A Novel Secure and Robust Watermarking of Medical Images Using SSVD

N. Rathina kumar[a*] & Dr. C. Ramya[b]

[a*]Research Scholar, Department of Electronics and Communication Engineering, PSG College of Technology, Coimbatore-641004, Tamilnadu, India. Email: snmrkme@gmail.com
[b]Associate Professor, Department of Electronics and Communication Engineering, PSG College of Technology, Coimbatore-641004, Tamilnadu, India. Email: ramyamaharajan@yahoo.in

Article History: Received: 10 November 2020; Revised 12 January 2021; Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: Digital image watermarking is an effective methodology for the content to be authenticated, both for normal and medical images. Moreover, the progressive developments in internet users have significantly increased today. In addition to being undetectable to the human eyes, the image watermark should also be durable and trustworthy. This research enumerates the proposal of an enhanced methodology on the basis of Singular value decomposition (SVD) and Discrete wavelet transform (DWT) image water marking systems. The Shuffled SVD (SSVD) is considered as the default SVD-variable. Here, the DWT splits the images into 4 subbands (LL, HL, LH and HH). The LL subband is divided into equally sized blocks. Following application of SSVD in several block of the LL subband, the principal components of the watermark images were placed. From the simulation results, it was observed that, there is a greater resilience and a positive error in this proposed medical image watermarking system.
Keywords: Digital image watermarking, Medical image, Singular value decomposition, Discrete wavelet transform, Discrete cosine transform, Discrete fourier transform.

---

1. Introduction

1.1. Need for Watermarking

We live in an era in which the Internet applications in our real-life are so strong that we rely on it in every direction. Over past few years, digital materials such as texts, movies, photographs, audios, etc., have greatly increased over the Internet and have converted the world into a worldwide community. However, when the present access technology is integrated, multimedia information are more sensitive to security vulnerabilities as they could be changed or distributed without prior authorization. Safety risks include infringement of copyrights, piracies, hacking, unauthorised business and delivery, robbery and other statistical attacks as well as alterations.

The Institute for policy innovation (IPI) estimated the yearly breaches on films, music and softwares that were caused by violations of pirate rights, trillions of dollars, and thousands of job losses. Researchers reported a huge annual loss concerning cinema business in May 2014 alone. In addition to copyright, the privacy and security of multimedia data is crucial [1].

The image and electronic patient register (EPR) are, for example, transferred between unsecured web connections for the usage of medical images in e-health systems [2]. A minute modification in a medical image could result in a mistaken and thus fatal diagnosis. The cutting-edge algorithms are critical towards ensuring secure and dependable media in these circumstances.

Although, encryption is explored as a potential solution for specific scenarios, encryption methods entail visual and statistical changes in the data that usually are suspicious and leads to numerous attacks [3]. The disguise of information is an efficient and alternative method for security and authentication in multimedia images and IPR issues, including steganography as well.

1.2. Digital Image Watermarking

Digital image watermarking demonstrated that, it is one of the most advanced IPR protection and authentication solutions [4]. Digital watermarking is a technique that masks the host media information such as video, images, etc. It enables the protection of images, videos and works as a critical tool for dealing with numerous IPR-related multimedia problems.

An Institute's logo, a doctor's signature, history of cases, a personal logo etc., could be a digital watermark. Success rate of watermarking is typically influenced by numerous serious components like durability, payload, lack of perception and safety. If the image processing attacks were present, an aqueduct is considered resilient, i.e., a watermark is removed from an attacked image [5]. The number of concealed bits that can be included in a certain host media is called payload. While retaining the quality of the host media, the HVS system does not discover the existence of the watermark on the host media as extremely unknowable. If an opponent removes a flag of the watermark, the flag is safe, and without an encryption key it cannot be shown in acceptable forms [6].

1.3. Watermark Security

One of the fundamental problems in digital watermarking is the security of a watermark. Cryptographic techniques have proved a demanding factor in terms of security objectives, especially in medical image processing applications where anonymity is an essential aspect [7],[8].

2. Digital Image Watermarking of Medical Images

Digital image watermarking of medical images is considerably important so as to effectively prevent the medical information from being falsely used. The medical image watermarking of the space domain and the watermarking of the frequency domain are the two principal elements.

We have to integrate the watermark with pixel data over space domain techniques. However, image watermarks were employed to convert the coefficients of domain watermarking.

Well-evaluated approaches including DCT [9], DWT [10] and DFT [11] are the different conventionally employed domain transformation approaches.

3. Watermarking Algorithms

3.1. Discrete Cosine Transform

Normally signals handle effectively by DCT. The images become the frequency domain here. It is used in numerous areas such as pattern recognition, compression of information and medical image processing. In space domains, this technology is stronger than watermarking technologies [12]. Fig.1., shows the representation of watermark used to embed in DCT.

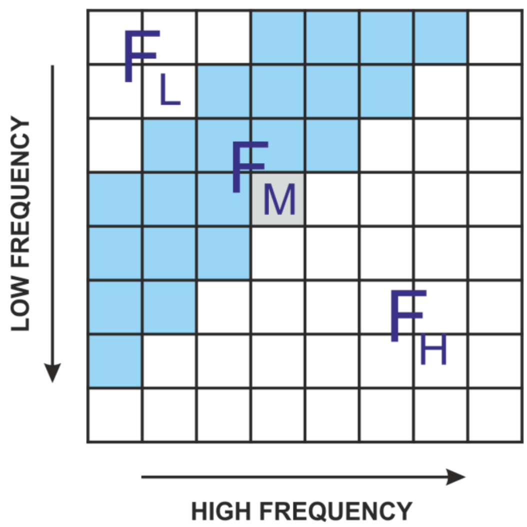


Fig.1. Watermark used to embed in DCT

3.2. Discrete Wavelet Transform

Consider a multi-resolution image with a DWT representation. This representation offers a simple base for interpreting the conception of image. In several resolutions, this DWT analyses the signal. DWT splits the image into two high and low-frequency quadrants. A single image is applied to the DWT. This process goes on until the signal has decomposed altogether.

This is separated into four parts, i.e., in two-dimensional images using DWT [13].

LL: In the original image, the visual characteristics are low. We might say that in this section the image was approximated.

LH: It is made up of vertical visual details.

HL: The image is original and has horizontal features.

HH: It includes information on the original image at high frequency.

As the information from the coefficients for low frequencies is known, the watermark is integrated into the coefficients of lower frequencies. The initial image was rebuilt from the decomposed image when IDWT is applied.

Fig.2., shows the schematic representation of level decomposition

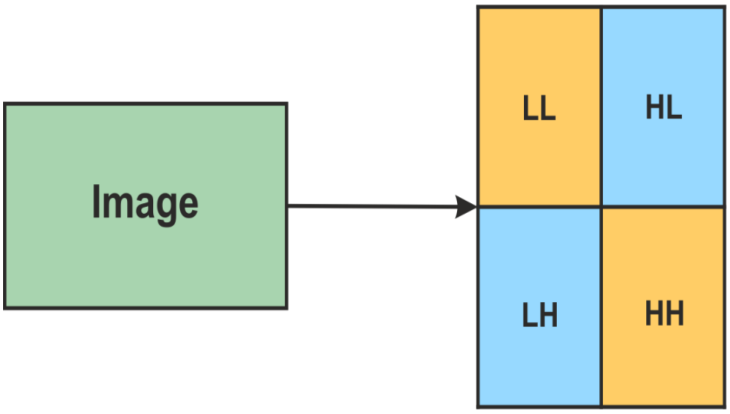


Fig.2. Level Decomposition

3.3. Discrete Fourier Transform

DFT enables increased resilience to geometric attacks like scaling, translating, spinning, etc. It divides the images into sine and cosine waveforms. Double-specific integration can be done using direct and template integrations. The DFT magnitude and phase coefficient are modified in the direct integration approach and is integrated with the watermark [14],[15].

The template-based approach of integration employs the concept of templates. During integration phase, we enter the template utilised for the DFT domain transformation factor. When the image is transformed, the first item in this templating is to resync.

4. Proposed Methodology

4.1. Discrete Wavelet Transform

DWT offers good location features of spatial frequency. Due to this, in DWT, watermarks can be constructed to maintain the host visual transparency. DWT possesses few of the most important advantages when compared to DCT. The images get separated into two categories of filters such as scalable and wavelet filters such as LL, LH, HL and HH.

The high frequency image subband HL possesses horizontal image details, and the LH sub-band possesses vertical image details. Low frequency corresponds to LL subband of an image.

4.2. Shuffled Singular Value Decomposition (SSVD)

The matrix $M \times N$ will be deconstructed as,

$$A = U \times S \times V^T \qquad (1)$$

The orthogonal matrix is that of the U-matrix ($M \times M$) and V matrix ($N \times N$). Left and right are called as single columns *U* and *V*. The horizontal and vertical images are displayed based on this. S $M \times N$ matrix is a single diagonal value matrix (SVs). The grey layer values *U* and *V* are specified in the matrix *S*.

Due to the stability of unique values, SVD is commonly employ in various image processing and medical image processing applications. Even if the matrix is rotated or transposed, these individual values remain unchanged. SVD is also fairly all-pervasive as rectangle as well as square matrices is feasible.

Several SVD approaches for medical image watermarking are commonly acclaimed for their enhanced features. The host or transform domain with set watermark values is included in several SVD-based systems.

The correlation values of the retrieved and implanted watermarks after various image processing and geometer attacks display exceptionally strong approaches. Such systems, however, face false positive developments. False positive means, a false watermark is removed from a picture where the watermark fully differs from the original watermark.

This happens when there is a significant association between the matrix of the singular value and appropriate watermarking. In SSVD, before decomposition into *U, S, V*, the image components are shuffled. In this proposed system, shuffled image is extracted as shown in the Fig.3.

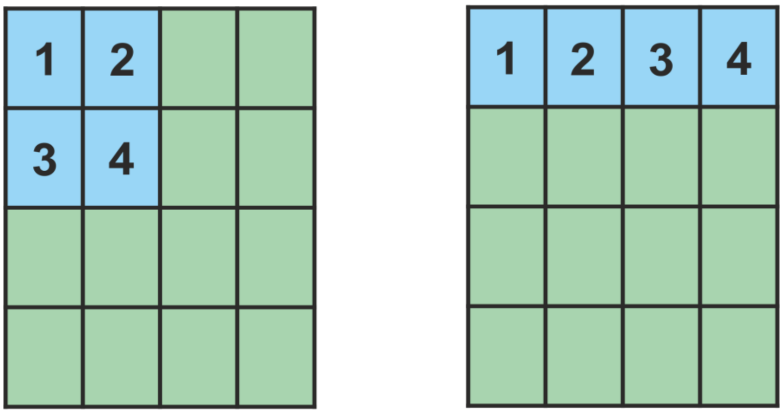


Fig.3. Shuffled matrix

Embedding watermark in the image

- Apply SSVD to the image.
- Image is broken into small pieces of n x n size.
- Shuffling is done as shown in the Fig.3.
- Apply SVD as: $X = U_W \times S_W \times V_W^T$
- The principal component of watermarking is evaluated as:

  $PC=U_W \times S_W$

- Just by applying DWT, the image is subdivided into 4 components LL, LH, HL and HH.
- With size of m x m, LL subband is further splitted into small components.
- Then, SVD is applied to perform decomposition by using the expression,

  $$LL(i, j) = U \times S \times V^T$$

- The image block (i,j) has the largest singular value equal to the first member of the S matrix, known as $\lambda_{max}\ i, j$
- In order to change the greatest single value of each block, the watermark principle components are applied.
- Inverse SVD is applied to each block to create the modified LL sub-band.
- The watermarked image is produced by IDWT by executing modified LL subband DWT on the original LL image. Fig.4. shows the watermark embedding in the proposed method.

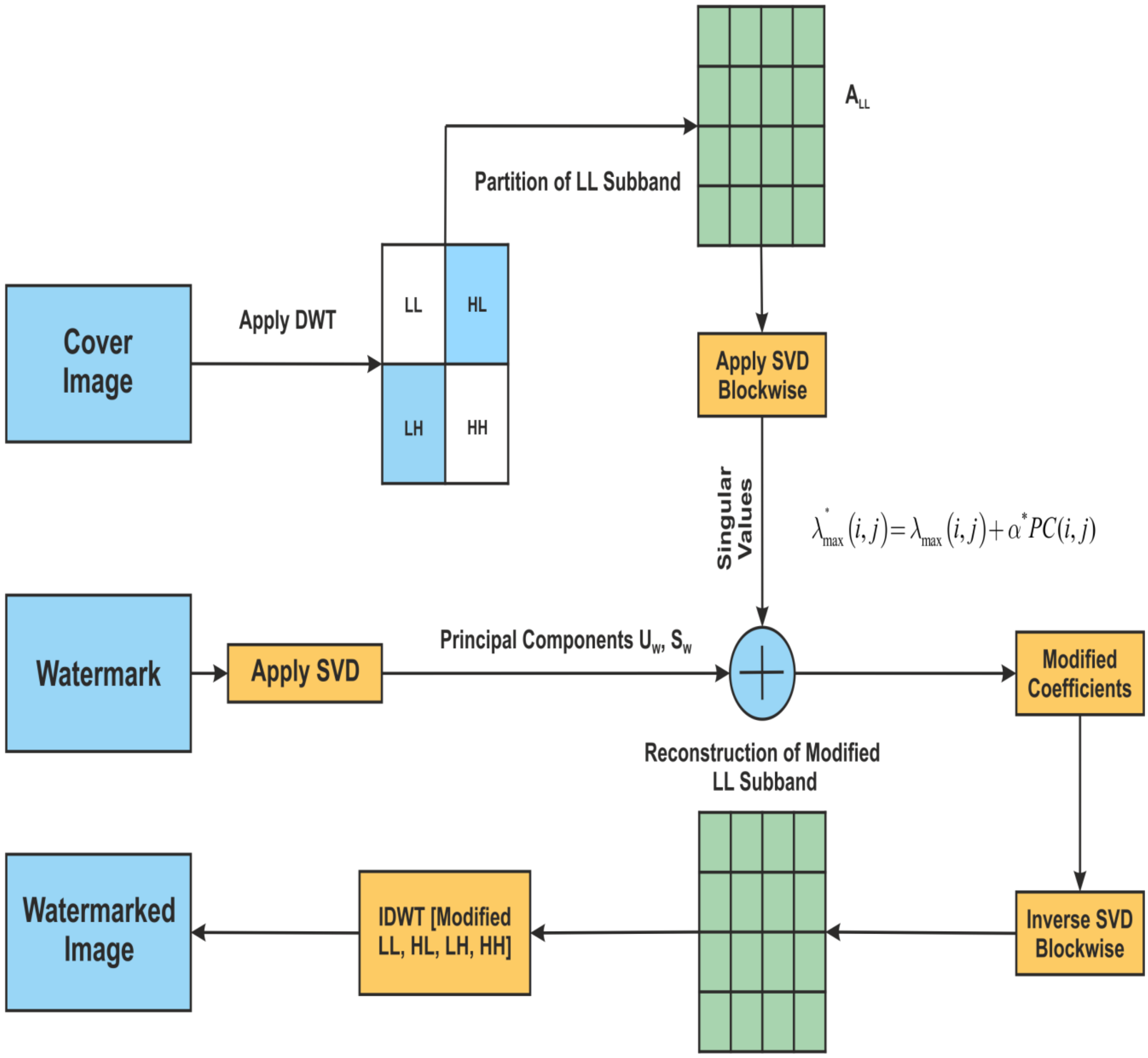


Fig.4. Watermark embedding in the Proposed Method

Extraction of watermark

- Using one DWT level, the potentially corrupted watermarked image is splitted into four sub-bands, LL, HL, LH and HH.
- Apply SVD to obtain the principal components:

$$W_{US}^{*}(i,j)=\frac{1}{\alpha}\left(\lambda_{\max}^{*}(i,j)-\lambda_{\max}(i,j)\right)$$

$$W^{*}=W_{US}^{*}(i,j)V_{W}^{T}$$

- For watermark extraction, Inverse shuffling is used. Fig.5. shows the complete processes involved in extracting the watermark.

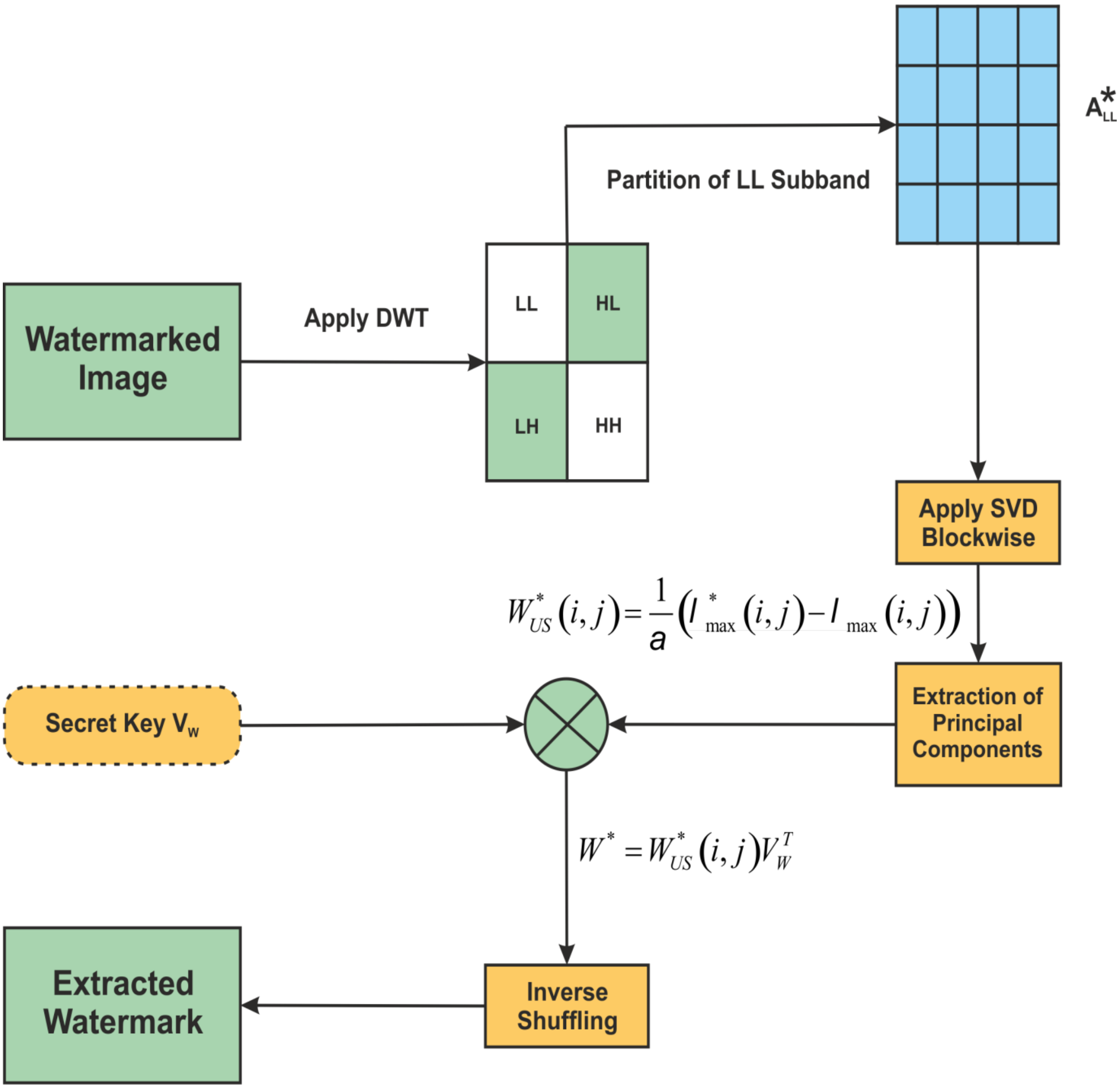


Fig.5. Process of watermark extraction in Proposed Method

5. Results and Discussions

An examination and assessment of the proposed watermarking algorithm's effectiveness is carried out by considering medical images for all concerned potential attacks, and the result were validated using some image quality parameters including Peak signal-to-noise ratio (PSNR), Normalized cross correlation (NCC) and Structure similarity index (SSIM). The parameters that were used for simulation are given in Table 1.

Table 1. Simulation Parameters

Parameters	**Type**
Image Type	Dicom Image
Filters	Median, Average
Noise ratio	5, 25, 45, 65, 85 (in percentage)
Noise type	Gaussian, Salt and pepper
Metrics	PSNR, NC, SSIM

5.1. Peak Signal to Noise Ratio

PSNR is the most often used image quality assessment parameter. The watermark quality is evaluated by calculating the PSNR for the watermarked image with respect to the cover image. Considering, C as the cover image and Cw as the watermarked image, then PSNR can be expressed mathematically as,

$$PSNR - 10\log_{10}\left(\frac{R2}{MSE}\right) \qquad (2)$$

Where, MSE is the mean square error and is expressed mathematically as,

$$MSE = \frac{\sum_{M,N}\left[l_1(m,n) - l_2(m,n)\right]^2}{M \times N} \qquad (3)$$

The formula for calculating the size of C, given the size of Cw is M×N. More better the PSNR, the better is the image quality. The PSNR of a watermarked image should be as high as possible.

5.2. Normalized Correlation

The degree of similarity between the original watermark and the derived watermark is expressed in terms of NC [16].

$$NC = \frac{\sum_i \sum_i W(i,j) \times W_X(i,j)}{\sum_i \sum_i \left[W(i,j)\right]^2} \qquad (4)$$

If we substitute W for the original watermark and Wx for the extracted watermark, it should be near to unity in the correlation between the two images.

5.3. Structural Similarity Index Metric

SSIM [17], which is supposed to be linked to the overall quality assessment of the HVS, is utilised to estimate the degree of similarity between the original colour image i and the watermarked image w

$$SSIM(x,y) = \left[l(x,y)\right]^{\alpha} \times \left[c(x,y)\right]^{\beta} \times \left[s(x,y)\right]^{\gamma} \qquad (5)$$

Where, l(Ix,y) signifies the luminance comparison function, c(x, y) corresponds to the contrast comparison function, s(x, y) represents the structure comparison function.

5.4. Capacity Analysis

Each DCT block of the cover image contains one bit of watermark. As a result, the total number of bits that can be embedded into a 512×512 grey scale image is 4096. The corresponding number for a 512×512 colour image is 4096, and, as 4096 bits can be inserted into each colour plane of the image, a total of 12308 bits can be embedded, and when compared to certain existing procedures, it is very much lesser.

5.5. Perceptual Quality Analysis

The 64×64 binary watermark displayed in Fig.6., was embedded in a variety of different sized grey scale images which are 512×512 in size.

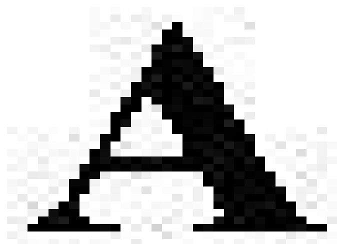
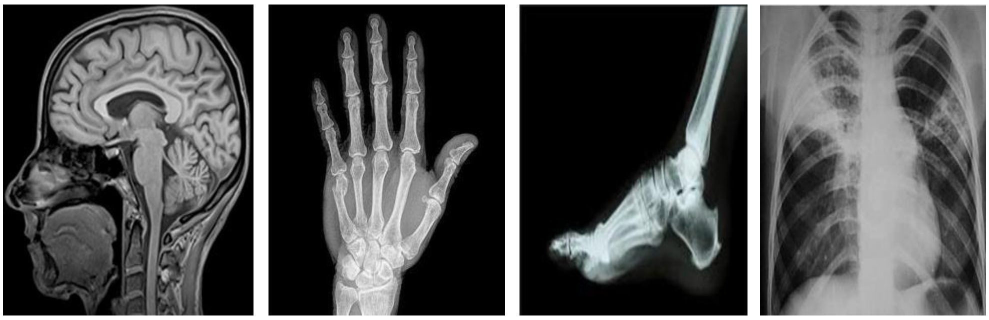


Fig.6. Watermark of size 64 ×64

Measuring the magnitude of PSNR from a range of about 39 dB to over 41 dB suggests that, the watermarked image is of superior quality. Fig.7., shows various 512×512 images for an examination of the proposed medical image watermark embedding algorithm and the corresponding watermarked image is displayed in Fig.8.

HEAD HAND FOOT LUNGS WATERMARK

Fig.7. Original host images



HEAD HAND FOOT LUNGS

Fig 8. Watermarked image

Table 2. Objective quality metrics for host image

IMAGES	PSNR (dB)	SSIM	NCC
Head	41.86	0.9876	1
Hand	43.60	0.9675	1
Foot	42.98	0.9656	1
Lungs	41.40	0.9876	1

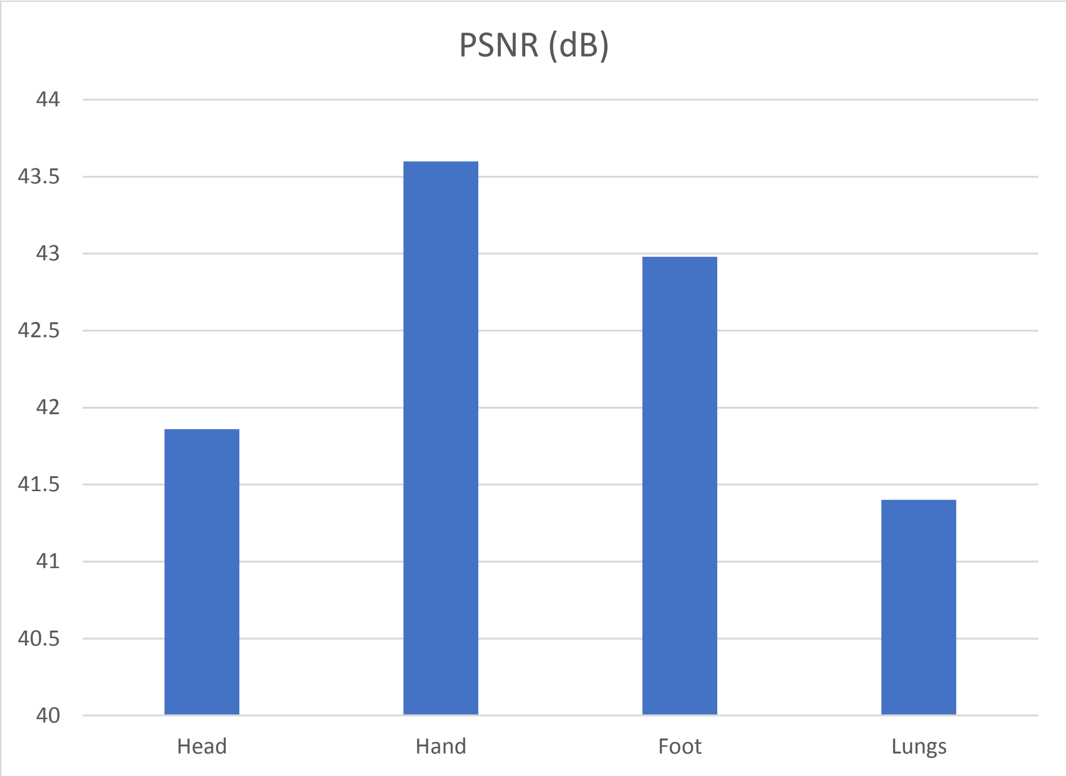


Fig.9. PSNR for host image

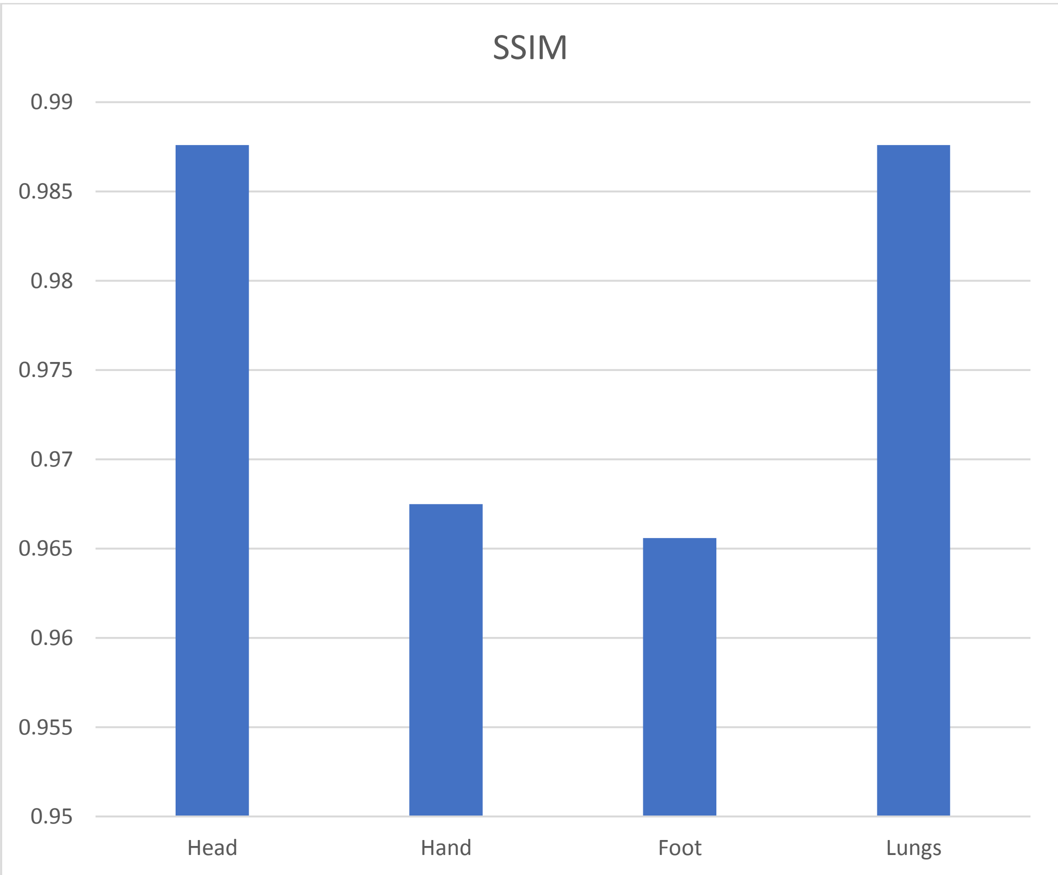


Fig.10. SSIM for host image

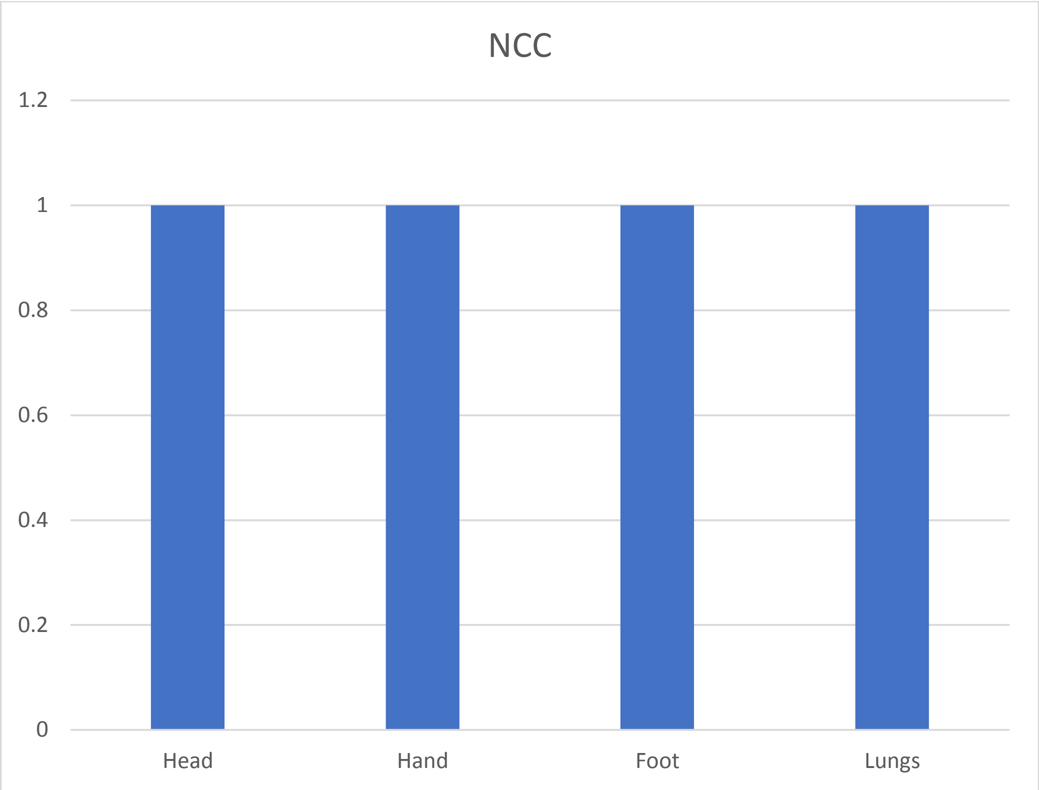


Fig.11. NCC for host image

Figs.9-11 shows the PSNR, SSIM and NCC for the host image. As objective parameters, SSIM and PSNR have been used in Table 2 to analyse the quality of the watermarked image.

With the proposed approach, images with an overall quality range of 39 dB to 43 dB would be created. In addition, the extraction algorithm is validated as correct because the logos were not found in the marked media. When it comes to the PSNR of watermarked images, embedding strength S has a substantial impact.

5.6. Robustness Analysis

Robust watermarking refers to watermarking media that gives rise to a visible watermark even after it has been subjected to attacks.

Attacks such as rotation, cropping, resizing, filtering, or the insertion of noise was used to test the robustness of this proposed system.

NCC and SSIM were adopted for the sake of system robustness.

5.7. Watermark Extraction after Gaussian Noise

With zero mean and variance of 0.005, the PSNR of the watermarked image after adding Gaussian noise is shown in Fig.12., the corresponding extracted watermark images after gaussian noise is shown in Fig.13.

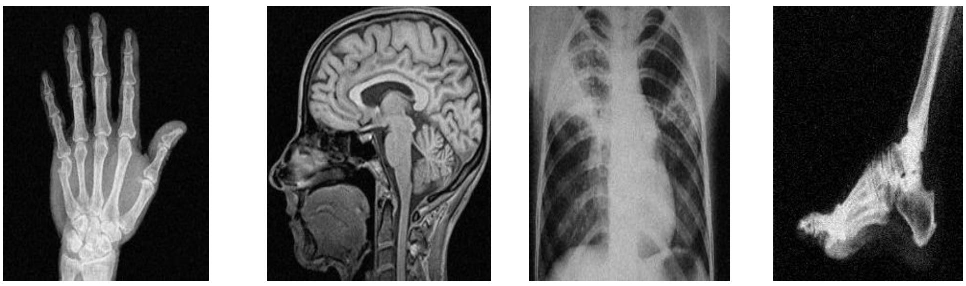


Fig.12. Gaussian noise attacked images

Hand head Lungs Foot

Fig.13. Extracted watermark images after Gaussian noise

5.8. Watermark Extraction after Salt and Pepper Noise

Fig.14, depicts the salt and pepper noise attacked images with noise density = 0.002, and the analogous extracted watermark images after noise is shown in Fig.15.

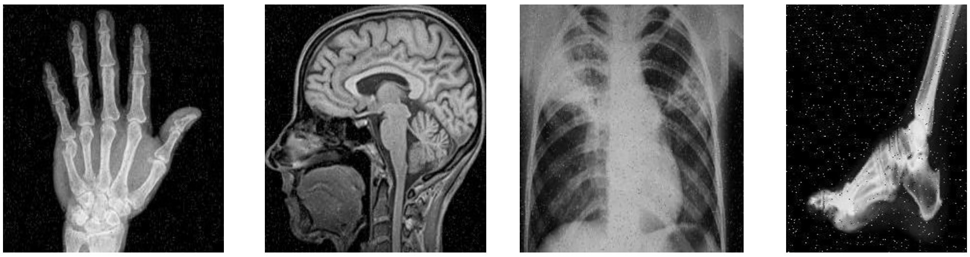
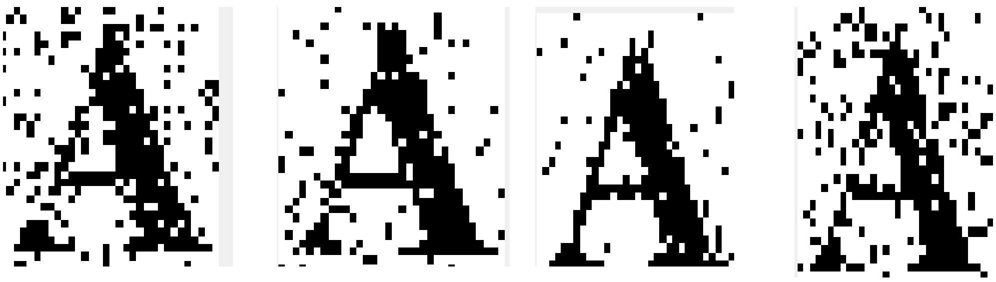


Fig.14. Salt and pepper noise attacked images



Hand head Lungs Foot

Fig.15. Extracted watermark images after salt and pepper noise

5.9. Watermark Extraction after Average Filtering

Fig.16., shows the average filter of size 3x3 attack images and the final watermark extraction is shown in Fig.17.

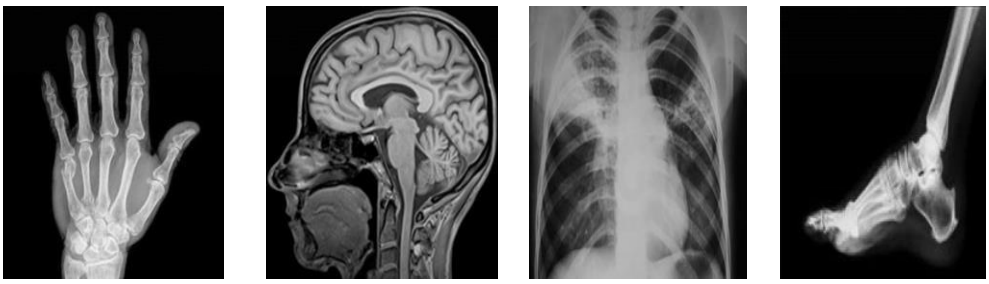
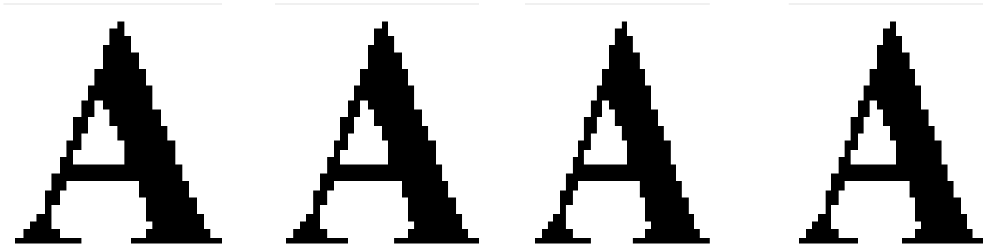


Fig.16. Average filter attack images



Hand Head Lungs Foot

Fig.17. Extracted watermark images after average filter

5.10. Watermark Extraction after Median Filtering

A median filter of size 3×3 is applied to the watermarked images are shown in Fig.18., and the corresponding extracted watermark images are shown in Fig.19.

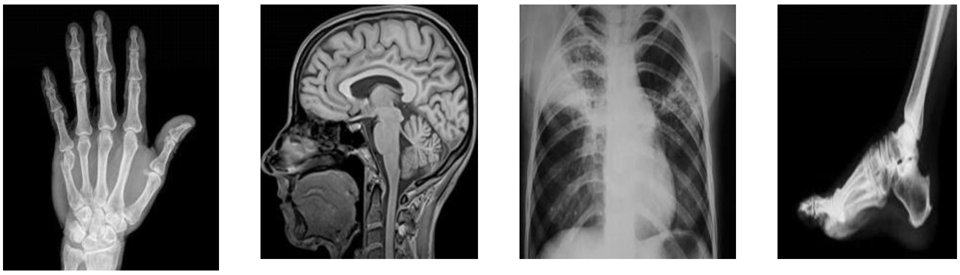
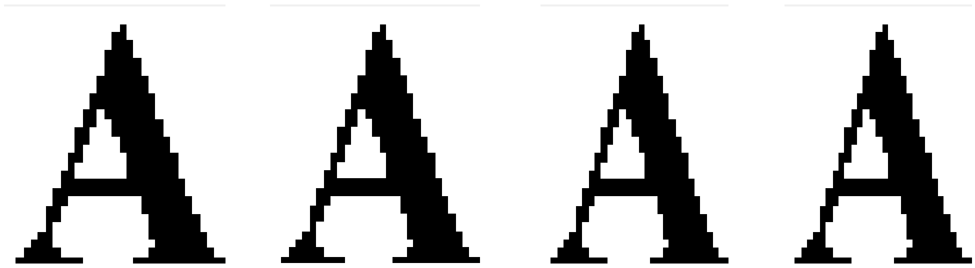


Fig.18. Median filter attacked images



Hand head Lungs Foot

Fig.19. Extracted watermark images after median filter

Table 3. PSNR and NCC values of extracted watermark against different noise attacks

IMAGE	PSNR (dB)				NCC			
	ussian noise	**Salt & pepper**	**Average filtering**	**Median filtering**	**ussian noise**	**Salt & pepper**	**Average filtering**	**Median filtering**
Foot	8.02	9.731	32.57	32.57	0.8656	0.8967	0.8976	**0.9786**
Hand	8.135	9.13	32.57	32.57	0.9445	0.9786	0.8796	**0.9872**

Head	10.31	10.70	32.57	32.57	0.9405	0.8768	0.9876	**0.9731**
Lungs	**13.04**	**13.35**	**22.65**	**23.56**	**0.9872**	**0.8967**	**0.9786**	**0.9620**

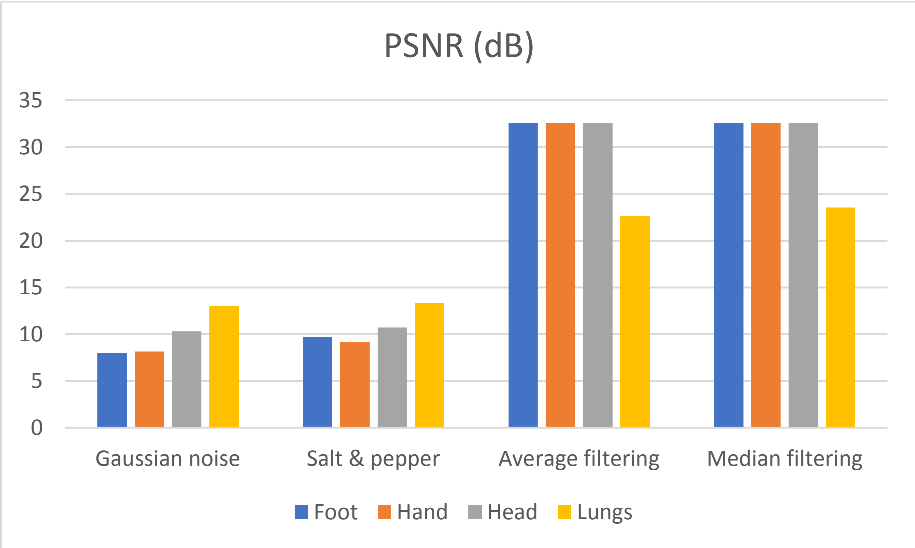


Fig.20. Comparison of PSNR with different noise attacks

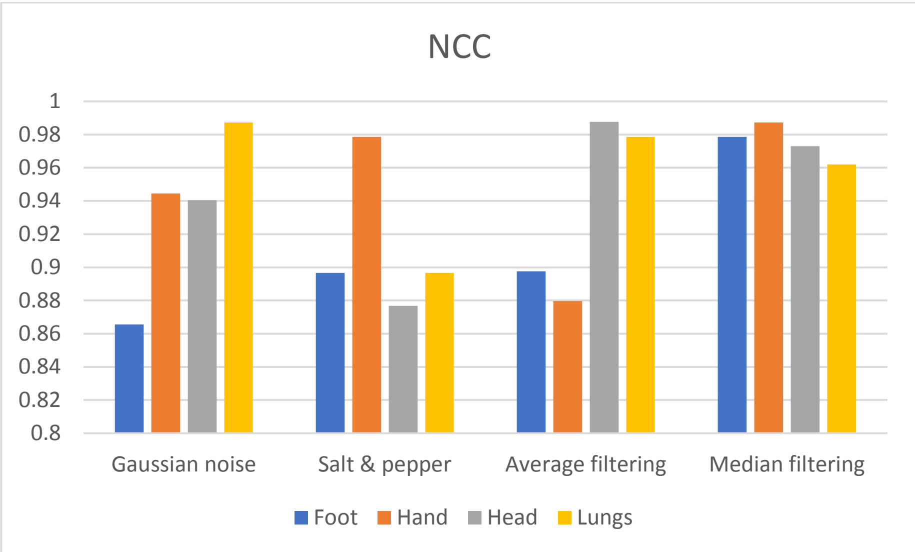


Fig.21. Comparison of NCC with different noise attacks

On the other hand, in Table.3. & Figs.20-21, we can see that the watermarked images were treated to a 0.02 mS/m noise density of salt and pepper noise, and a zero mean and variance of Gaussian noise. With these results, we can see that the results are robust to distortion, such as a noticeable watermark. The system was seen to be robust towards image filtering such as 3×3 median filtering and 3×3 average filtering attacks, the robustness of the system was examined with 3×3 median filtering and 3×3 average filtering attacks. Robust against filtering attacks does, in fact, yielded better results.

6. Conclusion

In this paper, a novel medical image watermarking system using SVD based approach was investigated. The operation of proposed method uses the advantages of both DWT spatial-frequency decomposition property and single value stability characteristics. This strategy demonstrates good stability against numerous peers. This methodology is deprived of false positive problems, unlike most SVD techniques. The PSNR and Correlation coefficient data are also displayed in this study for various scale factors and cover images. This strategy can therefore be used for all medical image scenarios. The image processing functions such as filtering, Gaussian noise, etc., were executed in the test environment to verify if the performance would meet or exceed the needed requirements. The comparison results showed that, the proposed system is more imperceptible, robust, and has a lower payload than the previously proposed methods. Additionally, the incorporated watermark's double layer of protection further ensures that this method is highly secure in nature. Hence, it can be concluded that the application of copyright protection and ownership verification are suitable with the suggested scheme over medical images. As such, this proposed scheme can be used to tackle various medical image integrity concerns and also handles critical security issues effectively in modern telemedicine and e-healthcare applications.

References

[1] Maurya, R., Kannojiya, A. K., & Rajitha, B. (2020). An Extended Visual Cryptography Technique for Medical Image Security. 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). doi:10.1109/icimia 48430.2020.9074910.

[2] Pai, M.M.M., Ganiga, R., Pai, R.M. et al. Standard electronic health record (EHR) framework for Indian healthcare system. Health Serv Outcomes Res Method (2021). https://doi.org/10.1007/s10742-020-00238-0.

[3] Banu S, A., & Amirtharajan, R. (2020). A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. Medical & Biological Engineering & Computing. doi:10.1007/s11517-020-02178-w.

[4] Begum, M., & Uddin, M. S. (2020). Analysis of Digital Image Watermarking Techniques through Hybrid Methods. Advances in Multimedia, 2020, 1–12. doi:10.1155/2020/7912690.

[5] Paul, R., Schabath, M., Gillies, R., Hall, L., & Goldgof, D. (2020). Mitigating Adversarial Attacks on Medical Image Understanding Systems. 2020 IEEE 17th International Symposium on Biomedical Imaging (ISBI). doi:10.1109/isbi45749.2020. 9098740.

[6] Bhargava, N., Sharma, M. M., Garhwal, A. S., & Mathuria, M. (2012). Digital image authentication system based on digital watermarking. 2012 International Conference on Radar, Communication and Computing (ICRCC). doi:10.1109/icrcc.2012.6450573.

[7] Haddad, S., Coatrieux, G., Moreau-Gaudry, A., & Cozic, M. (2020). Joint Watermarking-Encryption-JPEG-LS for Medical Image Reliability Control in Encrypted and Compressed Domains. IEEE Transactions on Information Forensics and Security, 15, 2556–2569. doi:10. 1109/tifs.2020.2972159.

[8] Tufail, H., Zafar, K., & Baig, R. (2018). Digital Watermarking for Relational Database Security Using mRMR Based Binary Bat Algorithm. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). doi:10.1109/trustcom/bigdatase.2018.00298.

[9] Ravi, P., & Krishnan, J. (2018). Image Enhancement with Medical Image Fusion using Multiresolution Discrete Cosine Transform. Materials Today: Proceedings, 5(1), 1936–1942. doi:10.1016/j.matpr.2017.11.296.

[10] Aravindan, T. E., & Seshasayanan, R. (2019). Medical image DENOISING scheme using discrete wavelet transform and optimization with different noises. Concurrency and Computation: Practice and Experience. doi:10.1002/cpe.5540.

[11] Nayak, J., Bhat, P. S., Acharya U, R., & UC, N. (2004). BioMedical Engineering OnLine, 3(1), 17. doi:10.1186/1475-925x-3-17.

[12] S. Kushlev and R. P. Mironov, Analysis for Watermark in Medical Image using Watermarking with Wavelet Transform and DCT, 2020 55th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST), 2020, pp. 185-188, doi: 10.1109/ICEST49890.2020.9232700.

[13] B. P. Kulkarni, S. Sai Krishna, K. Meenakshi, P. Kora and K. Swaraja, Performance Analysis of Optimization Algorithms GA, PSO, and ABC based on DWT-SVD watermarking in OpenCV Python Environment, 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-5, doi: 10.1109/INCET49848.2020. 9154134.

[14] D. Rosiyadi, H. Prasetyo, S. J. Horng and A. Indra Basuki, "Security Attack on Secret Sharing Based Watermarking Using Fractional Fourier Transform and Singular Value Decomposition," 2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), 2020, pp. 343-347, doi: 10.1109/ICRAMET51080. 2020.9298671.

[15] S. Sheidani and Z. Eslami, "Blind Multipurpose Image Watermarking Based on Secret Sharing," 2019 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), 2019, pp. 1-8, doi: 10.1109/ISCISC 48546.2019.8985160.

[16] J. Liu, W. wang, S. Shen and X. Jiang, "A New Lateral Cephalogram Image Stitching Technique Using Gaussian Mixture Model and Normalized Cross-Correlation," 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2021, pp. 1574-1579, doi: 10.1109/IAEAC50856.2021.9390708.

[17] E. Alexiou and T. Ebrahimi, "Towards a Point Cloud Structural Similarity Metric," 2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 2020, pp. 1-6, doi: 10.1109/ICMEW46912.2020.9106005.