International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 09 | Sep 2022 www.irjet.net p-ISSN: 2395-0072

Hybrid Transforms Based Watermarking, Encryption and Compression of Bio-Medical Images

T. Spandana[1], R. Gurunadha[2]

[1]M. Tech scholar, Dept. Of Systems and Signal Processing, JNTU-GV College of Engineering Vizianagaram(A), Andhra Pradesh, India.
[2]Associate Professor, Dept. of Electronics and Communication Engineering, JNTU-GV College of Engineering Vizianagaram (A), Andhra Pradesh, India.

---***---

Abstract – *In this paper, we are discussing about the Hybrid transforms-based watermarking, encryption and compression of bio-medical images. The entire system is designed using MATLAB Software with the version of 2021a. Nowadays, Medical information plays an important role in medical diagnosis, transferring of that information should be done in an encrypted manner. Proposed novel Image Watermarking which is based on the Discrete Wavelet Transform (DWT), Hessenberg Decomposition (HD) and Singular Value Decomposition (SVD). Inverse Discrete Wavelet Transform (IDWT) used for retrieval of image. In this, watermark is embedded into sub-bands coefficient. Sub-band coefficients are marked by adding a watermark of the same size of the three sub-bands. Comparison of embedding a watermark at vertical (LH), horizontal (HL) and diagonal (HH) details. Here, Compression scheme applied on the watermarked image to reduce size of the data without losing its quality. AES encryption is used for security and proposed methodology analyzed on data sets of MRI of brain images and Retina images. The performance metric is analyzed after de-watermarking with different orders of Daubechies wavelets by using parameters like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Root Mean Square Error (RMSE) and Compression Ratio (CR).*

***Key Words*: Image Watermarking, DWT, HD, SVD, IDWT, Compression, AES Encryption**

1.INTRODUCTION

Watermarking is a process of embedding information into a digital signal such as image, video, audio data to easily identify the ownership of the original data. Therefore, it will be embedded in a way which makes it difficult to be visualize with the human eye and to be removed. As computers are more and more integrated via the network, the distribution of digital data is becoming faster, easier, and less effort to make exact copies. One of the present research areas is to protect digital watermark inside the information so that ownership of information will not be claimed by the third party. The working domain of the watermarking is either spatial or frequency. Medical data exchange between the departments is not just hospitals, but between hospitals in different geographical areas. Medical images require strict security measures. The medical information can often be shared to the professionals to improve treatment. Huge amount medical data should be processed in hospitals for clinical and medical purpose of research. Malicious attacks on this medical data repots should be avoided and also can create medical images with watermarks certification. Image quality is distorted in the spatial and transform domains. The process of inserting and extracting watermarking process. In the original image, a watermark (hidden image information) is inserted. If Images are retrieved from the database, allowing physicians to see Authentication Phase with Extraction watermark. However, upon successful watermark extraction, created and the doctor can proceed with the diagnosis trust. Development of the DWT-HD-SVD Algorithm Based on the watermark used for this study. A series of biomedical images are hidden under the cover image. Embedding and retrieval of watermarks in data can be analyzed. This transformation includes frequency and Location information, as opposed to the Fourier transform. Here, Signal energy is concentrated in specific wavelet coefficients with the discrete wavelet transform. This property is useful when image compression is needed. lossless compression is used to Minimize data size. Encryption and decryption are Used the security. Proposal performance of medical data storage is also evaluated by multiple metrics such as mean squared error (MSE), peak signal signal-to-noise ratio (PSNR), root-mean-square error (RMSE), and Compression ratio (CR).

2. LITERATURE SURVEY

A safer and more robust digital watermarking method based on encryption algorithms and asymmetric RSA Encryption techniques have been proposed to protect hidden things (DWT) and singular value decomposition (SVD). The power to estimate embedding a watermark in the low-frequency sub bands of the host image. Transmitted biomedical images and visual data are Watermark encryption algorithm and use of this algorithm compression, watermarking, Encryption to protect data. medical imaging combined with security analysis of A study of encryption/watermarking (E/W) systems found that Wavelet transform (DWT) and singular values Decomposition Techniques to Reduce Ambiguity (SVD)

Guaranteed by singular value decomposition (SVD). Digital Watermarking Method Combining Discrete Wavelets Transformation by Singular Value Decomposition (DWT) Show that DWT-SVD produces good images uses block encryption techniques to achieve this. Watermark image encryption and compression, the method relies on watermarks. Distributors need to know each user`s encryption key to complete the process processing, management and distribution of private keys; Error trying to improve watermark security Watermark extraction takes time. proposed a new image watermarking approach based on DWT-HD-SVD, AES encryption are trying to improve watermark security and watermark extraction.

3. PRELIMINARIES

This section presents the three techniques DWT, HD, and SVD used in the proposed watermark method. Multi-resolution timescale signal of DWT can improve watermark performance. HD performs as the matrix transforms have further improved robustness. In addition, SVD-based watermarking schemes have improved performance in defending against geometric attacks.

3.1 Discrete Wavelet Transform

The Discrete Wavelet Transform is the transform used in both Numerical and functional analysis. Wavelet is sampled. This transform uses discrete values. This conversion includes Advantages of collecting both frequency and location information, Contrast with the Fourier transform. signal energy Focus on specific wavelet coefficients in discrete Wavelet transform (DWT). This property is useful for images compression. A multi-resolution representation called DWT used to Decode step by step from low resolution to high resolution. DWT separates the signal into two halves. High Frequency and low frequency. high frequency segment represents the edge component, and the low frequency is the section and is again divided into a high frequency section and a low frequency section. Since the human eye is not sensitive to edge variations, High frequency components are usually used.

LL	LH
HL	HH

Fig -1: DWT Sub-bands

Here, LL band filter in 1-stage DWT decomposition contains a lot of information from the original image. Vertical, horizontal, skew(diagonal) information of the original images is included in the LH, HL, and HH bands. LL band Only images can reproduce the original image. Other bands are ignored.

3.2 Hessenberg Decomposition

HD is a type of matrix decompositions can be used for square matrix decomposition. A n × n square matrix X can be decomposed by using HD as shown by

$$P\ H\ P^{T} = HD(X),$$

where P is an orthogonal matrix and H is an upper Hessenberg matrix, and $h_{i,j} = 0$ when $i > j + 1$. HD is computed by the Householder matrices. Householder matrix Q is an orthogonal matrix and it is expressed as

$$Q = (I_n - 2\mu\mu^T)/\mu^T\ \mu,$$

where μ is a non-zero vector in R^n, and I^n is a n × n identity matrix. n−2 steps are in the overall procedure. Therefore, HD is computed as

$$P = (Q_1Q_2 \ldots Q_{n-2})^T X\ (Q_1Q_2 \ldots Q_{n-2})$$

$$\Rightarrow H = P^T X\ P$$

$$\Rightarrow X = P\ H\ P^T$$

3.3 Singular Value Decomposition

It is a factorization of that matrix into three matrices in linear algebra. It possesses some unique algebraic characteristics and communicates key geometrical and theoretical insights into linear transforms. It is also having several interesting data science applications. It is a signal processing technique that is widely employed. SVD is used for noise reduction and image compression, among their things.

$$A=U \sum V$$

A is a m x n matrix that you obtained from an image or another data source. The orthogonal matrices ***U*** *and* ***V*** are orthogonal matrices and ∑ is a diagonal matrix. Finding the eigenvalues and eigen vectors of AA^T and A^TA is the first step in calculating the SVD.

The columns of V are formed by the eigenvectors of A^TA, while the columns of U are formed by the eigenvectors of AA^T. Singular values in S are also square roots of eigenvalues from AA^T or A^TA... singular values are always numbers that are genuine.

It is normally acts on the host image, or the host image is first segmented into numerous small blocks and then decomposed using SVD to generate singular values, which are used to incorporate watermark information. The SVD coeffects' size is constant, the singular values can describe an image's essential algebraic properties, and singular values are likely to vary substantially when the image is slightly disrupted.

3.4 Encryption

Encryption is essential to Internet security today. The encryption system transforms and encrypts sensitive data as Code with mathematical calculations. only the correct key reveals the original data and make sure it's safe from everyone Except authorized parties. encryption is Hide data by transforming it into a secret code.

Data encryption and decryption research known as cryptography. For computers, what is plaintext? Ciphertext refers to encrypted data, but unencrypted data.

There are three main types of encryptions for security, these are AES, DES, and RSA. Advanced Encryption Standard (AES) is best Encryption standard. AES Encrypts data in single blocks rather than as individual bits. the Block size indicates the name of each AES type of encrypted data. Here, same key is used for encryption and decryption. Decryption, although the technique is implemented Separately.

This process involves encryption and decrypt, but the only difference is the decryption Implemented in reverse order.

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

Where, B_{i-1}^e is the previous encrypted block and K_e is the encryption key.

3.5 Compression

Image compression is a technique for diminishing the irrelevance and redundancy of image data so that it can be stored or transmitted in a more Efficient manner. Image compression is the process of Shrinking the size of an image without sacrificing its quality.

In a file and send or communicate with others. One of the most widely used transform techniques for image compression of medical images using wavelets is Discrete Wavelet Transform (DWT). This DWT is very useful for compressing signal and shows better results for medical gray scale images.

While using DWT the important parameters that are taken into consideration are testing the image, wavelet function, number of iterations and calculation complexity. These wavelets transforms are used to process and improve signals in fields like medical imaging where image degradation is not tolerated.

4. PROPOSED WORK

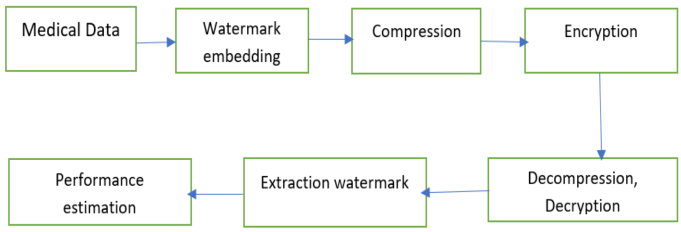

Fig -2: Block diagram of proposed method

The datasets considered in this project are a set of retina images and MRI of brain images.

4.1 Watermark Embedding:

Here, we design an algorithm for the application of the watermark. watermark, encryption, and compression are represented in this algorithm. In the process of watermark embedding, two level DWT is applied on the host image and the low frequency sub band was then obtained and sub band was further processed by HD and SVD. In addition, the scaling factor is added to control the watermark embedding strength. The new value was subdivided once again to get a new singular value which was used to reconstruct frequency sub band. Finally, the watermarked image was formed by making using of new sub band after the process of inverse discrete wavelet transform. After that apply the compression on the watermarked image and the AES encryption is applied to the compressed image. The decryption and the decompression are conducted separately.

Algorithm for applying watermarking to an image:

1. Start the program
2. Look at the first image in the input (cover image).
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. HD is performed on LL, and it is shown as PHP ^{T} = HD(LL).
9. Extract the RGB color from input image 1 and input image 2, apply SVD algorithm on red, green, and blue color and SVD to H i.e., $HU_w HS_w HV^T_w = SVD(H)$.
10. W is applied with SVD, i.e., $U_w S_w V^T_w = SVD(W)$.
11. Compute an embedded singular value HS^*_w by adding HS_w and S_w with a scaling factor α by $HS^*_w = HS_w + \alpha S_w$

12. The watermarked sub-band H^* is generated by using the inverse SVD, i.e., $H^* = HU_w HS^*_w HV^T_w$.
13. Apply the watermarking with some intensity and get the output image with the help of IDWT.
14. Save the watermarked image with the help of imwrite command.
15. Apply the compression on the watermarked image and save the compressed image in a secret folder with the help of imwrite command.
16. Apply the encryption to the compressed watermarked image.

4.2 Watermark Extraction:

The operation of DWT was applied to the watermarked image, and the low frequency approximate coefficient of Which was further decomposed. The Watermark was obtained under the utilization of the original host image and the newly formed singular value.

Algorithm for de-watermarking:

1. Start the program
2. Now Read the secret folder.
3. Save the Decrypted & decompressed image with the help of imwrite command.
4. Read the watermarked image.
5. Apply the DWT technique with Haar wavelet to divide the image for watermarking. The image is then divided into 4 sub-bands i.e., ω_m-LL, ω_m-LH, ω_m-HL, ω_m-HH.
6. HD is performed on LL_w by $P_w H_w P^T_w = HD(LL_w)$ Apply SVD to H_w, i.e., $HU^*_w HSb^*_w HV^*_w{}^T = SVD(H_w)$ and Extract the RGB color from original image and apply SVD algorithm on red, green, and blue color. The extracted singular value S^*_w is gained by $S^*_w = (HSb^*_w - HS^*_w)/\alpha$. The extracted watermark W^* is reconstructed by inverse SVD, which is described by $W^* = U_{w2} S^*_w V^{-T}_{w2}$.
7. Apply the watermarking with some intensity and get output image with help of IDWT.
8. Save the extracted watermark with the help of imwrite command.
9. Calculate the parameters like MSE, PSNR, RMSE and CR of watermarked image.

5. EXPERIMENTAL RESULTS

In this section, the performance measures were evaluated and proposed algorithm is evaluated using the available dataset. which are based on the TCGA and _test datasets is presented in this work. The TCGA dataset contains 50 images, _test dataset contains 25 images.

Table -1: Database Description

S. No	Dataset type	Size of dataset	No. of images
1	TCGA	14MB	50
2	Test dataset	6MB	25

5.1 Analysis of algorithm

Many of watermarking algorithms 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-HD-SVD watermarking by comparing the performance measures of the watermarked image.

Watermarking when using Brain MRI and Retina images

Fig -5(a): Input images for watermarking

The cover image is at the left, at the same time as the watermark image is at the right, as shown in fig.5(a). When we apply the watermark embedding to the MRI of brain database all the images are hidden under cover image but earlier than making use of the watermark the pre-processing level is involved.

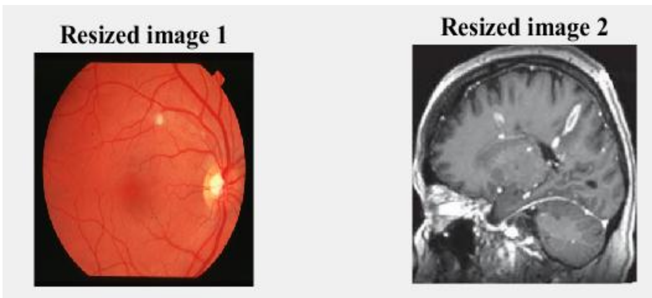

Fig -5(b): input images after preprocessing

As illustrated in fig 5(b), the input images are rescaled to a consistent size.

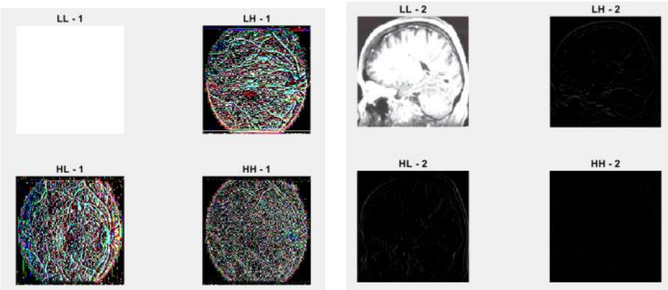

Fig -5(c): application of wavelets to input images

The wavelets are applied to both the input image and the watermarked image after the pre-processing 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. Here, the LL sub-bands containing the most information.

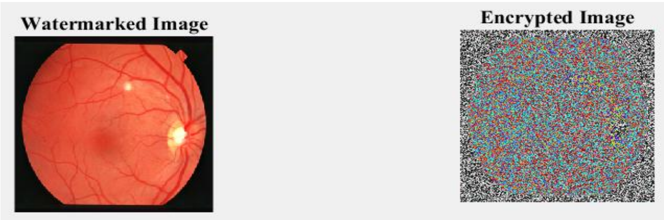

Fig -5(d): watermarking and encryption

As illustrated 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.

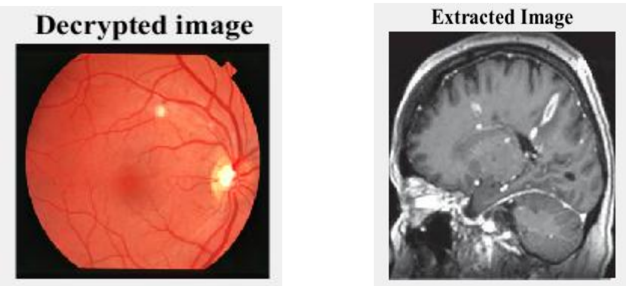

Fig -5(e): Decrypted and extracted image

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

Image quality measurement:

Some quality of measures can be used to determine the distortion in the watermarked image by comparing it to the original image. The following sections are widely used.

Mean Square Error (MSE):

It is the averaged value of the square of the pixel-by-pixel difference between the original image and stego-image which gives us a measure of the error produced in that cover image by using the data embedding process.

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

Where P, Q represents the height and width of the image respectively.

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

Peak Signal to Noise Ratio (PSNR):

To find the watermarked image's quality loss in comparison to the original image. The PSNR of an image affects its imperceptibility. PSNR is calculated by using the formula as follows.

$$PSNR = 10\ log_{10} = (L*L/MSE)$$

Here, L is the value of the image height. For 8-bit image, L=255. Any image with a brightness of greater than 30 DB is acceptable in the application of multimedia. In medical imaging the data quality is paramount, and PSNR of around 50Db indicates that the image is of high quality and that there has been no significant degradation in the image compared to the original.

Root Mean Square Error (PMSE):

The squared root of MSE is used to calculate RMSE. It is a metric used to indicate how much a pixel changes in means of processing. Because RMSE is dependent of scale, it should only use to evaluate the prediction errors of different models for a single variable, not between the variables.

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

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

Compression Ratio (CR):

The squared root of MSE is used to calculate the Root Mean Square Error (RMSE). The Root Mean Square Error 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.

$$CR = n1/n2$$

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

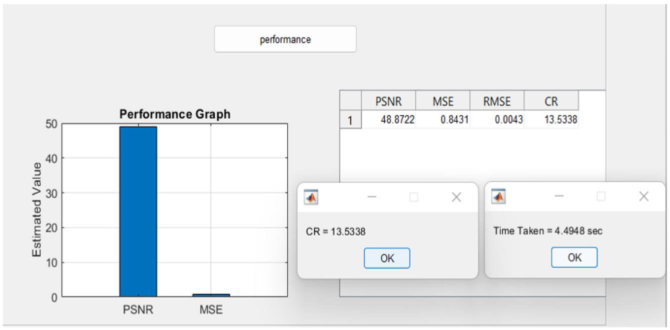

Fig -5(f): Performance measures for the MRI Database

This 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 5 sec. The encrypted and compressed images are stored in a separate folder.

	1 meansqerror	2 PSNR	3 RMSE	4 compression_ratio
1	0.8401	48.8746	-0.0025	13.0114
2	0.8410	47.7144	-0.0024	13.5074
3	0.8076	47.7735	-0.0023	13.0567
4	0.8071	47.7682	0.0044	13.5331
5	0.8008	48.3180	0.0033	13.0928
6	0.8048	48.6623	-0.0041	13.2100
7	0.8070	47.7286	0.0023	13.2256
8	0.8185	47.1323	-0.0030	13.3710
9	0.8246	48.3785	-0.0028	12.9125
10	0.8024	48.1202	0.0060	13.3333
11	0.8377	48.6001	0.0031	13.1138
12	0.8058	50.5284	0.0035	13.3730
13	0.8104	48.0012	-0.0028	12.7895
14	0.8010	48.0943	0.0030	13.2763
15	0.8302	48.0014	-0.0043	12.9964
16	0.8320	47.7928	-0.0026	13.0700
17	0.8148	48.6623	-0.0041	13.2100
18	0.7597	45.3242	0.0032	13.2159
19	0.7843	48.6649	0.0039	13.1907
20	0.5109	45.0478	-0.0025	12.8866
21	0.8172	42.0077	-0.0024	13.0548
22	0.1723	43.4404	0.0025	13.3929
23	0.1264	42.6139	-0.0020	13.2959
24	0.7507	43.3503	-0.0022	13.4630
25	0.8356	48.0107	-0.0021	13.2314

Chart -1: Performance metrices for the Brain MRI Dataset using the db1 wavelet filter

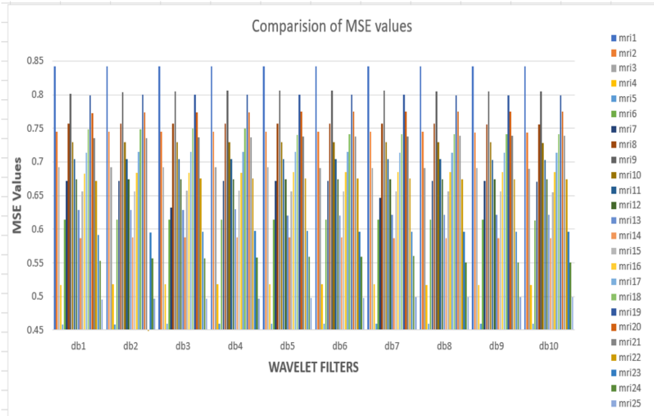

Chart -2: MSE for Brain MRI for different types of orders of dB filters

This MSE figure shows the result 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 degradation of image.

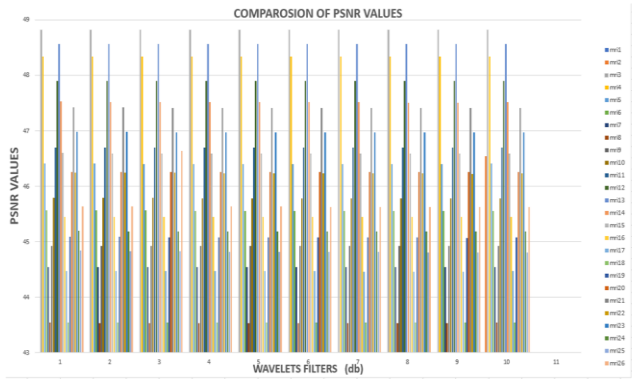

Chart -3: PSNR for brain MRI for different types of orders of dB wavelet filters

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

6. CONCLUSIONS

In this paper, the proposed image watermarking system is based on DWT-HD-SVD transforms. The invisibility and robustness of this method are analyzed by the numerical simulation trails and the results shown the better quality.

In addition, the comparison with the related works is listed and the corresponding metric values show that the proposed method has a better performance which is used 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.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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

[5] 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

[6] 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.

[7] W. Puech and G. Coatrieux. Chapter 10: Coding: Encryption Watermarking-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.

[8] 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.

[9] 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.

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

[11] 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

[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] 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.

[14] W. Puech and G. Coatrieux. Chapter 10: Coding: Encryption Watermarking-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.

[15] 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.