Advanced Medical Image Watermarking Technique of Hiding Patient Information for Medical Image Authentication

Ram Pratap Singh, Mr. Shyam Shankar Dwivedi

Abstract— **Digital Watermarking describes methods of embedding the data into the cover image or host an image. The data which is to be embedded is called watermark. Watermark is the secret message that is embedded into host image, to keep the copyright information inside the host image and prevent it from any unauthorized modifications. There are two types of watermarking namely visible watermarking and invisible watermarking. This medical image watermark technique can avoid unnecessary modification by unauthorized person. In this paper Discrete Wavelet Transform based watermarking scheme is used for medical image watermarking using MATLAB software. The proposed method provides performance metrics better than the existing method.**

The various benchmarks and attacks are applied on the watermarked images to evaluate the performance of the proposed scheme. Experimental results indicate that the proposed watermarking scheme is highly robust and does not degrade the original signal. To minimize the difference between original and watermarked singular values, an optimized-quality formula is proposed. First, the peak signal-to-noise ratio (PSNR) is defined as a performance index in a matrix form. Then, an optimized-quality functional that relates the performance index to the quantization technique is obtained.

The proposed method achieves high values of peak signal to noise ratio (PSNR) of watermarked image and high values of normalized correlation (NCC) of the extracted watermark.

Index Terms— **Image Watermarking; DWT (discrete wavelet transformation) ; Image Extraction; PSNR;MSE;NCC**

I. INTRODUCTION

Digital image watermarking is a method of embedding the data into the cover image or host image. The embedding method can be spatial domain based or transform domain based. In spatial domain based method the watermark content is embedded into coefficients of image transform.

Digital image watermarking is a technique of embedding a secret information (watermark) to a cover image. There are three common requirements for watermarking schemes: robustness, capacity and invisibility. However, there is a trade-off between these requirements. For example, a stronger watermark can be used to increase the robustness, but in this case watermark becomes noticeable. On the contrary, increasing the capacity decreases the robustness. Consequently, one must make a choice between these three requirements according to the application. For telemedicine technique, during the storing and transmission of medical images (i.e. Computed Tomography (CT), Magnetic Resonance Imaging (MRI) and X-ray imaging) the security of the digital data has a critical importance. Furthermore, we need to embed patient's information to the medical image without causing any perceptual changes. So, the perceptual invisibility of the watermarking scheme must be very high to maintain the quality of original medical image [1, 2].

The embedding method can be spatial domain based or transform domain based. In spatial domain based method the watermark content is embedded into coefficients of image transform. The image transform can be either of Discrete Fourier Transform (DFT) [3], Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) [4] [5]. With the different resolution levels, DWT can provide both space and frequency localization and so DWT is more effective when compared to other transform domain watermarking. But transform domain watermarking provides more invisibility than spatial domain watermarking. Medical images or medical information (such as X-Ray images, CT scan, MRI Scan images etc.,) need to be more secure and reliable [6] [7]. The medical information should be secure and prevented from modification by unauthorized person and also replacement of one's report by others. These problems can be resolved by hiding the patient information in the medical images by watermarking approach, so that the doctor can diagnose the medical image and also it is more secure. When the medical image watermarking is done, a special care is needed, so that the medical content is not disturbed or lost. The patient information is embedded into medical image without disturbing the quality or original content of the medical image. [8] [9]

In this study, DWT and LDW based medical image watermarking scheme is proposed. In the proposed scheme, patient's information is embedded to the medical image as a binary watermark. The aim of this study is to embed the patient's information to the medical image without degrading the quality of medical image for personal authentication. At the watermark embedding stage, original cover (medical) image is decomposed by LWT into LL, LH, HL and HH sub-bands. Inverse LWT the watermarked image is obtained

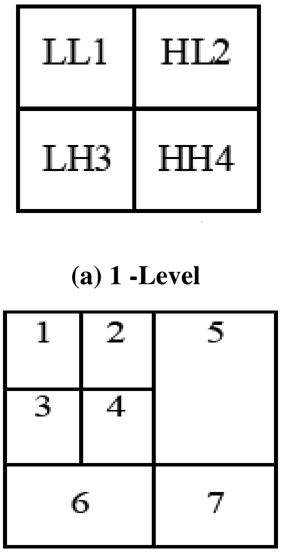
II. DISCRETE WAVELET TRANSFORM (DWT)

Discrete Wavelet Transformation (DWT) [10] of image produces the multi-resolution representation of image. A multi-resolution representation provides a simple hierarchical framework for interpreting the image information. At different resolutions, the details of an image generally characterize different physical structures of the image. At a

Ram Pratap Singh, M.Tech Scholar, Department of Computer Science & Engineering, Rameshwaram Institute of Technology and Management, Lucknow, India.

Shyam Shankar Dwivedi, Associate Professor, Department of Computer Science & Engineering, Rameshwaram Institute of Technology and Management, Lucknow, India.

low level resolution, these details correspond to the larger structures which provide the image content. Wavelet transformation consist of two main steps namely DWT and IDWT (Inverse DWT). DWT segments a digital signal into high frequency quadrant and low frequency quadrants. The low frequency quadrant is split again into two more parts of high and low frequencies and this process is repeated till the signal has been entirely decomposed. In watermarking, generally 1-5 level of decompositions is used. The reconstruct of the original signal from the decomposed image is performed by IDWT. Several types of wavelets exist for decomposition. Generally, application of DWT divides an image into four sub bands (Figure 1a), which arise from separable applications of vertical and horizontal coefficients. The LH, HL and HH sub bands represents detailed features of the images, while LL sub band represents the approximation of the image. To obtain the next coarse level, the LL subband is further be decomposed (Figure 1b), thus resulting in the 2-level wavelet decomposition. The level of decomposition performed is application dependent. The present work considers decomposition up to two levels [11].



(a) 1 -Level

(b) 2-Level

Figure 1: Wavelet Decompositions

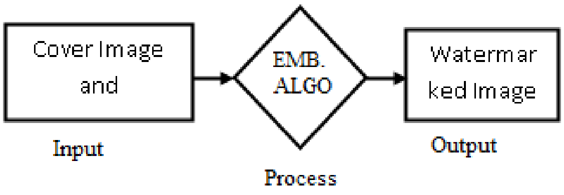
III. PROPOSED METHOD

The proposed watermarking scheme is introduced in this section. The watermark is extracted without the original image.

A. Embedding Algorithm

Input: Cover Image and Watermark Image

Output: Watermarked Image



The patient information or the watermark image is embedded into the medical image as follows-

Step 1: Inverse Discrete Wavelet Transform (IDWT) is applied to the host or original medical image to decompose the image into low and high frequency sub-bands. After performing IWT on the image, four non-overlapping multi-resolution coefficient sets- LL, HL, LH and HH can be obtained.

Step 2: Then, low frequency sub-band (LL) is divided into 3×3 non-overlapping blocks. For each block, the centre pixel is considered as the threshold and the pixels surrounding the centre pixel are considered as the neighbour pixels. Fig. 2 depicts the 3×3 block representation.

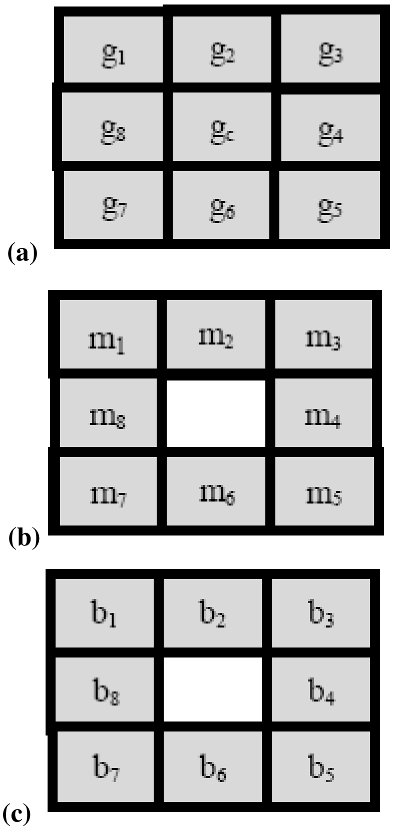


Figure 2: (a) gray values of 3×3 blocks (gi); **(b)** gray differences (mi) and **(c)** binary bits (bi) according to the sign of gray differences.

Step 3: The gray differences between centre pixel and neighbor pixels are calculated. The differences can be obtained by:

$$m_i = g_i - g_c, \qquad (1)$$

Where, i = 1 to 8. m_i are the gray differences, g_i are the gray values of neighbour pixels and g_c is the gray value of the centre pixel

Step 4: According to the sign of the gray differences, binary bits (1 and 0) are assigned as follows:

$b_i = 1$; $if\ m_i \geq 0$

$b_i = 0$; $Otherwise$

Step 5: Logical Exclusive OR (XOR) operation is applied to the bits those are obtained according to the sign of the gray differences. The XOR results can be obtained by:

$$ex = b_1 \oplus b_2 \oplus b_3 \oplus \dots\dots \oplus b_8 \qquad (2)$$

Where, ⊕ indicates the XOR operator and ex represents binary results 0 or 1.

Step 6: The patient information is taken as the binary watermark image. Then, the chaotic watermark is obtained by applying XOR operation between binary watermark image and generated logistic map.

Step 7: Watermark bits are embedded into the blocks of LL sub band, one by one. In other words, one bit of watermark bits is embedded into one block.

Step 8: The bits of chaotic watermark are embedded into each block of LL by observing the neighbour pixels conditions. Let w be one of bits of chaotic watermark. The XOR result (ex) is compared with the value of w. If the value of w is same as the value of ex, the neighbour pixels of the block will be unchanged. If the value of w is not same as the value of ex, one of the neighbour pixels will be modified to make the result of ex consistent with corresponding result of w. This modification of one of neighbour pixels is done by using following steps:

i) At first, the minimum value (min) is calculated from the absolute gray differences (|m_i|).

ii) From the neighbour pixels, the pixel (g_{min}) which gives minimum gray difference is detected. If minimum value is obtained from multiple neighbour pixels, any one of multiple pixels can be used.

iii) Gray value of this detected pixel is modified as follows:

$$g_m = (g_{min} - min) - \beta \quad ; \; if \; b_{min} = 1 \qquad (3)$$

$$g_m = (g_{min} - min) + \beta \quad ; \; if \; b_{min} = 0 \qquad (4)$$

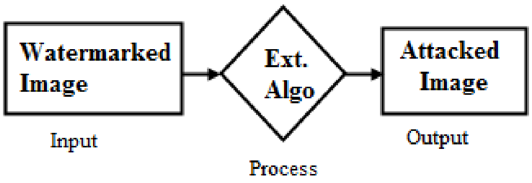
Where, g_m is the modified gray value of pixel g_{min}, which gives minimum gray difference. b_{min} represents the value of binary bit according to the gray difference sign, which is obtained from the difference between g_{min} and g_c. β is the scaling factor.

Step 9: Finally, the watermarked image can be obtained after performing inverse wavelet transform.

B. Extraction Algorithm

Input: Watermarked Image

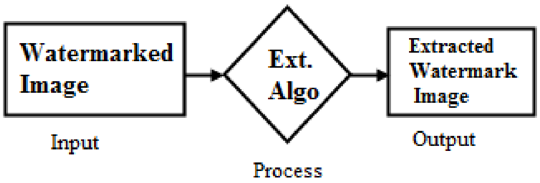
Output: Attacked Image



Step 1: Apply Blur Attack (BA) and Average Attack (AA), Gaussian Attack (GA), Crop Attack (CA) on watermarked image for security and robustness.

Input: Watermarked Image

Output: Extracted Watermark Image



The watermarked medical image as follows-

Step 2: IWT is applied to the watermarked image to obtain low frequency (LL) sub-band of watermarked image.

Step 3: Low frequency sub-band (LL) is divided into 3×3 non-overlapping blocks.

Step 4: Gray differences between centre pixel and neighbour pixels of 3×3 blocks are calculated.

Step 5: Binary bits (1 and 0) are assigned according to the sign of the gray differences. If the gray difference of a neighbour is negative, the binary bit of that neighbour is zero (0). On the other hand, if the gray difference of a neighbour is greater than or equal to zero, the binary bit of that neighbour is one (1). For 8 neighbour pixels, 8 binary bits can be obtained.

Step 6: Logical Exclusive OR (XOR) operation is performed on the binary bits. The chaotic watermark bit can be extracted from the XOR result of the corresponding block.

Step 7: Finally, the watermark image is obtained from the extracted chaotic watermark by applying XOR between logistic map and extracted chaotic watermark

IV. PERFORMANCE PARAMETER

In this thesis, we have used Peak Signal to Noise Ratio (PSNR) and Cross- Correlation (CC) to measure the quality of the images. In order to evaluate the performance of the watermarked images, there are some quality measures such as MSE (mean square error), PSNR (peak signal to noise ratio), and NCC (normalized cross correlation).

The phrase Peak Signal to Noise Ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

The PSNR is most commonly used as a measure of quality of reconstruction in image compression etc. It is most easily defined via the Mean Squared Error (MSE). For two m×n monochrome images I (x, y) and K (x, y), where one of the images is considered a noisy approximation of the other, MSE is defined as:

$$PSNR \; in \; dB = 10log_{10}\left(\frac{255^2}{MSE}\right) \qquad (5)$$

$$MSE = \frac{\sum_i \sum_j (\gamma(i,j) - \gamma(i,j)^2)}{M \times N} \qquad (6)$$

$$NCC = \frac{\sum_i \sum_j (w(i,j) - w(i,j)')}{\sum_i \sum_j (|w(i,j)^2|)} \qquad (9)$$

Here, 255 is the maximum pixel value of the image. When the pixels are represented using 8 bits per sample, value of 2^8 is 255. More generally, when samples are represented using linear PCM with B bits per sample, maximum possible value of 255 is 2B-1. For colour images with three RGB values per pixel, the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Typical values for the PSNR in image watermarking are between 30 and 40 dB.

The correlation coefficient, a concept from statistics, is a measure of how well trends in the predicted values follow trends in past actual values. It is a measure of how well the predicted values, from a forecast model, "fit" with the real-life data. The correlation coefficient is a number between 0 and 1. If there is no relationship between the predicted values and the actual values, the correlation coefficient is 0 or very low. As the strength of the relationship between the predicted values and actual values increases, the value of correlation coefficient also increases. A perfect fit gives a coefficient of 1.0. Thus the higher value of correlation coefficient is better. It indicates the strength and direction of a linear relationship between two random variables.

V. RESULTS

The proposed algorithm has been simulated by using MATLAB software. For proposed watermarking process, different medical images of different sizes have been taken as the cover images and different binary images have been taken as watermark images or different patient information. We have used the following attacks, while watermarking the images

1) Blur Attack
2) Average Attack
3) Gaussian Attack
4) Crop Attack

Original image or input images have a RGB combination. Image processing begins with an image acquisition process. The two elements are required to acquire digital images.

The following figure 3 has been taken to test the system.

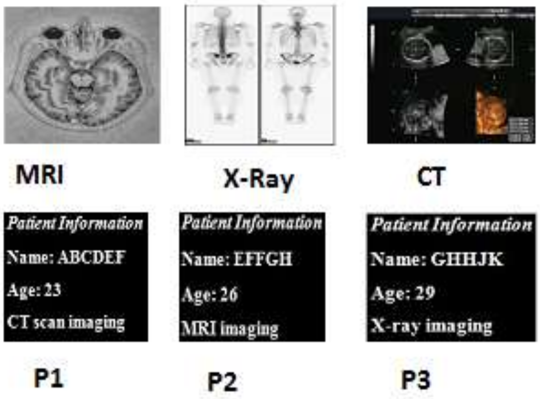


Figure 3 Experimental Dataset

Here in Figure 4, we have taken cover image as MRI image and watermark image as Patient-1 image with Blur attack using ref techniques.

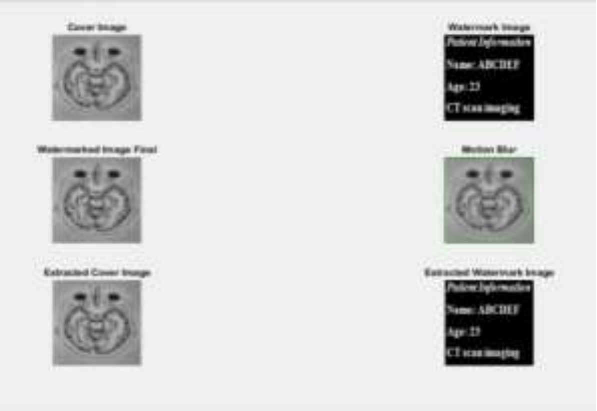


Figure 4: Ref Watermarking Procedure with Blur attack

Here in Figure 5, we have taken cover image as MRI image and watermark image as Patient-1 image with Average attack using ref techniques.

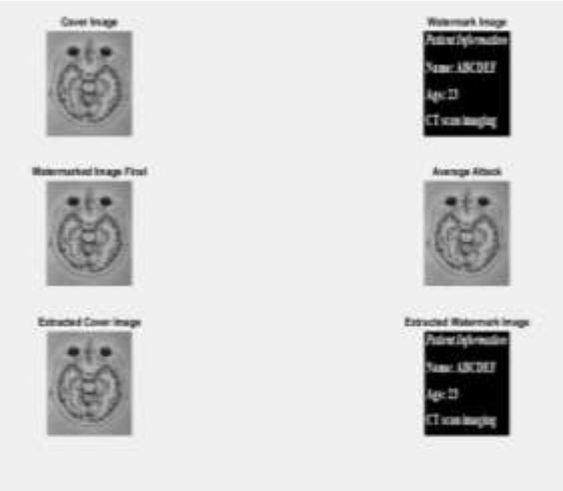


Figure 5: Ref Watermarking Procedure with Average attack

Here in Figure 6, we have taken cover image as MRI image and watermark image as Patient-1 image with Gaussian attack using ref techniques

.

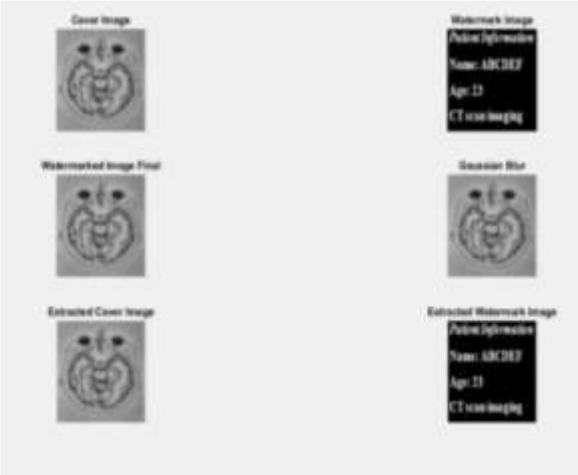


Figure 6: Ref Watermarking Procedure with Gaussian attack

Here in Figure 7, we have taken cover image as MRI image and watermark image as Patient-1 image with Gaussian attack using ref techniques.

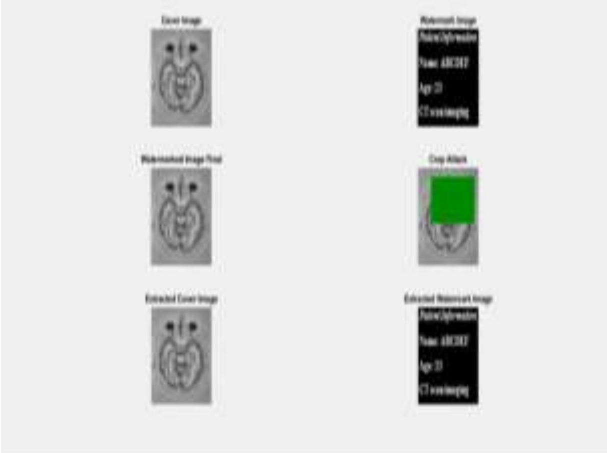


Figure 7: Ref Watermarking Procedure with Crop attack

Here in Figure 8, we have taken cover image as X-ray image and watermark image as Patient-2 image with Blur attack using ref techniques.

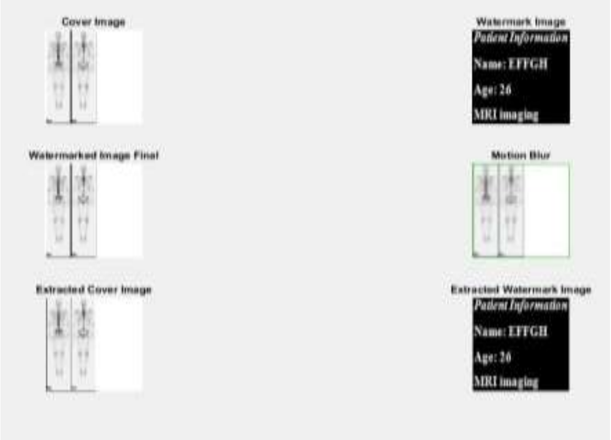


Figure 8: Ref Watermarking Procedure with Blur attack

Here in Figure 9, we have taken cover image as X-Ray image and watermark image as Patient-2 image with Average attack using ref techniques.

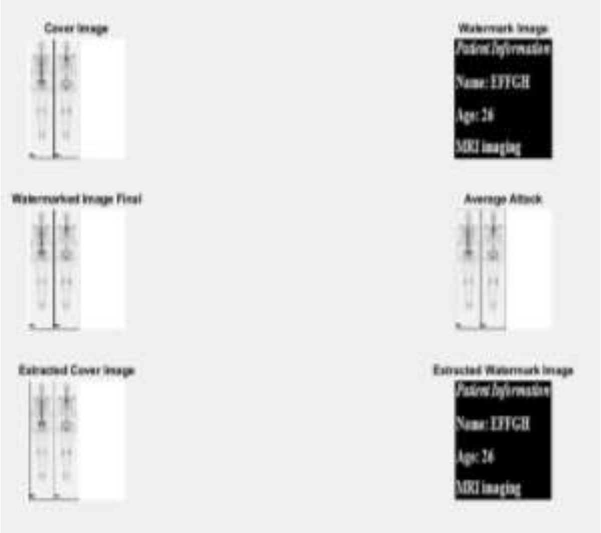


Figure 9: Ref Watermarking Procedure with Average attack

Here in Figure 10, we have taken cover image as X-Ray image and watermark image as Patient-2 image with Gaussian attack using ref techniques.

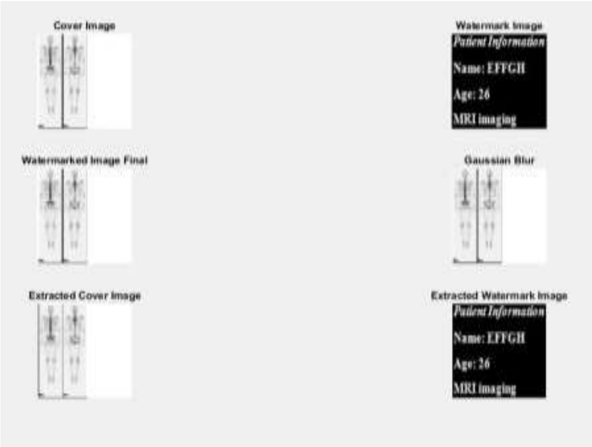


Figure 10: Ref Watermarking Procedure with Gaussian attack

Here in Figure 11, we have taken cover image as X-Ray image and watermark image as Patient-2 image with Gaussian attack using ref techniques.

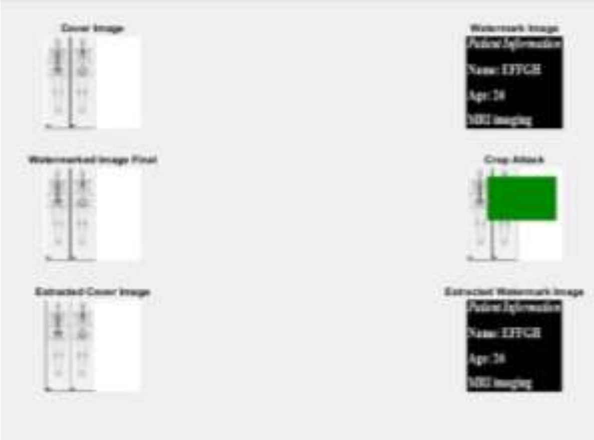


Figure 11: Ref Watermarking Procedure with Crop attack

Here in Figure 12, we have taken cover image as CT image and watermark image as Patient-3 image with Blur attack using ref techniques.

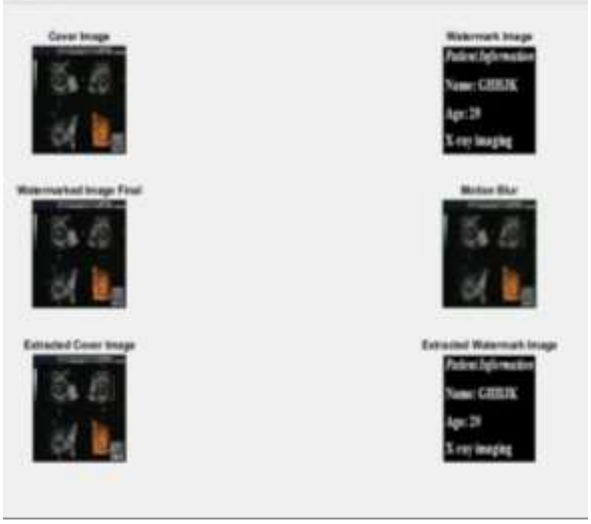


Figure 12: Ref Watermarking Procedure with Blur attack

Here in Figure 13, we have taken cover image as CT image and watermark image as Patient-3 image with Average attack using ref techniques.

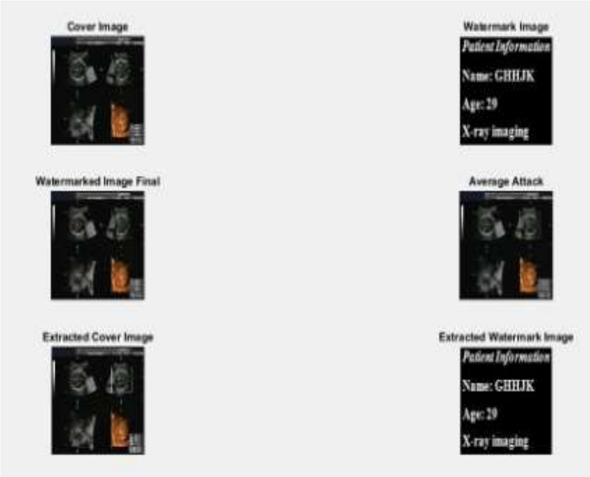


Figure 13: Ref Watermarking Procedure with Average attack

Here in Figure 14, we have taken cover image as CT image and watermark image as Patient-3 image with Gaussian attack using ref techniques.

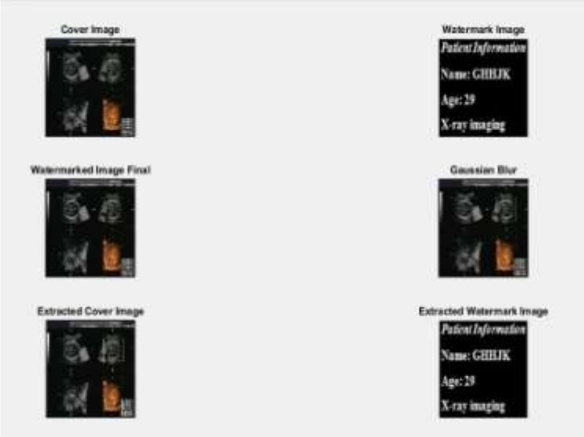


Figure 14: Ref Watermarking Procedure with Gaussian attack

Here in Figure 15, we have taken cover image as CT image and watermark image as Patient-3 image with Crop attack using ref techniques.

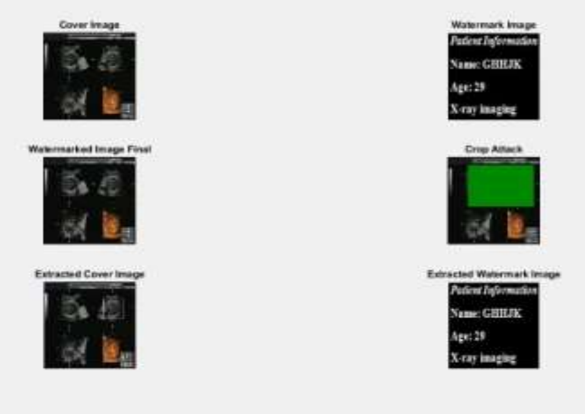


Figure 15: Ref Watermarking Procedure with Crop attack

Here in Figure 16, we have taken cover image as MRI image and watermark image as Patient-1 image with Blur attack using Proposed techniques.

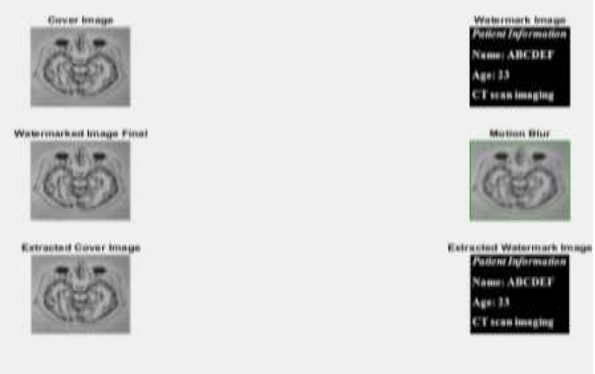


Figure 16: Proposed Watermarking Procedure with Blur attack

Here in Figure 17, we have taken cover image as MRI image and watermark image as Patient-1 image with Average attack using Proposed techniques.

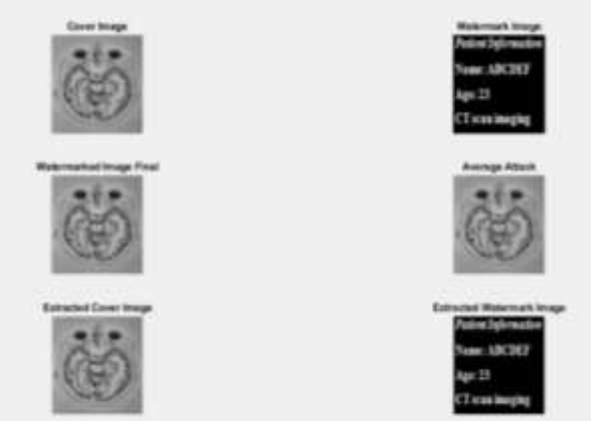


Figure 17: Proposed Watermarking Procedure with Average attack

Here in Figure 18, we have taken cover image as MRI image and watermark image as Patient-1 image with Gaussian attack using Proposed techniques.

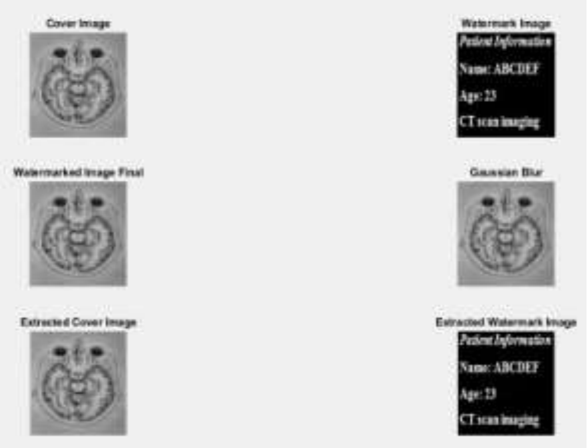


Figure 18: Proposed Watermarking Procedure with Gaussian attack

Here in Figure 19, we have taken cover image as MRI image and watermark image as Patient-1 image with Gaussian attack using Proposed techniques.

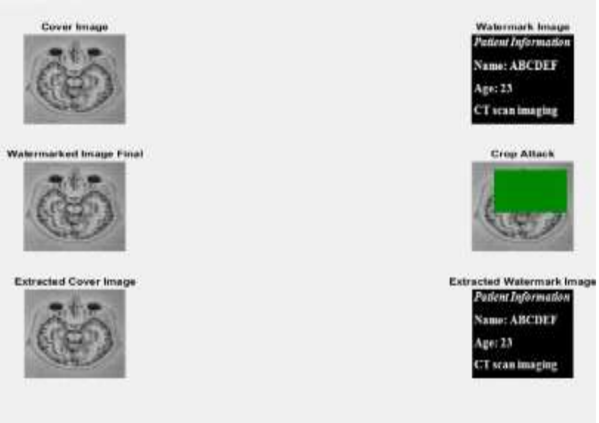


Figure 19: Proposed Watermarking Procedure with Crop attack

Here in Figure 20, we have taken cover image as X-ray image and watermark image as Patient-2 image with Blur attack using Proposed techniques.

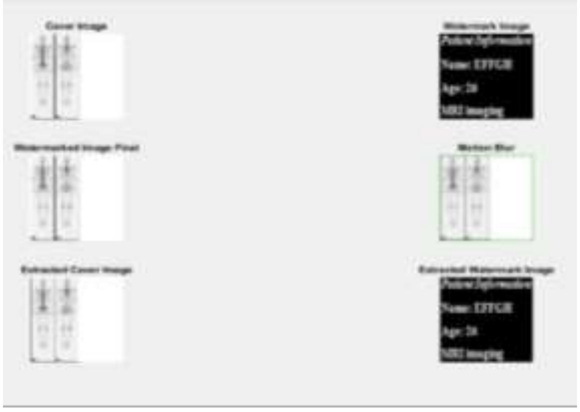


Figure 20: Proposed Watermarking Procedure with Blur attack

Here in Figure 21, we have taken cover image as X-Ray image and watermark image as Patient-2 image with Average attack using Proposed techniques.

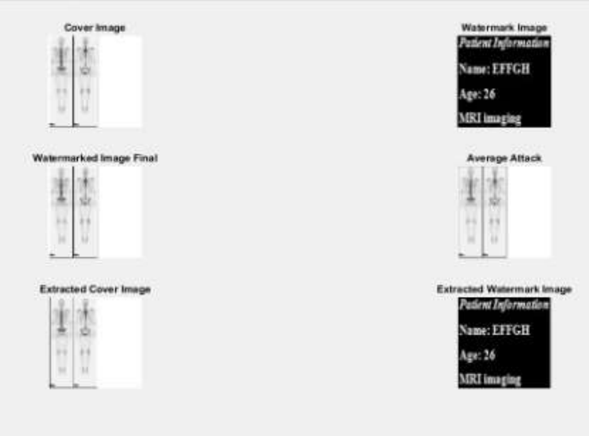


Figure 21: Proposed Watermarking Procedure with Average attack

Here in Figure 22, we have taken cover image as X-Ray image and watermark image as Patient-2 image with Gaussian attack using Proposed techniques.

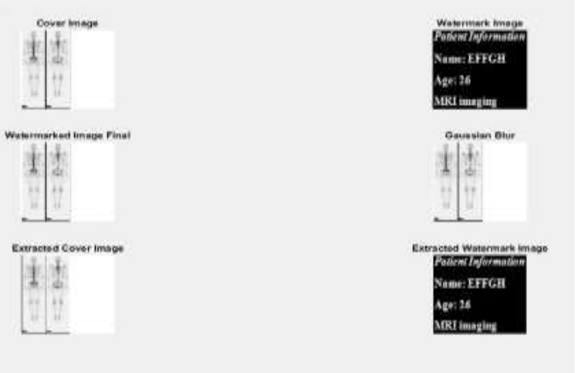


Figure 22: Proposed Watermarking Procedure with Gaussian attack

Here in Figure 23, we have taken cover image as X-Ray image and watermark image as Patient-2 image with Gaussian attack using Proposed techniques.

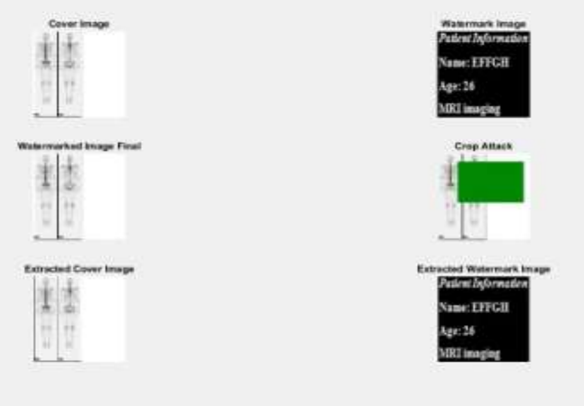


Figure 23: Proposed Watermarking Procedure with Crop attack

Here in Figure 24, we have taken cover image as CT image and watermark image as Patient-3 image with Blur attack using Proposed techniques.

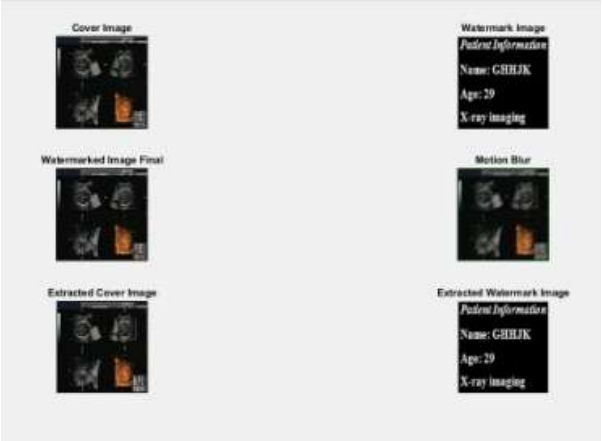


Figure 24: Proposed Watermarking Procedure with Blur attack

Here in Figure 25, we have taken cover image as CT image and watermark image as Patient-3 image with Average attack using Proposed techniques.

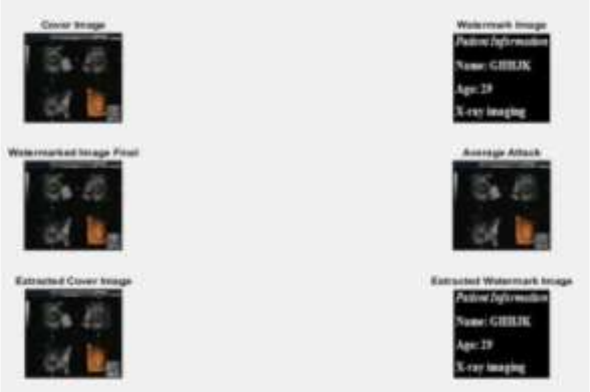


Figure 25: Proposed Watermarking Procedure with Average attack

Here in Figure 26, we have taken cover image as CT image and watermark image as Patient-3 image with Gaussian attack using Proposed techniques.

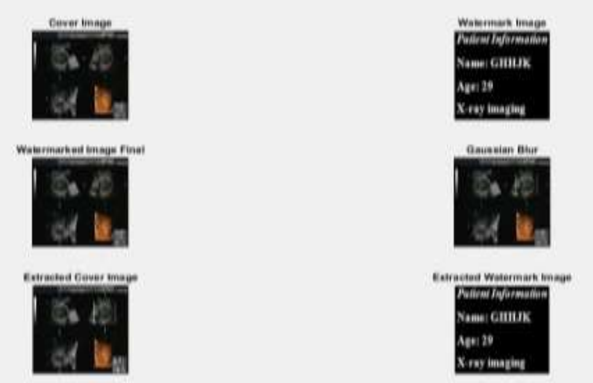


Figure 26: Proposed Watermarking Procedure with Gaussian attack

Here in Figure 27, we have taken cover image as CT image and watermark image as Patient-3 image with Gaussian attack using Proposed techniques.

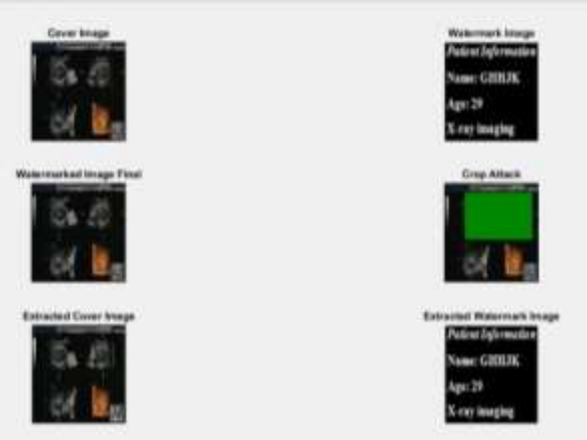


Figure 27: Proposed Watermarking Procedure with Crop attack

Table 1: PERFORMANCE OF NC AGAINST ATTACKS

Attack Type	**MRI+ Patient-1**	**X-Ray+ Patient-2**	**CT+ Patient-3**
	NCC	**NCC**	**NCC**
Blur	1.0005	1.0001	0.992
Average	1.0007	1.0002	0.995
Gaussian	1.0009	1.0005	0.998
Crop	1.002	1.0005	0.995

Table 1 shows the Performance of NCC for proposed scheme. It describes the performance of NCC using proposed algorithm.

VI. CONCLUSION

The present work proposed a multiple watermarking technique which combined wavelets based on texture properties to watermark copyright and authentication information inside a cover image. The proposed method is examined by the performance metrics MSE and PSNR. From the above simulation results, comparison table and the bar graph shown, it is clear that the proposed method provides MSE values 4 times lower than the existing methods and PSNR values are increased by 34%. When we use higher level DWT methods for watermarking it is expected to give the result with lesser execution time when compared to this method. The future work is to perform watermarking by using 2 levels and 3 levels DWT for the medical image authentication.

REFERENCES

[1] Moniruzzaman, Hawladar, Hossain, Md., “Wavelet Based Watermarking Approach for Hiding Patient Information in medical Image for Medical Image Authentication”, 17th International Conference on Computer and Information Technology (ICCIT), 22-23 December, 2014.

[2] Paulopoulas, G. S., Kaoutsouris, D., “Multiple Image Watermarking Scheme Applied to Medical Image Management”, IEEE Trans. on Information Technology in Biomedicine, Vol. 10, Number 4, pp. 3241-3244, 2006

[3] V. Solachidis, I. Pitas, “Circularly symmetric watermark embedding in 2-D DFT domain,” IEEE Trans. Image Process., vol. 10, pp. 1741–1753, 2001.

[4] B.L. Gunjal, R.R. Manthalkar, “Discrete Wavelet Transform Based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images,” Third Int. Conf. Emerging Trends in Engineering and Technology. India, pp. 124-129, November 2010.

[5] S. A. Mostafa, N. El-sheimy, A. Tolba, F. Abdelkader, and H. M. Elhindy, “Wavelet packets-based blind watermarking for medical image management,” The open biomedical engineering journal, vol. 4, 2010.

[6] Giakoumaki, Sotiris Pavlopoulos, and Dimitris Koutsouris, “Multiple Image Watermarking Applied to Health Information Management”, IEEE Trans. on information technology in biomedicine, vol. 10, no. 4, October 2006.

[7] Giakoumaki A, Pavlopoulos S and Koutsouris. “A multiple watermarking scheme applied to medical image management,” in: Engineering in Medicine and Biology Society. IEMBS’04. 26th Annual International Conference of the IEEE, vol. 2, pp. 3241–3244, 2004.

[8] S. C. Rathi and V. S. Inamdar, “Medical Images Authentication Through Watermarking Preserving ROI,” Health Informatics - An International Journal (HIIJ), vol.1, no.1, August 2012.

[9] A. Giakoumaki, S. Pavlopoulos, D. Koutsouris, “Multiple Digital Watermarking Applied to Medical Imaging,” Proceedings of the 2005 IEEE, Engineering in Medicine and Biology 27th Annual Conference, Shanghai, China, September 1-4, 2005.

[10] Petitcolas, F. A. P., Anderson, R. J. and Kuhn, M. G., (1999), “Information Hiding—A Survey”, Proceedings of the IEEE, VOL. 87, NO. 7, JULY 1999

[11] Macq. B.M. & Quisquater. J.J. (1994), “digital Image multiresolution encryption”, The journal of the intractive Multimedia Association Intellectual property project. L (1) 179-206

Ram Pratap Singh, M.Tech Scholar, Department of Computer Science & Engineering, Rameshwaram Institute of Technology and Management, Lucknow, India.

Shyam Shankar Dwivedi, Associate Professor, Department of Computer Science & Engineering, Rameshwaram Institute of Technology and Management, Lucknow, India.