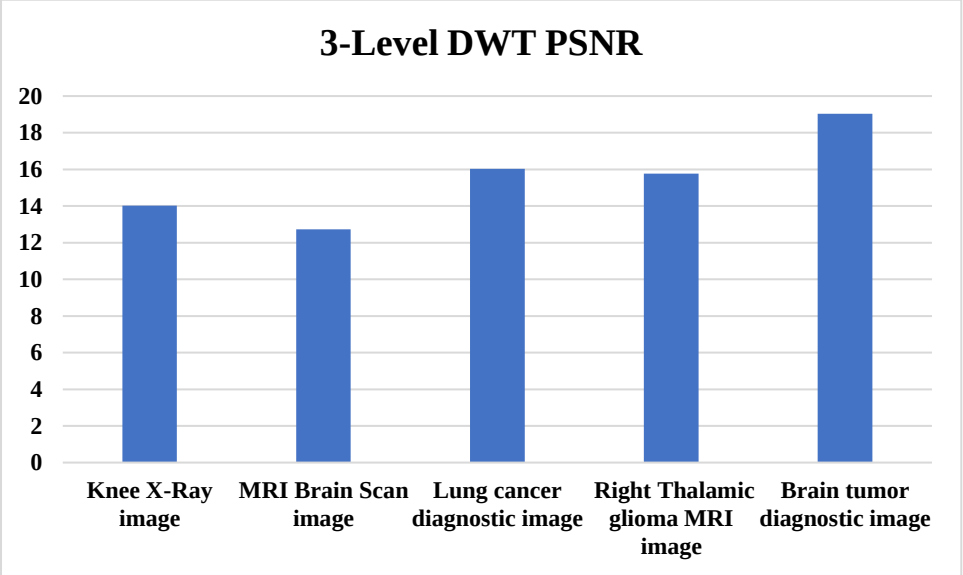

Fig. 8.1: PSNR values for different test images using 3 - level DWT

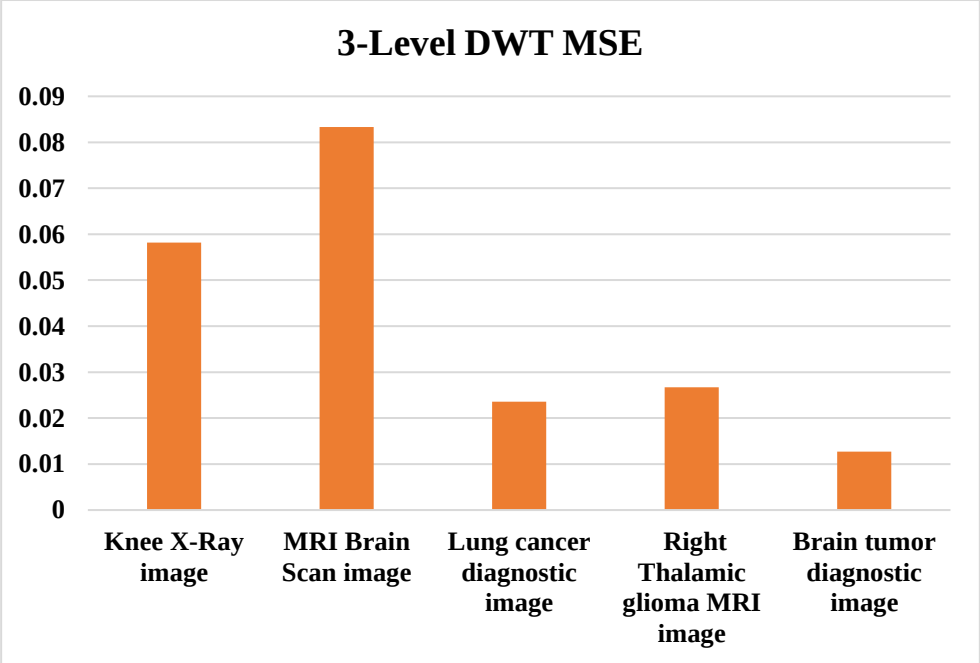

Fig. 8.2: MSE values for different test images using 3 – level DWT

Fig 8.1 and Fig 8.2 shows the graphical representation of variations in MSE and PNNR values for different test images using 3-level DWT.

Fig. 9.1:MRI scan of head

Fig. 9.2:Ultrasound image

Table II: COMPARING – 2 LEVEL & 3 LEVEL DWT BASED ON PSNR AND MSE VALUES

Image	**2-level DWT MSE**	**2-level DWT PSNR**	**3-level DWT MSE**	**3-level DWT PSNR**
MRI scan of head (Fig.9.1)	0.0381	12.649	0.0262	15.8235
Ultrasound image (Fig.9.2)	0.0294	16.437	0.0184	18.9224

Table II compares the PSNR and MSE values determined from the Fig 8.1 and Fig 8.2 recovered after applying 2 level and 3 level DWT on a host medical image. It is seen that the value of PSNR is higher in 3 level DWT than in 2-level. This indicates that the 3 level DWT has higher performance than 2 level DWT.

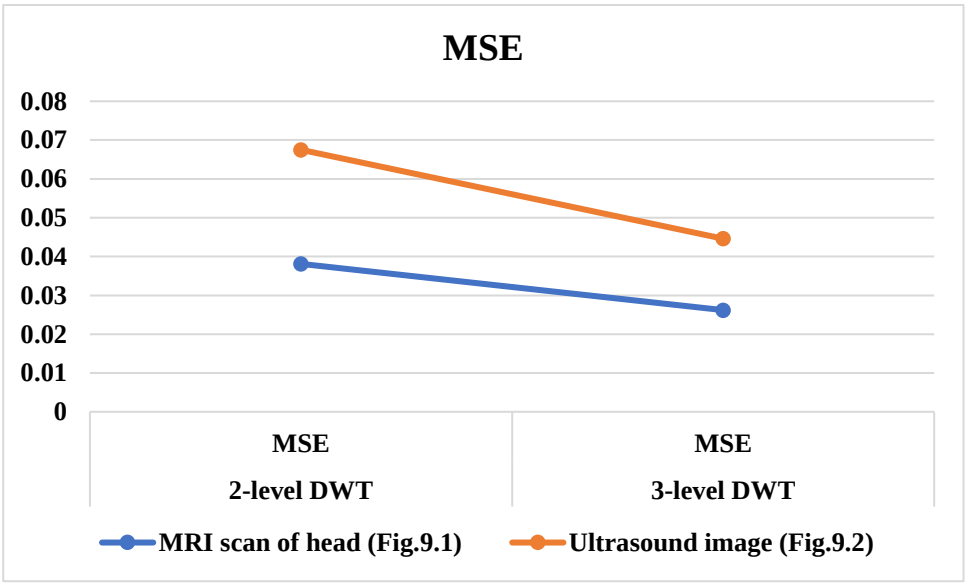

Fig. 10.1: Comparison of MSE for 2-level DWT and 3-level DWT

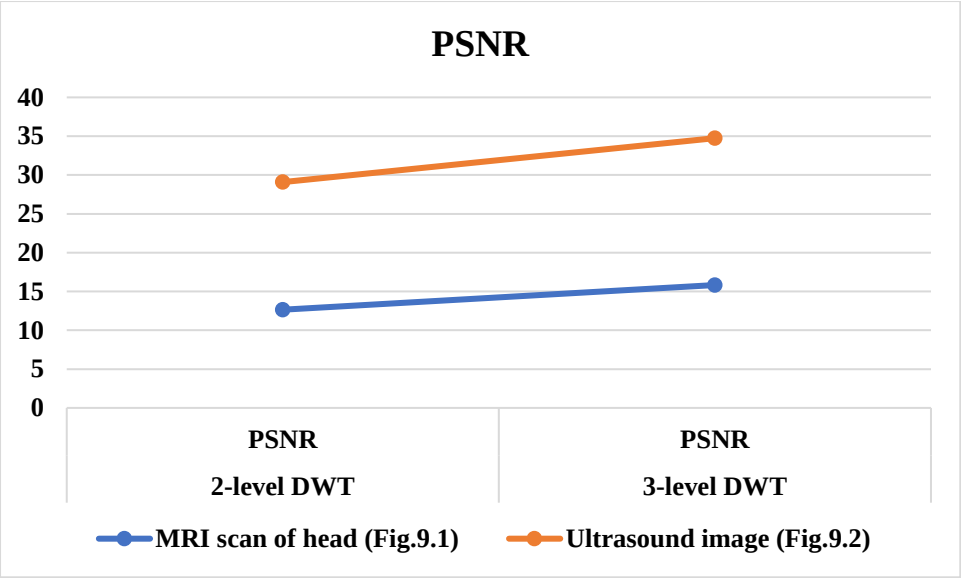

Fig. 10.2: Comparison of PSNR for 2-level DWT and 3-level DWT

Fig 10.1 and Fig 10.2 shows the graphical representation of variations in MSE and PNNR values 2-level DWT and 3-level DWT. From the comparison it is clear that the proposed 3-level DWT outperforms the 2-level DWT.

V. CONCLUSION:

This paper emphasis on 3 level discrete wavelet transforms based watermarking scheme with fingerprint authentication. This watermarking assures the user on facts integrity and authenticity, copyright evidence, content ownership and security for the digital information. The main requirement for a watermark is that it should be highly resistant against intentional and unintentional removal and it has to sustain a good fidelity. These requirements are provided by DWT based image watermarking with the help of biometric authentication.

REFERENCES

[1] E.K. Wong, Q.G.Mei and N.D.Memon,"Data hiding in binary text documents," in photonics West 2001-Electronic Imaging. International Soceity for Optics and Photonics,2001, pp.369-375.

[2] Y.-C. Tseng, H .-K. Pan , and Y. – Y . Chen, "A secure data hiding scheme for binary images,"IEEE Transactions on communications,vol.50,no. 8,pp.1227-1231,2002.

[3] BLiu and M.Wu, "Data hiding in binary image for authentication and annotation",IEEE Transactions on Multimedia, Vol. 6,no. 4,pp.528-538,2004.

[4] A.C.Kot and H.Yang, "Pattern-based data hiding for binary image authentication by connectivity-preserving", IEEE Transactions on Multimedia,vol.9,no.3,pp.475-486,2007.

[5] A.C Kot, H Lu and J.Cheng,"Secure data hiding in binary document images for authentication," in International Symposium on Circuits and Systems,vol.3.IEEE,2003.

[6]S. Rahardja , H. Yang, and A.C Kot, "Orthogonal data embedding for binary images in morphological transform domain-a high-capacity approach, "IEEE Multimedia, vol. 10,no.3,pp. 339-351,2008.

[7] H.Zhang and M.Guo, "High capacity data hiding for binary image identification", in International Conference on Pattern Recognition.IEEE,2010,pp.1441-1444.

[8] A.C. Kot, H . Cao , "On establishing edge adaptive grid for bilevel image data hiding, " IEEE transactions on Information Forensics' and Security,vol.8,no.9,pp.1508-1518,2013.

[9] Y.Q.Shi,H.Lu and A.C.Kot,"Distance-reciprocal distortion measure for binary document images", IEEE Signal Processing Letters,vol.11,no.2,pp.228-231,2004.

[10] W.Lu,B.Feng and W.Sun, "Secure binary image steganography based on minimizing the distortion on the texture", IEEE Transactions on Information Forsenics and Security,vol.10,n0.2,pp.243-255,2015.

[11] Rahim, R., Murugan, S., Mostafa, R. R., Dubey, A. K., Regin, R., Kulkarni, V., & Dhanalakshmi, K. S. (2020). Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords. Webology, 17(2).