Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

Watermarking and Compression of Bio-Medical Images

M.Susmitha
M.Tech scholar,
Department of Electronics and Communication Engineering
JNTUK Vizianagaram, Andhra Pradesh, India

Dr. B. Nalini
Assistant Professor of
Department of Electronics and Communication Engineering
JNTUK Vizianagaram, Andhra Pradesh, India

Abstract*—Medical information plays a crucial part in medical diagnosis nowadays, and it should be transmitted in an encrypted way. For conveying medical image information, we suggest a combined watermarking-encryption-compression approach. The main goal is to establish medical data storage and security, which will be useful for health card-based treatment. Watermarking medical images have long been acknowledged as a good way to improve security, authenticity, and content verification in this area. In this research, we provide a method for authenticating medical images that combines the Discrete Wavelet Transform (DWT)-Singular Value Decomposition (SVD) authentication approach with the Inverse Discrete Wavelet Transform (IDWT) image retrieval technology. The watermarks are included in the detail coefficient of the sub-bands in our approach. The coefficients of the sub-bands are marked by the embedding a watermark in vertical (LH), horizontal (HL), and diagonal (HH) details, as well as a comparison of embedding a watermark at vertical (LH), horizontal (HL), and diagonal (HH) details. To reduce the size of the data without sacrificing quality, a compression algorithm is used to the watermarked image, and AES encryption is employed to add extra protection. The proposed methodology is analysed on sets of Retinal images and brain MRI images. This scheme maintains the quality of an image while storing data of retinal images and MRI images under one Aadhar card. The performance to static is evaluated using many metrics such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Root Mean Square Error (RMSE), and Compression Ratio (CR). These different performance metrics were analysed after de-watermarking with different orders of Daubechies wavelet.

Keywords*— *Watermarking, Encryption, Compression, Aadhar, DWT, SVD, AES

I. INTRODUCTION

Medical data interchange across departments within a hospital, as well as between hospitals in various geographic areas, is already commonplace. Unfortunately, image exchange via open networks such as the internet is insecure. Because the vital decision is based on this information provided by these medical images, they require stringent security. This medical information can be shared frequently among health professionals to improve therapy. The data storage and security on the medical data which is benefited the health-card-based treatment. This development of the authentication using Watermarking and Compression of biomedical images serves the society to store their medical data on the cloud and use it for their future diagnosis. Digital watermarking is a technique that is used to maintain the authenticity and ownership of digital media such as pictures, music, and video. Huge amounts of medical data must be processed in hospitals for clinical and research purposes. Malicious attacks on these medical data repositories must be avoided. For this purpose, digital watermarking can be employed to achieve medical image authentication. The Aadhar card is used for authentication and a set of biomedical images is hidden under the Aadhar card. While numerous digital watermarking systems exit in both the spatial and transform domains, the image quality is distorted. The insertion and extraction processes are more crucial in the watermarking procedure. In the original image (Aadhar Card), a watermark (hidden image information) is inserted. When the image is retrieved from the database, the doctor will be able to see the authentication phase, which will include the extraction watermark.

However, once the extraction watermark is successfully created, the doctor can proceed to the diagnosis with confidence. The development of the DWT-SVD Algorithm for watermarking, which is utilised for authentication, is the basis for this study. The Aadhar card is used for authentication and a set of biomedical images is hidden under the Aadhar card.

The DWT-SVD and IDWT techniques are implemented for the embedding and retrieval of the watermark on the data. This transform has the advantage of capturing both frequency and location information, as opposed to the Fourier Transform. Signal energy is concentrated on specific wavelet coefficients in the Discrete Wavelet Transform. This property is useful for image compression. Lossless compression is used for minimizing the size of the data. Encryption and decryption are used to enhance the security. The performance of the suggested medical data storage under one identity is evaluated using several metrics such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Root Mean Square Error (RMSE), and Compression Ratio (CR).

The second section deals with a literature survey on image watermarking, encryption, and compression followed by detailed techniques of watermarking and Encryption methods in session 3. In session 4 we explain about proposed methodologies and in session 5 we deal with the performance metric of our algorithm followed by Conclusion and Feature work in sessions 6 and 7 respectively.

II. LITERATURE SURVEY

A more secure and robust digital watermarking method based on the scrambling algorithm and the RSA asymmetric encryption technique has been proposed to protect the hidden data. A hybrid decomposition of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) based on estimated performance embeds the watermark in the low-frequency sub-band of the host image. The protection of

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

transmitted bio-medical images and visual data is done by using a watermarking encryption algorithm and this algorithm is implemented by compression, watermarking, and encryption to secure data [2]. To demonstrate the security of medical images, the security analysis of combined encryption/watermarking (E/W) system findings was performed using 8-bit depth ultrasound images as well as 16-bit encoded PET images. Quantization Index Modulation (QIM), a substitutive watermarking algorithm, a stream cipher algorithm is used in this system. The AES and CBC modes are used for the DICOM standard to make results precisely [3]. In [4], a watermark was developed using a hybrid of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) techniques to reduce ambiguity in patient data during therapy. The integrity of the watermark is ensured using the Singular Value Decomposition (SVD). This scheme guarantees the integrity of data, maintains secrecy when sharing the patient's information, and is strong to several conventional attacks. [5] presents a strong digital watermarking method that combines the Discrete Wavelet Transform (DWT) with Singular Value Decomposition (SVD). The watermark has been applied to the sub-bands of the cover image's single values. The performance measures show that DWT-SVD produces images with good imperceptibility and perceptual quality. JPEG-LS and AES block cipher techniques are employed in [6] to accomplish watermarking encryption and compression on images, our solution can safely make a message available in both encrypted and compressed domains while decreasing visual distortion, according to testing on many retina and ultrasound images.

Existing approaches have numerous flaws. The usage of threshold does not produce high robustness because the method is reliant on watermarking. However, the data embedding capacity of these methods is limited, and their security must be enhanced. Furthermore, their methods employ the asymmetric encryption methodology. Even though different keys are used for encryption and decryption, the distributor must know each user's encryption key to complete the copyright authentication mechanism. As a result, while processing secret keys, management, and dissemination, a security risk occurs, and compressed file transmission may result in a loss of biological problem quality. To address this flaw, we try to improve the security of the watermark by making it takes to extract the watermark. Following that, we suggested a novel image watermarking approach based on the DWT-SVD, AES encryption, and other techniques in the process of copyright authentication. As a result, while processing secret key management and dissemination, a security risk occurs, and compressed file transmission, may result in loss of biomedical problem quality. To overcome this drawback, we attempt to improve the security of the watermark with good imperceptibility as well as lower consuming time for the extraction of the watermark. Then, based on the DWT-SVD, AES encryption and lossless compression, we suggested a new image watermarking approach.

III. BACKGROUND WORK

A. Discrete Wavelet Transform

In terms of addressing the imperceptibility and robustness requirements of digital watermarking methods, the frequency domain watermarking approaches were found to be more effective than spatial domain watermarking techniques [8]. Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT) all are frequency domain transforms. Due to its superior spatial localization and multi-resolution properties, which are like theoretical models of the human visual system, DWT has grown more popular in digital image watermarking. However, DWT has become more popular in digital image watermarking due to its superior spatial localization and multi-resolution properties, which are like theoretical models of the human visual system. Increasing the degree of DWT in DWT-based digital image watermarking approaches could result in even more speed gains.

The Discrete Wavelet Transform is a transform used in both numerical and functional analysis. The wavelets are sampled with discrete values in this transform. This transform has the advantage of capturing both frequency and local information, as opposed to the Fourier Transform. Signal energy concentrates on specific wavelet coefficients in the Discrete Wavelet Transform (DWT). This property is useful for image compression.

A multi-resolution representation called DWT can be used to gradually decode from a low resolution to a higher resolution. The DWT separates the signal into two halves: High frequency and low frequency. The high-frequency segment describes the edge components, whereas the low-frequency section again separated into high and low-frequency sections. Because the human eye less sensitive to fluctuations in edges, high-frequency components are commonly used.

LL	LH
HL	HH

Figure1: DWT sub-bands

The LL band filter in the DWT one-level decomposition contains a lot of information from the original image. The vertical, horizontal, and diagonal information of an original image is Contained in the LH, HL, and HH bands. The LL Band Image is the only one that may be used to reproduce the original image; The other bands are ignored.

B. Singular value decomposition

The method of Singular Value Decomposition (SVD) can be thought of as a matrix transformation. This transformation decomposes an MXN sized image into a 2-D MXN matrix to provide three matrices: U, S, and V. It also has several interesting data science applications. Singular Value Decomposition (SVD) is a commonly used signal processing technique. SVD is used for noise reduction and image compression, among other things.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

The formula of singular value decomposition is,

$$A = U \sum V$$

Here A is a m x n matrix that you obtained from an image or another data source. The orthogonal matrices are matrices that are orthogonal to each other. The matrices *U* and *V* are orthogonal, while ∑ is a diagonal matrix. Finding the eigenvalues and eigenvectors of *A*A^T and A^TA is the first step in calculating the SVD. The eigen vectors of A^TA form the columns of *V*. whereas the eigenvectors of *A*A^T form the columns of *U*. singular values in *S* are also square roots of *A*A^T or A^TA eigenvalues... singular values are always genuine numbers. The host image is frequently decomposed using SVD to provide singular values, which are then used to add watermark information, or the host image is split into many small blocks and then decomposed using SVD to yield singular values. The SVD coefficients' mmagnitude is constant, singular values can describe the image's essential algebraic properties, and singular values are likely to vary dramatically when the image is somewhat disrupted.

C. Encryption

Encryption is essential for today's internet security. An encryption system scrambles sensitive data by converting it to code using mathematical calculations. only the correct key can reveal the original data, ensuring that it remains safe from all except authorized parties. Encryption is the process of transforming data into a secret code that conceals the data's true meaning. The study of encrypting and decrypting data is known as cryptography. In computers, plaintext refers to unencrypted data, whereas ciphertext refers to encrypted data. There are 3 major types of encryption techniques are available to provide security those are AES, DES, and RSA. Among them, Advanced Encryption Standard (AES) is the best encryption standard.

In contrast, with previous encryption algorithms, AES encrypts data in a single block rather than as individual bits. The block sizes yield the names for each type of AES encrypted data. The same key is used for both encryption and decryption, although the techniques are implemented separately. The process is similar for both encryption and decryption but only the difference is the decryption is implemented in reverse order. The encrypted version of the i^{th} block is defined as

$$B_i^e = AES\ (B_i \Theta B_{i-1}^e, K_e)$$

Where B_{i-1}^e stands for the preceding encrypted block and K_e stands for the encryption key?

D. Compression

Data compression is a method of encoding a corresponding data F into another data object FC in such a manner that FCS representation occupies fewer bits. The compression ratio of the image compression technique is referred to as F FC, and it is an important parameter for evaluating different data compression algorithms. There seem to be two kinds of data compression schemes: lossless and lossy. No information is lost during the decompression phase in lossless techniques and F is reconstructed exactly after decompression. Text and data compression are examples of lossless compression. Some information is lost during decompression in the last techniques, so F is not recreated exactly after decompression. A wide range of applications, including video and audio, use lossy compression. Image compression is a technique for diminishing the irrelevance and redundancy of image data so that it can be stored or transmitted more efficiently. As the medical industry expands in everyday life, image compression techniques. to store large amounts of data and information are in high demand. The process of shrinking the size of an image without affecting its quality is known as image compression. The smaller file size makes it easier to store more images. In a file and send or communicate with others.

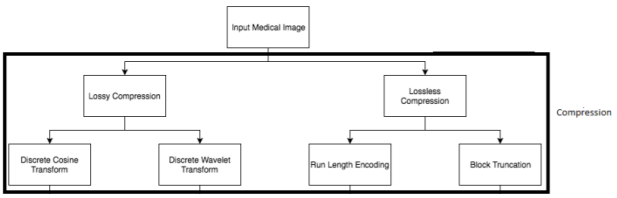

Figure2: Block diagram of image compression

The Discrete Wavelet Transform (DWT) is one of the most extensively utilized transform techniques for image reduction of medical images using wavelets. This DWT is excellent for compressing signals, and it also produces superior outcomes for medical grayscale images. The image being tested, the wavelet function, the number of iterations, and the calculation complexity are all key aspects to consider when employing DWT. In applications like medical imaging, where image degradation is not permitted, wavelet transforms are employed to analyse and Improve signals.

IV.PROPOSED WORK

In this part, we offer a new watermarking strategy (shown in Figure 3) to safeguard medical images. Watermark embedding and extraction are the two procedures involved in watermarking. The algorithm operations are represented by the blocks in the diagram.

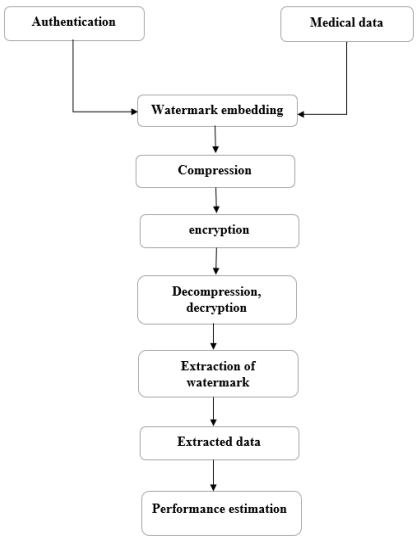

Figure3: Block diagram of the proposed methodology

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

Authentication: In this project, the Aadhar card is used for authentication purposes.
Medical data: The datasets considered in this project are a set of brain MRI images and retinal images.
Watermark embedding: In this project, we design an algorithm for the application of the watermark. watermark, encryption, and compression are presented in the algorithm.

Applying two-level DWT to the host image, getting the low- frequency sub band, and then processing the sub band with singular value decomposition are all steps in watermarking embedding process. The scaling factor is also used to change the Watermark embedding strength. The new value was then split again to produce a new singular value, which was then used to reconstruct the frequency sub-band. The watermarked image was made utilising a new sub-band after executing the inverse DWT transform. The DWT the watermarked image is then compressed, And the compressed images then encrypted with AES. After that the decryption and decompression are carried out.

Genal watermarking:

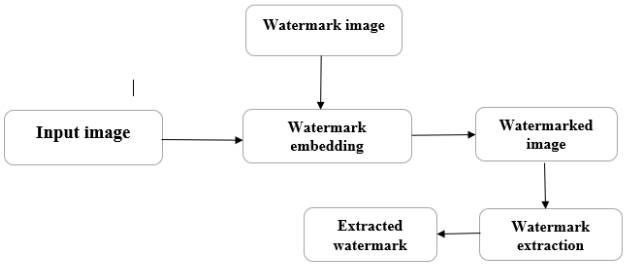

Figure 4: Typical watermarking system

The following is an algorithm for applying watermarking to an image:

1. Start the program.
2. Look at the first image in the input (cover image, i.e., Aadhar card).
3. Open Dataset 2 (Host image) or image 2 (input image).
4. Resize the image 1 to 300X300.
5. Resize the image 2 to 300X300 and generate a key value to apply wavelets on the images.
6. To partition the image for watermarking, use the DWT approach using the haar wavelet.
7. After applying the DWT to the image, it is separated into four sub-bands: h-LL, h-LH, h-HL, h-HH
8. Using the SVD technique on red, green, and blue hues, extract the RGB color from input image 1 and input image 2.
9. Using IDWT, apply some intensity to the watermarking and retrieve the resulting image.
10. Use the imwrite command to save the watermarked image.
11. Apply the compression on the watermarked image and save the compressed image in a secret folder with the help of the imwrite command.
12. Apply the encryption to the compressed watermarked image.

Watermark extraction:

The DWT technique was applied to the watermarked image, with the low-frequency sub-band being further fragmented into four sub-bands, The Watermark image retrieved by applying the IDWT on the watermarked image.

De-watermarking algorithm:

1. Start the program.
2. Read the secret folder.
3. Use the imwrite command to save the decrypted and decompressed image.
4. Read the image with the watermark.
5. Use the DWT technique with haar wavelet to de=ivied the image for watermarking. The image is then divided into four sub-bands: ω_m-LL, ω_m-LH, ω_m-HL, ω_m-HH.
6. Apply the SVD method on red, green, and blue hues after extracting the RGB color from the source image.
7. With the aid of commands, you may extract the watermarked image.

   S_ewatr=(S_imgr3-S_imgr1)/0.10
   S_ewatg=(S_imgg3-S_imgg1)/0.10
   S_ewatb=(S_imgb3-S_imgb1)/0.10

   ewatr = U_imgr2*S_ewatr*V_imgr2'
   ewatg = U_imgg2*S_ewatg*V_imgg2'
   ewatb = U_imgb2*S_ewatb*V_imgb2'
8. Using IDWT, apply some intensity to the watermarking and receive the resulting image.
9. Use the imwrite command to save the extracted watermark.
10. Calculate the metrics of the watermarked image, such as MSE, PSNR. RMSE and compression ratio.

V.EXPERIMENTAL RESULTS

In this section, for experimental analysis the standard database was considered, the proposed method of performance measures was evaluated. The proposed algorithm is evaluated using the available dataset. The report of experimental results based on the TCGA and _test datasets is presented in this work. The TCGA dataset contains 31 images, _test dataset contains 20 images and the Aadhar is used for authentication purposes.

A. Database

TABLE I. DATABASE DESCRIPTION

Dataset type	Size of dataset	No. of images
TCGA	14MB	31
Test dataset	6MB	20
Aadhar	148KB	1

B. Analysis of algorithm

Many watermarking algorithms that are unable to provide better quality and imperceptibility of the image have been subjected to performance measures. To address this issue, this work is to perform DWT-SVD watermarking by comparing the performance measures of the watermarked image.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

Watermarking when using the Brain MRI database

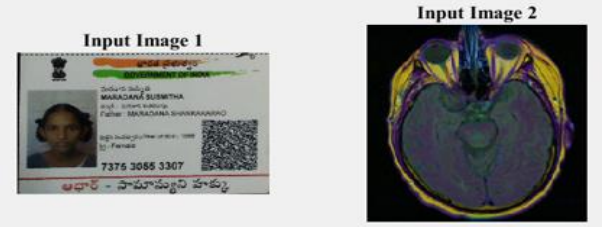

Figure 5(a): Input images for watermarking

The cover image is on the left, while the watermark image is on the right, as seen in fig.5(a). When we apply the watermark embedding to the Brain MRI database the result shows that all the images hide under the one Aadhar card. But before applying the watermark the pre-processing stage is involved.

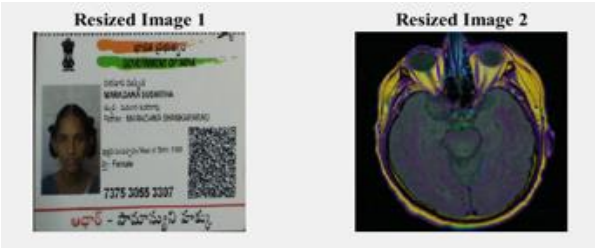

Figure5(b): input images after preprocessing

As illustrated in fig.5(b), the input images are rescaled to a consistent size. The RGB image is then transformed to grayscale.

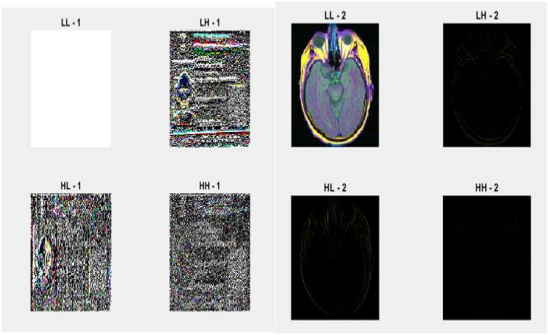

Figure5(c): application of wavelets to input images

The wavelets are applied to both the input image and the watermarked image after the preprocessing stage, dividing the images into four sub-bands: LL-1, LH-1, HL-1, HH-1, LL-2, LH-2, HL-2, and HH-2. In an image, the LL sub-bands contain the most information.

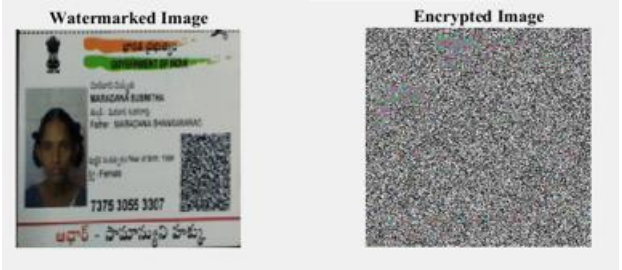

Figure5(d): watermarking and encryption

As shown in fig.5(d) the left image shows the watermarked image after the watermarking phase the image is subjected to compression and encryption. The encrypted image will be like shown in the above rightmost figure.

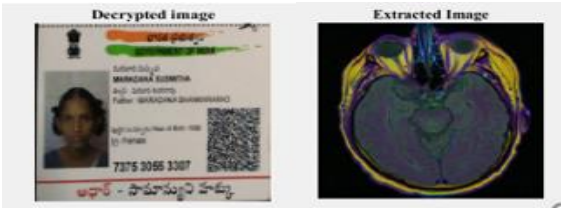

Figure5(e): Decrypted and extracted images

The decrypted image is generated by applying the decryption to the compressed image, as illustrated in fig.5(e), and the extracted watermarked image is presented on the right. By applying the De-watermarking, the Brain MRI image was retrieved from the watermarked image.

C. Image Quality measurement

The quality measurement bought on the host data at the insertion of the watermark is large in watermarking techniques. Some quality measures can be used to determine the distortion in the watermarked image by comparing it to the original image. The most widely used approaches are detailed in the following sections.

D. Mean Square Error (MSE)

The average squared difference between an original image and a distorted image is defined as MSE. The MSE estimates the damage caused by the watermark. The MSE examines watermarking degradation.

$$MSE=\frac{1}{PQ}\left[\sum_{i=1}^{P}\sum_{j=1}^{Q}(m(i,j)\text{-}n(i,j))\text{^}2\right]$$

Where P and Q represent the image's height and width, respectively.

- m (i, j) represents the original images pixel value and
- n (i, j) represents the embedded image's pixel value.

E. Peak Signal to Noise Ratio (PSNR):

If we want to find the watermarked image's quality loss in comparison to the original image. The PSNR of an image affects its imperceptibility. It assesses the distortion generated by the watermarked image on the original image. After the watermark has been inserted, The PSNR is calculated as follows.

$$PSNR = 10\ log_{10}\left(\frac{L*L}{MSE}\right)$$

Where L is the image's highest value. For an 8-bit image, L=255. In multimedia applications, any image with a brightness of greater than 30 DB is acceptable. However, with medical imaging, data quality is paramount, and PSNR of around 50Db indicates that the image is of high quality and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

that there has been no significant degradation in the image compared to the original.

F. Root Mean Square Error (RMSE):

The squared root of MSE is used to calculate the Root Mean Square Error (RMSE). The Root Mean Square Error (RMSE) is a metric that indicates how much a pixel changes because of processing. Because RMSE is scale-dependent, it should only be used to evaluate the prediction errors of different models or model configurations for a single variable, not between variables.

$$\text{RMSE} = \sqrt{\overline{(f-o)^2}}$$

Where, f=forecasts (expected values or unknown results)
0=observed values (known results)

G. Compression Ratio (CR):

Image compression is the process of reducing the size of an image file in bytes without sacrificing the images' quality. More images can be saved in each amount of disc or memory space because of the smaller file size.

$$\text{CR} = \frac{n1}{n2}$$

Where, let n1, n2 denote the number of bits in the original and compressed images

Figure5(f): Performance measures for the MRI Database

The above figure shows the performance measures and graph for the Brain MRI database and the time taken for the entire watermarking and de-watermarking is around 7sec. and the encrypted and compressed images are stored in a specific folder.

	1 meansqerror	2 PSNR	3 RMSE	4 compression_ratio
1	1.5585	46.2038	-0.0022	6.0753
2	1.3618	46.7898	-0.0026	6.0423
3	1.3542	46.8141	-0.0024	6.0496
4	1.4165	46.6186	-0.0024	6.0753
5	1.4620	46.4815	-0.0021	6.1042
6	1.5924	46.1103	-0.0027	6.1308
7	1.8171	45.5371	-0.0023	6.1017
8	1.7482	45.7049	5.3416e-05	6.1254
9	1.4991	46.3725	-0.0023	6.0716
10	1.6833	45.8692	-0.0011	6.1312
11	1.8019	45.5735	-6.2003e-04	6.1555
12	1.4423	46.5402	-9.4849e-04	6.0840
13	1.4639	46.4756	-5.4610e-04	6.0992
14	1.9036	45.3350	4.8412e-05	6.1652
15	1.6499	45.9564	-0.0033	6.0959
16	1.6472	45.9633	-0.0032	6.1166
17	1.6510	45.9533	-0.0029	6.0963
18	1.6260	46.0197	-0.0013	6.0934
19	1.8477	45.4644	1.9601e-04	6.1450
20	1.5632	46.1905	-0.0012	6.0819

Figure5(g): The performance metrics for the Brain MRI dataset using the db1 wavelet filter

The above figure shows the performance metrics for the 20 images in a single sheet.

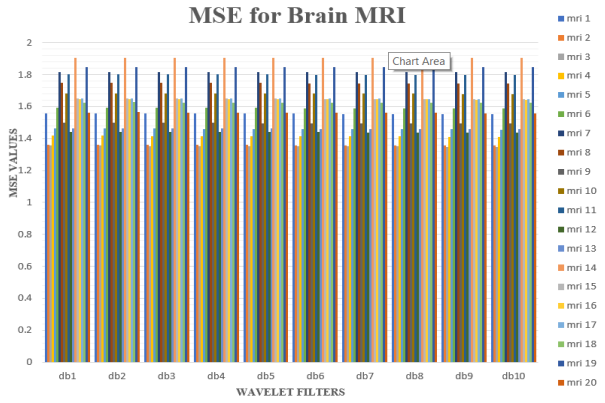

Figure5(h): MSE for Brain MRI for different orders of dB filters

The above figures show the results for the MSE values of the Brain MRI dataset for different orders of the Daubechies wavelet filters. The Mean Square Error (MSE) is used to determine the image degradation.

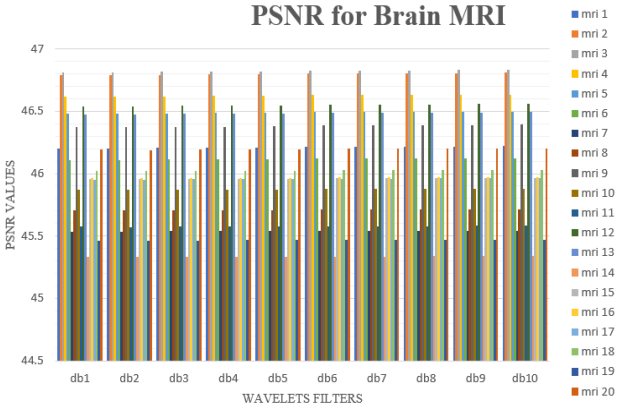

Figure5(i): PSNR for brain MRI for different orders of dB wavelet filters

The above figure shows the results for PSNR values of the Brain MRI dataset for different orders of the Daubechies wavelet filters. To determine the imperceptibility the PSNR is calculated to the extracted watermarked images.

VI.CONCLUSION

The purpose of this work is to secure the images transferred via telemedicine as much as possible. These images are watermarked with the patient's details to avoid any mistake between the patient's radiographs. As a result, during the extraction, the doctor will be able to check with certainty that the reports belong to the treated patient. some inherent drawbacks of existing methods used for quantitative analysis of watermarking for color images are studied.

The main novelty of this work is, capturing many medical images at once and feeding them into the algorithm. Here the 14 and 6 MB TCGA and _test datasets are hidden under a single Aadhar card. The decrypted and compressed images are stored in a certain folder without losing their quality. The AES encryption is used for more security. Finally, got a fruitful image after extraction. Metrics like MSE, PSNR, RMSE, and Compression Ratio are calculated to show the performance results.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 12, December-2021

REFERENCES

[1] Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Systems with Applications, 97, 95–105. doi:10.1016/j.eswa.2017.12.003

[2] Puech, W. (2008). [IEEE 2008 First Workshops on Image Processing Theory, Tools and Applications (IPTA) - Sousse, Tunisia (2008.11.23-2008.11.26)] 2008 First Workshops on Image Processing Theory, Tools and Applications - Image Encryption and Compression for Medical Image Security. , (), 1–2. doi:10.1109/ipta.2008.4743800 R. Nicole, "Title of paper with the only first word capitalized," J. Name Stand. Abbrev., in press.

[3] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 5, pp. 891–899, Sep. 2012

[4] M.] Zermi, N., Khaldi, A., Kafi, M.R. *et al.* A lossless DWT-SVD domain watermarking for medical information security. *Multimed Tools Appl* **80,** 24823–24841 (2021). https://doi.org/10.1007/s11042-021-10712-7

[5] Thakkar, F.N. and Srivastava, V.K., 2017. A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimedia Tools and Applications, 76(3), pp.3669-3697

[6] S. Haddad, G. Coatrieux, A. Moreau-Gaudry, and M. Cozic, "Joint Watermarking-Encryption-JPEG-LS for Medical Image Reliability Control in Encrypted and Compressed Domains," in *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2556-2569, 2020, DOI: 10.1109/TIFS.2020.2972159.

[7] Sumedh P. Ingale1, Prof. C. A. Dhote," Digital Watermarking Algorithm using DWT Technique," International Journal of Computer Science and Mobile Computing, Vol.5 Issue.5, May- 2016, pg. 01-09

[8] Ariatmanto, D., Ernawan, F. An improved robust image watermarking by using different embedding strengths. *Multimed Tools Appl* **79,** 12041–12067 (2020). https://doi.org/10.1007/s11042-019-08338-x

[9] N. Boujemaa et al., "Fragile watermarking of medical image for content authentication and security," IJCSN-Int. J. Comput. Sci. Netw., vol. 5, no. 5, pp. 1–7, 2016.

[10] W. Puech and G. Coatrieux. Chapter 10: Coding: EncryptionWatermarking-Compression for Medical Information Security. Compression of Biomedical Images and Signals, A. Na¨ıt-Ali and Christine CavaroMenard, Digital Signal Processing, ISTE-Wiley, May 2008

[11] W. Puech and J.M. Rodrigues. A New Crypto-Watermarking Method for Medical Images Safe Transfer. In Proc., 12th European Signal Processing Conference (EUSIPCO'04), pages 1481–1484, Vienna, Austria, 2004

[12] Sunesh, Vinita Malik, Neeti Sangwan, Sukhdip Sangwan." Digital Watermarking using DWT-SVD Algorithm," Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 7 (2017) pp. 2161-2171 © Research India Publications

[13] Chetna, Krishan Kumar." Data and Information Hiding on Color Images Using Digital Watermarking," International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct 2014

[14] Y. He, G. Yang, and N. Zhu, "A real-time dual watermarking algorithm of H. 264/AVC video stream for video-on-demand service," AEU-Int. J. Electron. Commun., vol. 66, no. 4, pp. 305–312, 2012.

[15] S. P. Metkar and M. V. Lichade, "Digital image security improvement by integrating watermarking and encryption technique," in Proc. IEEE Int. Conf. Signal Process., Comput. Control (ISPCC), Sep. 2013, pp. 1–6

[16] G. Singh and S. Supriya, "A study of encryption algorithms (RSA, DES, 3DES, and AES) for information security," Int. J. Comput. Appl., vol. 67, no. 19, pp. 33–38, Apr. 2013.

[17] M. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS," IEEE Trans. Image Process., vol. 9, no. 8, pp. 1309–1324, Aug. 2000.

[18] Zhen-Ming Lu, Dian-Guo Sheng Xu, and -He Sun, "Multipurpose Image WatermarkingAlgorithm Based on Multistage Vector Quantization," IEEE Transactions on ImageProcessing, vol. 14, no. 6, June 2005

[19] Kim, Jong Ryul, and Young Shik Moon. "A robust wavelet-based digital watermarking using level-adaptive thresholding." Image Processing, 1999. ICIP 99. Proceedings. 999 International Conference on. Vol. 2. IEEE, 1999.

[20] M. N. A. Wahid, A. Ali, B. Esparham, and M. Marwan, "A comparison of cryptographic algorithms: Des, 3DES, AES, RSA, and blowfish for guessing attacks prevention," J. Comput. Sci. Appl. Inf. Technol., vol. 3, pp. 1–7, Aug. 2018.

[21] R. Acharya, U. Niranjan, S. Iyengar, N. Kannathal, and L. C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," Comput. Methods Programs Biomed., vol. 76, no. 1, pp. 13–19, Oct. 2004.

[22] Thakkar FN, Srivastava VK (2017) A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimed Tools Appl 76:3669–3697. https://doi.org/10. 1007/s11042-016-3928-7.