Journal of Engineering, Applied Science and Humanities

**Publisher:** Sunyani Technical University **[European Article Number:** 17908875546877**]**
**ISSN:** 2773-8418 (Print), **ISSN** 2773-8426 (Online) **[**© 2021 Science Publications**]**

# IMPLEMENTATION OF MEDICAL IMAGE WATERMARKING USING RDWT AND SVD FOR SECURE MEDICAL DATA TRANSMISSION IN HEALTHCARE SYSTEMS

**[1]Atianashie Miracle A, [2]Chukwuma Chinaza Adaobi, [3]Eneji Samuel Eneji, [4]Ibe Walter Eyong, [5]Ajie Gospel Ozioma & [6]Angib Maurice Udie**

[1,2]Catholic University College of Ghana

[3, 4, 5,6]Federal College of Education Obudu Cross River State, Nigeria

**Received 2021-07-14, Revised 2021-08-27, Accepted 2021-10-10**

**Abstract:** In telemedicine, the authenticity and integrity of medical images must be safeguarded. Copyright protection is provided through robust medical image watermarking (MIW) methods, and the original pictures may be retrieved at the receiver's end. But existing algorithms have limits in terms of balancing the tradeoff between robustness, imperceptibility, and embedded capacity. Aside from that, most MIW algorithms aren't built for color images. This article proposes a novel MIW technique based on the redundant discrete wavelet transform (RDWT) with singular value decomposition (SVD) to increase their performance in preserving medical color picture information. First and foremost, the RDWT-SVD is a reliable solution as compared to the conventional DWT. Second, modifying the wavelet domain coefficient ensures that integer values in the spatial domain change and that the watermarking process is reversible. Finally, the embedding approach makes full advantage of the original image's features and watermarking. The simulation results showed that the proposed method decreases the amount of original picture change and improves imperceptibility as compared to the conventional approaches.

**Keywords:** RDWT, SVD, MIW

## 1. INTRODUCTION

Growing use of Internet and exchange of information electronically has resulted into ever increasing need of security services specific to the type of data or information being protected [1]. Authentication and non-repudiation are two major services of information security and MIW is a commonly used method. Data in the form of multimedia content is exploding and hence digital image watermarking is an active research area. Transform domain methods for image watermarking are popular for robustness and imperceptibility (RIS). A lot of applications like digital copyrights management and protection make digital image watermarking a very active research field [2]. Internet has made it easy for people to share, promote and sell their intellectual property such as images, videos, documents, etc., which calls for protection of publishing copyright. A quick search on Google Scholar for research articles since 2015 for MIW returns 16,600 results: this gives an idea how active the area is. Because of rapid advancements in current technologies such as communication, networked multimedia systems, and digital data storage, all business applications have been shifting towards the digital era in recent years. In addition, during the last two decades, the usage of the internet in the corporate environment has quickly risen in order to gain more efficiency, convenience, and security by incorporating digitalization into their work. Text, pictures, music, video, and software are examples of digital data that are exchanged across an open public network and must be protected [3].

MIW is a novel method that can be used in medical, military, and archive applications [4]. The MIW also known as a digital signature, ensures the validity of a document. A watermark might be unique to each copy (for example, to identify the intended recipient) or shared by several copies (e.g., to identify the document source). The

**Publisher:** Sunyani Technical University **[European Article Number:** 17908875546877**]**
**ISSN:** 2773-8418 (Print), **ISSN** 2773-8426 (Online) **[**© 2021 Science Publications**]**

implanted watermarks, which can be in the form of text, picture, audio, or video, are difficult to remove and usually undetectable [5]. The insertion of a hidden watermark in digital data, regardless of how inconspicuous it is. However, the resulting embedded digital data suffers some deterioration. Reversible watermarking, which is regarded the best technique over encryption, has been created to circumvent this and obtain the original data. Finally, this work implemented the RDWT-SVD for geometric correction is adjusted so that attack parameters may be predicted more precisely with less data. This improves the proposed scheme's resistance against geometric assaults like rotation and scaling. The suggested approach is resistant to both common and geometric assaults and offers a large embedding capacity without causing visible picture distortion. Rest of the article contains as follows: Section 2 related work with drawbacks, section 3 detailed analysis of proposed method. Section 4 results and discussions and Section 5 conclusions and future works.

Image transforms used in the literature are DFT, Fractional Fourier Transform (FrFt) [6], DCT, Discrete Hadamard Transform (DHT) [7], SVD, DWT [8] and Contourlet Transform (CT) etc.
In [9] authors addressed DHT based MIW schemes have been used. Two of them are standard DCT embedding and standard SVD embedding. Third the authors have proposed to use BFOA for embedding. The standard procedure of DCT embedding is: applying forward DCT embedding the watermark in lower band using coefficients derived through pseudorandom function seeded with a key and inverting DCT to obtain watermarked image.

In [10] authors presented the standard procedure of SVD is to decompose image using SVD, inserting watermark in the diagonal matrix then applying SVD again to a linear function lastly stego image is formed by combining matrices from each step. In [11] authors presented DCT-SVD based extraction, the key is used to seed the pseudorandom generator and the coefficients are then used on the image decomposed using forward DCT. Computed vector is rearranged into the watermark. In [12] authors have proposed how to embed a grayscale watermark in host image which is colored. They have used uncorrelated color space for this purpose. Moreover, genetic algorithm is used for optimization. In [13] authors investigated the extraction process takes the RGB image as input and converts it to DFT form. DFT decomposition is then applied twice to obtain the middle sub subcomponent. Watermark image is obtained through inverse computation of embedding function. Unscrambling uses the secret key to rearrange the 16 blocks of watermark image.

In [14] authors presented the watermark image is divided into 16 blocks. The blocks are scrambled using a DWT-SVD and a pseudorandom number generator. A linear addition of watermark areas and corresponding 16 areas of third level component of host image using the coefficients is done to obtain the watermarked image. The watermarked image is then post-processed using inverse DCT transform. In [15] authors presented the quality of watermark image extracted can be improved through use of a NSCT optimization process. The tradeoff between quality and robustness is to be optimized. The Embedding strength factors used in linear computation of embedding decides this tradeoff. Authors observe that robustness is with attacks hence these attacks should be somehow incorporated into fitness function

## 2. MATERIALS AND METHODS:

MIW is a method of protecting medical digital files against unlawful usage. Further, MIW is the most prevalent authentication approach for protecting data from any form of misuse while it is being sent. A new MIW approach for biological photographs is proposed in this research. The biological picture is first preprocessed in the model using enhanced successive mean quantization transform called as RDWT, which also employs SVD decomposition. RDWT and IRDWT are then used to insert the watermark in the picture. Finally, using the inverse

**Publisher:** Sunyani Technical University **[European Article Number:** 17908875546877**]**
**ISSN:** 2773-8418 (Print), **ISSN** 2773-8426 (Online) **[**© 2021 Science Publications**]**

operation of the embedding technique, the watermark is recovered from the biological picture.

This work presents a novel technique for protecting medical pictures from assaults based on chaotic systems. A high-speed permutation process and adaptive diffusion are the two key components of the proposed technique. The chi-square test is also used to analyses the regularity of the histogram objectively. Key sensitivity analysis shows that photos cannot be decrypted even if the key is changed slightly, indicating that the technique is acceptable. Clearly, a portion of special pictures, such as an all-white image and an all-black image, is picked to test the selected plain-text. The suggested embedding and extraction methods for implementing a MIW system utilising the RDWT-SVD methodology are described in this section. Figure 1(a) depicts the suggested watermark embedding technique.

### 2.1 Watermark embedding

The following are the steps in the watermark embedding algorithm:

**Step 1:** Choose and read both the cover and watermark images.

**Step 2:** Use RDWT to break the cover picture (I) down into four sub-bands: HH, LH, HL, and LL as shown in figure 2.

**Step 3:** For LL sub band components, use SVD to derive single components U, S, and V.

**Step 4:** Now deconstruct the watermark picture with RDWT to get four sub-bands designated HH1, LH1, HL1, and LL1.

**Step 5:** Use SVD to extract singular components from the watermark image's decomposed LL1.

**Step 6:** Now use the following watermark embedding equation to generate the $S_{I^*}$

$$S_{I^*} = S_I + \alpha * S_W \quad (1)$$

Where $S_I$ denotes the obtained SVD coefficients of LL from step 3 while $S_W$ is obtained SVD coefficients of LL1 from step 5.

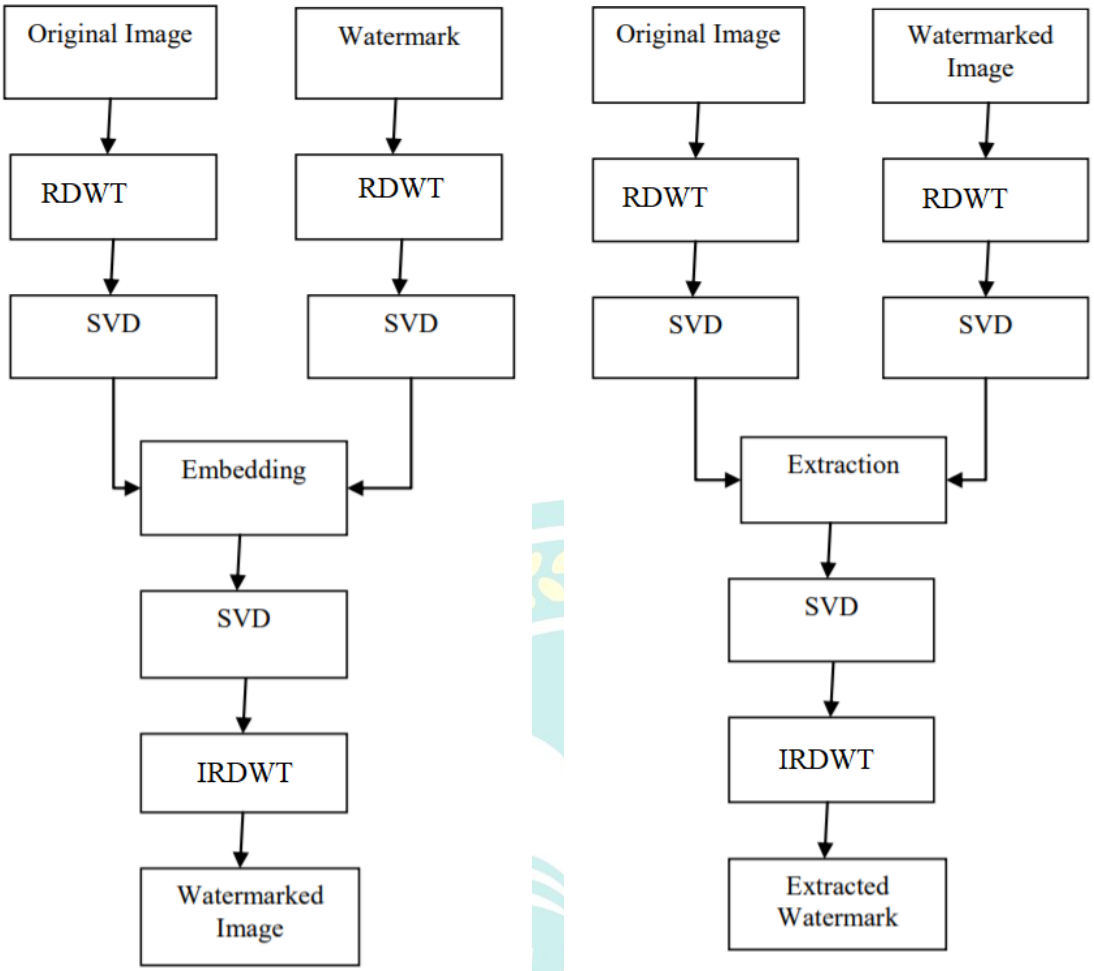
Where $S_I$ indicates the SVD coefficients of LL acquired in step 3 and $S_W$means the SVD coefficients of LL1 obtained in step 5.

**Step 7:** Now, using the equation (2), obtain the updated LL sub-band:

$$W_{LL} = U_I * S_{I^*} * V_I \quad (2)$$

**Step 8:** To produce a watermarked picture, apply inverse RDWT to the adjusted LL sub-band as well as LH, HL, and HH.

**Publisher:** Sunyani Technical University **[European Article Number:** 17908875546877**]**
**ISSN:** 2773-8418 (Print), **ISSN** 2773-8426 (Online) **[**© 2021 Science Publications**]**




(a) Embedding process (b) Extraction process

Figure 1: The suggested architecture for protecting the transfer of medical data.

**2.2. Watermark extraction**

Extraction is the inverse of embedding, in which the embedded watermark is retrieved using information collected during embedding that is only known by the authorised user, such as side information and ESFs. On a watermarked picture, the RDWT-SVD based DIW extraction procedure is as follows:

**Step 1:** Read the image with the watermark.

**Step 2:** Use RDWT to break it down into four sub-bands: HH2, LH2, HL2, and LL2.

**Step 3:** For LL sub band components, use SVD to derive single components U, S, and V.

**Step 4:** Next, remove the watermark as follows:

$$S_E = (S_W - S_I)/\alpha \quad (3)$$

$$E_{LL2} = U_{LL2} * S_E * V_{LL2} \quad (4)$$

**Step 5:** On extract the watermark, apply inverse RDWT to $E_{LL2}$ and LH2, HL2 and HH2.

**Publisher:** Sunyani Technical University **[European Article Number:** 17908875546877**]**
**ISSN:** 2773-8418 (Print), **ISSN** 2773-8426 (Online) **[**© 2021 Science Publications**]**

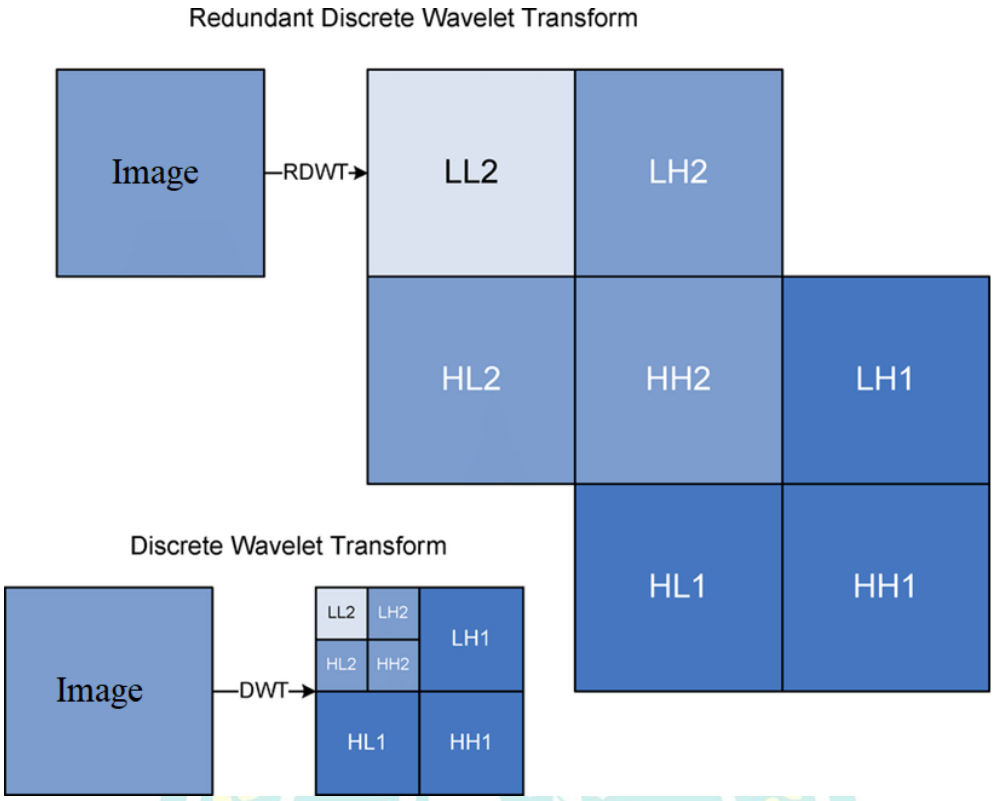
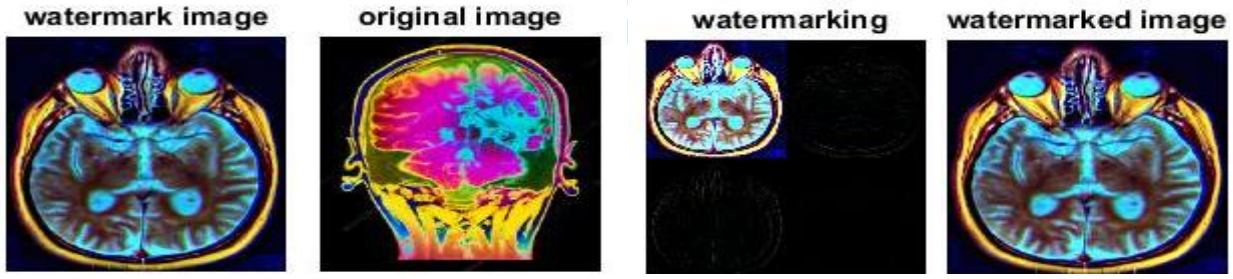



Figure 2: RDWT technique of decomposition

### 3. RESULTS DISCUSSION

This section presents the detailed simulation analysis using MATLAB R2016a software. To begin, the best adaptive scaling factor for watermarks with different sizes is determined by analyzing the scaling factor across NCC, PSNR, and SSIM. In the trials, the adaptive optimum scaling factors of watermarks with different sizes are employed. Subjective observation and objective quantitative analysis are used to detect the suggested method's invisibility and resilience. Furthermore, a variety of assaults with varying characteristics are employed to test the resilience. Finally, the suggested method's invisibility and robustness are compared to previous studies.




(a) (b) (c) (d)

Figure 3: watermark embedding images

**Publisher:** Sunyani Technical University **[European Article Number:** 17908875546877**]**
**ISSN:** 2773-8418 (Print), **ISSN** 2773-8426 (Online) **[**© 2021 Science Publications**]**

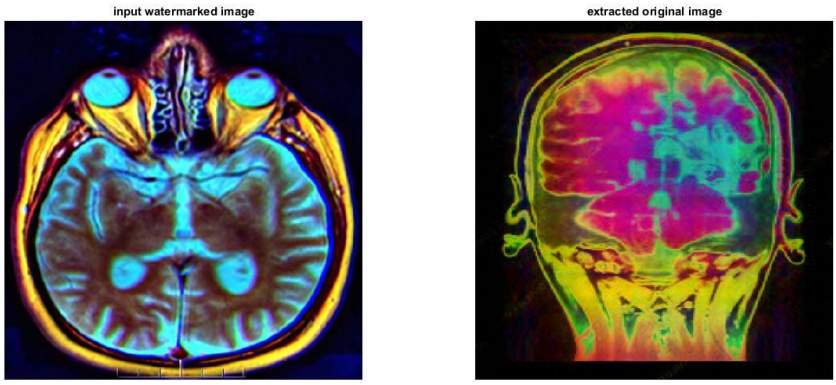



Figure 4: watermark extraction image

Figure 3 represents the watermarking embedding process with RDWT decomposition. Here, the original image is the CT scanned image and watermark image is the MRI scanned images. By using the RDWT decomposition, the original image is perfectly hided and generated the watermarked image as presented in Figure 3 (d) and looks like MRI image only, respectively. Figure 4 presents the watermark extraction process, the extracted images look similar like the original CT image, respectively.

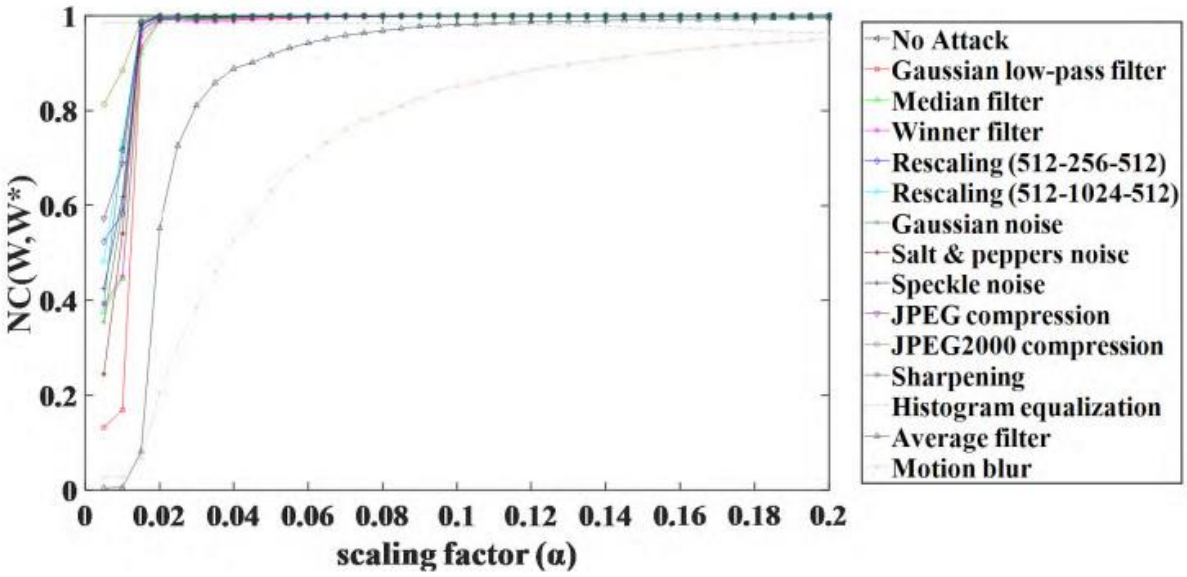



Figure 5: Performance of NCC under various attacks for various values scaling factor

**Publisher:** Sunyani Technical University **[European Article Number:** 17908875546877**]**
**ISSN:** 2773-8418 (Print), **ISSN** 2773-8426 (Online) **[**© 2021 Science Publications**]**

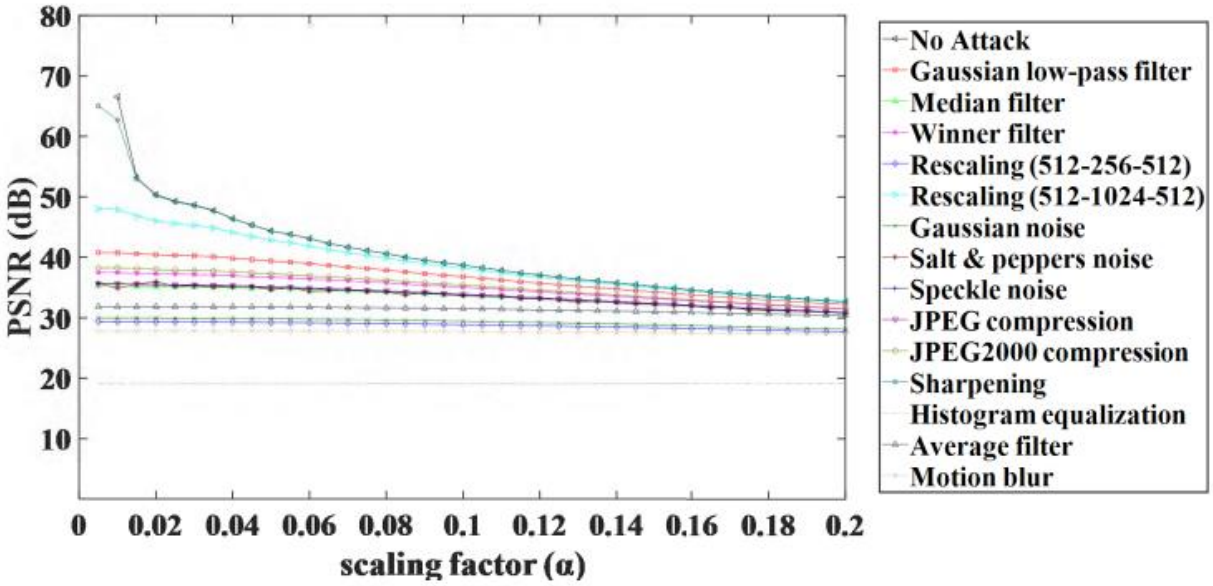



Figure 6: Performance of PSNR under various attacks for various values scaling factor

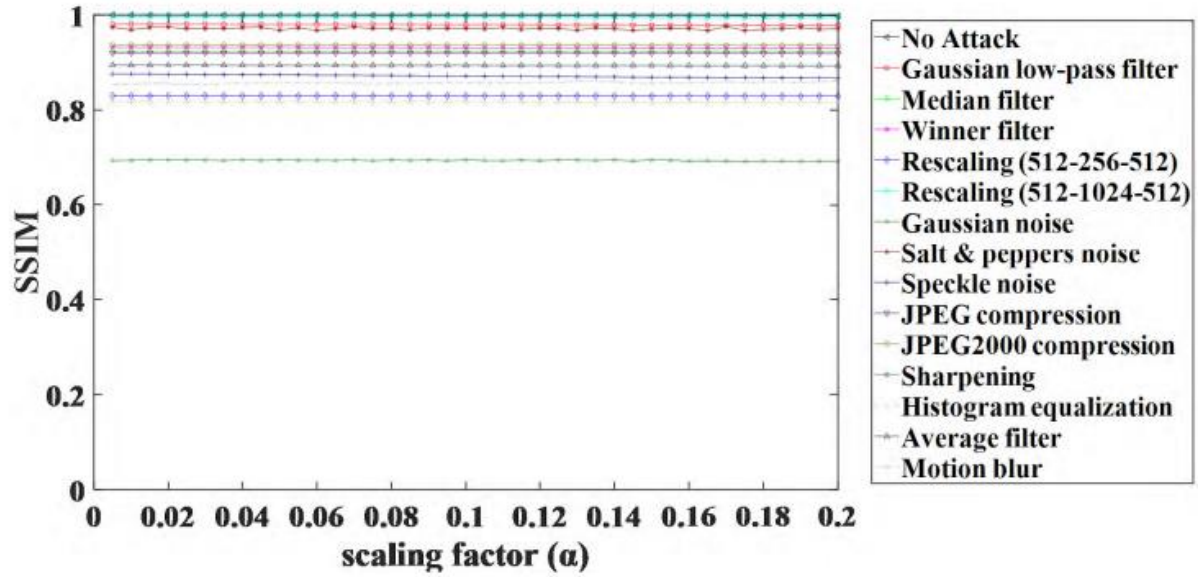



Figure 7: Performance of SSIM under various attacks for various values scaling factor

Figure 5, Figure 6 and Figure 7 presents the performance of NCC, PSNR and SSIM metrics under various attacks for various values scaling factors. Thus, from these figures, it is observed that the performance of proposed method is stable for various attacks, it is not decreasing drastically in most of the scenarios. Especially, the NCC, SSIM values remains constants for various levels, which indicates the proposed method resulted in optimal performance. Further, the PSNR values also constant for maximum attacks, thus the robustness is improved.

**Publisher:** Sunyani Technical University **[European Article Number:** 17908875546877**]**
**ISSN:** 2773-8418 (Print), **ISSN** 2773-8426 (Online) **[**© 2021 Science Publications**]**

**Table 1: Performance comparison with existing methods**

| Metric | DWT [11] | DCT-SVD [12] | DWT-SVD [14] | Proposed |
|---|---|---|---|---|
| **PSNR** | 45.75 | 48.68 | 56.677 | 65.456 |
| **SSIM** | 0.8138 | 0.846 | 0.894 | 0.983 |
| **NCC** | 0.7365 | 0.7936 | 0.836 | 0.9738 |

From the table 1, it is observed that the proposed method resulted in optimal performance as compared to the conventional approaches such as DWT [11], DCT-SVD [12], and DWT-SVD [14], respectively.

## 4. CONCLUSION

This article introduced a new RDWT-SVD-based watermarking approach for embedding a watermark image that may be as large as the cover picture. In the RDWT domain, changing singular values of the cover picture gives great robustness with common attacks. As a result of the RDWT implementation, the algorithm has a high PSNR and correlation coefficient of the watermarked picture. In comparison to DWT-based techniques, the suggested solution proved to be more resistant to different attacks. Further, this method can be extended with implementation of advanced transformations for more robustness.

## REFERENCES

[1]. Thanki, Rohit, et al. "An efficient MIW scheme based on FDCuT–DCT." Engineering science and technology, an international journal 20.4 (2017): 1366-1379.
[2]. Aparna, Puvvadi, and Polurie Venkata Vijay Kishore. "Biometric-based efficient MIW in E-healthcare application." IET Image Processing 13.3 (2019): 421-428.
[3]. Alshanbari, Hanan S. "MIW for ownership & tamper detection." Multimedia Tools & Applications 80.11 (2021).
[4]. Fan, Tzuo-Yau, Her-Chang Chao, and Bin-Chang Chieu. "Lossless MIW method based on significant difference of cellular automata transform coefficient." Signal Processing: Image Communication 70 (2019): 174-183.
[5]. Singh, Siddharth, et al. "SVD-DCT based MIW in NSCT domain." Quantum computing: an environment for intelligent large scale real application. Springer, Cham, 2018. 467-488.
[6]. Hassan, Bilal, et al. "An imperceptible MIW framework for automated diagnosis of retinal pathologies in an eHealth arrangement." IEEE Access 7 (2019): 69758-69775.
[7]. Khare, Priyank, and Vinay Kumar Srivastava. "A secured and robust MIW approach for protecting integrity of medical images." Transactions on Emerging Telecommunications Technologies 32.2 (2021): e3918.
[8]. Soualmi, Abdallah, Adel Alti, and Lamri Laouamer. "A New Blind MIW Based on Weber Descriptors and Arnold Chaotic Map." Arabian Journal for Science & Engineering (Springer Science & Business Media BV) 43.12 (2018).
[9]. Kumar, Sumit, and Rajib Kumar Jha. "FD-based detector for MIW." IET Image Processing 13.10 (2019): 1773-1782.
[10]. Kahlessenane, Fares, et al. "A robust blind MIW approach for telemedicine applications." Cluster Computing (2021): 1-14.
[11]. Bharati, Subrato, et al. "Analysis of DWT, DCT, BFO & PBFO algorithm for the purpose of MIW." 2018 International Conference on Innovation in Engineering and Technology (ICIET). IEEE, 2018.
[12]. Aparna, Puvvadi, and Polurie Venkata Vijay Kishore. "An efficient MIW technique in E-healthcare application using hybridization of compression and cryptography algorithm." Journal of Intelligent Systems 27.1 (2018): 115-133.

**Publisher:** Sunyani Technical University **[European Article Number:** 17908875546877**]**
**ISSN:** 2773-8418 (Print), **ISSN** 2773-8426 (Online) **[**© 2021 Science Publications**]**

[13]. Kahlessenane, Fares, et al. "A robust blind medical image watermarking approach for telemedicine applications." Cluster Computing (2021): 1-14.
[14]. Thakur, S., et al. "Improved DWT-SVD-based medical image watermarking through hamming code and chaotic encryption." Advances in VLSI, communication, and signal processing. Springer, Singapore, 2020. 897-905.
[15]. Balasamy, K., and D. Shamia. "Feature Extraction-based Medical Image Watermarking Using Fuzzy-based Median Filter." IETE Journal of Research (2021): 1-9.