International Journal of Informatics and Applied Mathematics
e-ISSN:2667-6990 Vol. 3, No. 2, 1-11

# A Transform Based Effective Robust Watermarking Method for Medical Data Security

Abdallah SOUALMI[1], Adel ALTI[1,2], and Lamri LAOUAMER[2]

[1] Department of Computer Science, LRSD Laboratory, Setif-1 University, P.O. Box 19000 Setif - Algeria
[2] Department of Management Information Systems, College of Business & Economics Qassim University, P.O. Box 6633, Buraidah, 51452, KSA
{sabdallah, alti.adel}@univ-setif.dz
laoamr@qu.edu.sa

**Abstract.** The evolution of new information technologies has led to the emergence of a wide range of e-health applications. These applications continuously evolve and transfer a significant amount of sensitive data over the Internet. Such applications carry some security risks such as alteration and unauthorized access. A robust and secure watermarking technique is needed to protect medical data from unauthorized access. This paper aims to propose a new robust watermarking approach for protecting sensitive medical data, using DFT transform and QR decomposition. The main idea consists of embedding the watermark DFT coefficients into cover image DFT coefficients of the QR coefficients using a scalling factor to strengthen the robustness and imperceptibility. Simulations results prove that the proposed technique could find a better trade-off between robustness and imperceptibility.

**Keywords:** Digital watermarking · Robust · Discrete Fourier Transform (DFT) · QR decomposition · Sensitive data protection.

## 1 Introduction

The advanced communications and multimedia technologies lead to the emergence of a wide range of e-health applications. These applications transfer a significant amount of data over unsecured networks, where the data could face alteration or unauthorized access. Consequently, data authorship could be lost or stolen. To this end, new efficient techniques that consider the special features must be proposed.

The cryptography is a very promising mechanism that makes data unreadable by an unauthorized party. However, these benefits, cryptography technique when data is decrypted, it brings new security risks such as unauthorized access and copyright violation [1, 2] .

Recently, the use of watermarking technique is raised as a compliment of cryptography for felling their drawbacks. It ensures copyright protection, proofing the authorship and integrity checking under vulnerable access [3]. It consists of embedding watermark data in a cover document (text, audio, image ,and video) [4]. The watermark is constructed in the spatial domain and embedded directly in the image pixel by modifying their intensity [5], or in the frequency domain [6] where it is embedded usually in the original image transform.

Watermarking techniques are classified according to the robustness into three categories: robust, semi-fragile, and fragile [7]. In robust watermarking approaches, the watermark resists after any attacks applied on the watermarked image, while, in semi-fragile, the watermark resists after minors attacks performed on the watermarked image. In fragile watermarking, the watermark is easily collapsed against any intentional or unintentional operation. Based on the watermark extracting techniques. Image watermarking techniques can be classified into three types: blind, semi-blind and non-blind [8, 9] . For the first kind, the extraction process doesn't require any of the original or watermark image. In the second type, the extraction process necessitates the presence of the original watermark, while for the last one, the , the original image is required for the watermark extraction. Therefore, the robust image watermarking should be resistant to all kinds of attacks. To realize this, several image watermarking techniques have been studied [10–16]. However, the frequency domain technique is robust with significant degradation of the image quality against various attacks.In this paper, our aim is to develop a new medical image watermarking technique that provides higher robustness while preserving medical image quality.

The rest of this paper is organized as follows: section 2 describes recent related works. Section 3 details the proposed approach in detail. Section 4 presents and analyzes the experimental results of the proposed method. Finally, section 5 concludes the work.

## 2 Related Work

Frequency domain-based watermarking show more robustness than spatial domain watermarking. In this section, we study the recent transform watermarking techniques existing in the literature [10–16].

In [10], Hanet et al.propose a hybrid technique based on Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Hermite chaotic neural network. The main idea is to apply the DWT and DFT on the cover medical image, after that select the low and median frequency band as data features; where these last are used to generate the watermark. The watermark is scrambled using Hermite chaotic neural network and encrusted in the DCT coefficients of the original image. This approach offers good trade-off between robustness and imperceptibility. However, it tested only against few attacks and it requires an important computational complexity.

In [11], the authors presented a non-blind watermarking algorithm based on Lifting Wavelet Transform (LWT) and Singular Value Decomposition (SVD). LWT and SVD are applied on the cover image. After that, the watermark is decomposed into four blocks and the SVD is applied on each of them. Finally, the singular values of the watermark are added to the singular value of the cover image. This approach gives good trade-off between imperceptibility and robustness against many attacks, except some geometric attacks such as histogram equalization, cropping.

In [14], the authors present a semi-blind method based on DWT, Countourlet transforms (CT), Schur Decomposition, SVD and Arnold transform, where the scrambled watermark singular value are embedded in the singular value of the host image after DWT, CT and Shur decomposition respectively. This method gives good results in terms of imperceptibility and robustness. However, this technique presents some vulnerability with some attacks such: salt and pepper noise (0.2) (PSNR in [11, 16] dB), Gaussian noise(0.1) (PSNR in [10, 12] dB). Also, it requires high computational complexity for embedding/ extracting processes.

In [15], Singh et al. proposed a hybrid method based on DWT and SVD. The idea is to generate a signature from the watermark using SVD after that embed it into the LL and HH coefficients in a strategic location that slected using a secret key. This proposed approach gives good results in terms of imperceptibility and robustness. However, it requires an important execution time for embedding/extracting processes.

The authors in [16] presented a blind medical images watermarking method based on DCT and fractional differentiator (FD), where the watermark image is embedded into the RONI DCT middle band frequency coefficients using FD, by generating direct spread spectrum sequence. This method gives good trade-off between imperceptibility, computational complexity and security. However, we couldnt measure the robustness degree because the method was tested only with few attacks.

The challenging problem of image watermarking is still on-going to develop a method that can provide full robustness. In this context, the proposed method improves the robustness comparing to some existing methods.

# 3 Proposed Technique

The main purpose of the proposed robust effective watermarking method is to protect medical data transmitted over unsecured communication channels. The watermark embedding process is performed by the sender before the transmission of the watermarked image. During the transmission of the watermarked image, the image is open potentially altered. The receiver extracts the embedded medical data using the same operations in the embedding process. The Watermark embedding/extracting processes are detailed as follow:

## 3.1 Watermark embedding process

The watermark embedding process is based on QR decomposition and DFT [10], as illustrated in Fig. 1 and detailed as follows:

*Step 1.* Decompose up the cover image into non-overlapping blocks of size 2x2.

*Step 2.* Performing QR decomposition [4]. on each block (Bi):

$$QR(Bi) = [U, V] \tag{1}$$

*Step 3.* Apply DFT on the V matrix obtained in step 2 and on the watermark image scrambled with Arnold chaotic map using a key (k).

*Step 4.* Select a block coefficient (BCi) and two watermark DFT coefficients (WCj and WCj+1), and embed them in the middle band coefficients of BCi , using scaling factor as follow-

$$\begin{cases} BC_i(1,2) = BCi + (1-\alpha) * WC_j \\ BC_i(2,1) = BC_i + (1-\alpha) * WC_{j+1} \end{cases} \tag{2}$$

Where $\alpha$ in ]0,1[.

Embedding two watermarks DFT coefficients in the middle band DFT coefficients of the V matrix doesn't affect the cover image intensity due to the good features of DFT and QR decomposition [4, 10].

*Step 5.* Apply $\mathrm{DFT}^{-1}$ on Ci to obtain the watermarked V matrix (Vw), then perform $\mathrm{QR}^{-1}$ to obtain the watermarked block using the following equation:

$$QR^{-1} = U * Vw * U^T \tag{3}$$

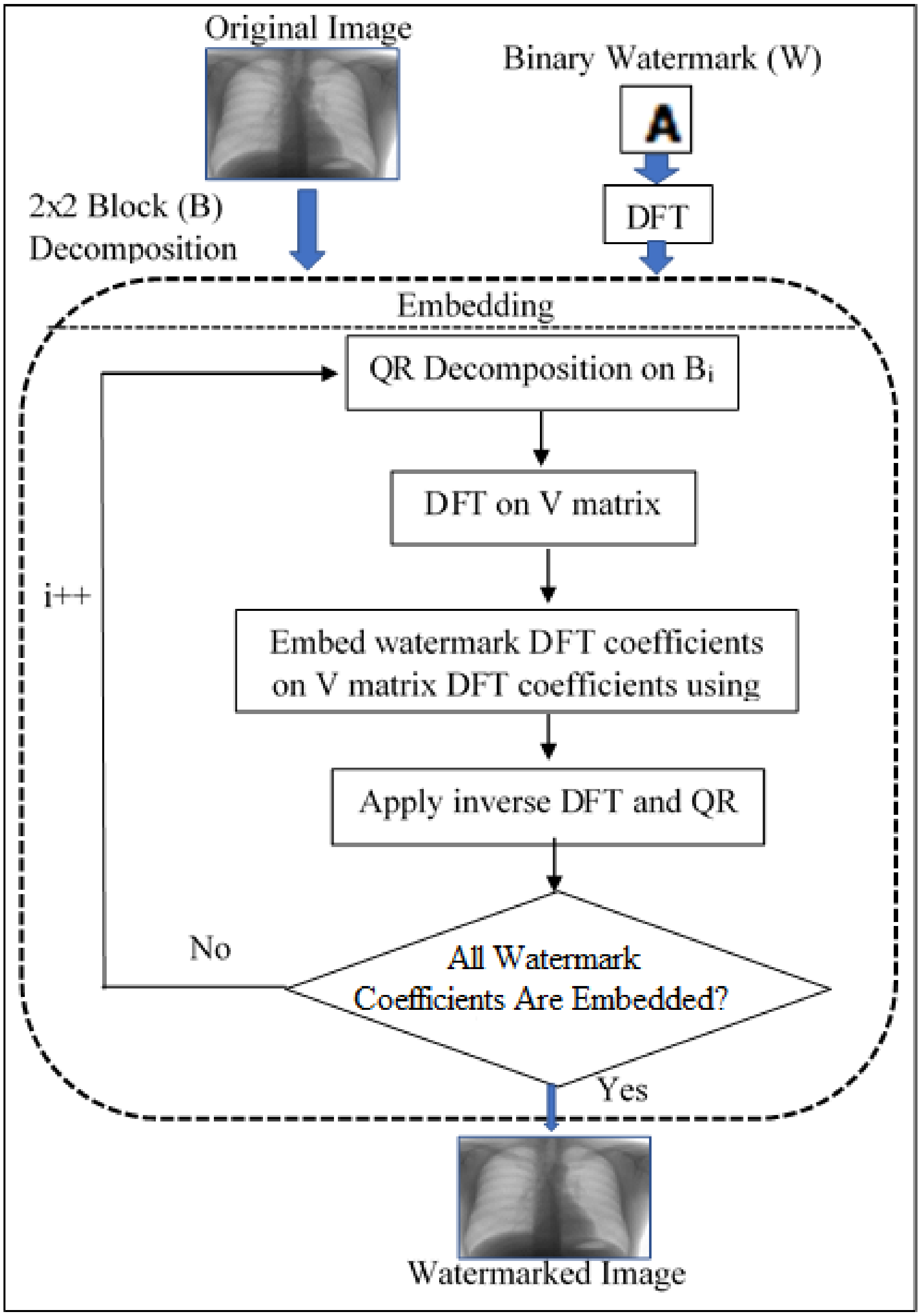


**Fig. 1.** Watermark embedding process.

*Step 6.* If not all the watermark DFT coefficients are embedded go back to step 4 with i+1 and j+2. Else end.

### 3.2 Watermark extracting process

The extraction process is semi-blind where it requires the original embedded data. The detailed extraction process is illustrated with a block diagram in Fig. 2 and discussed as follow:

*Step 7.* Decompose up the host image into 2x2 non-overlapping blocks.

*Step 8.* Performing QR decomposition on each block (Bi) using equation (1).

*Step 9.* Apply DFT on the V matrix obtained below.

*Step 10.* Select a blocks coefficients (BCi) and two watermark intensities ( WIj and WIj+1 ) and then extract the watermark DFT coefficients as follow:

$$\begin{cases} WC_j = \frac{WI_j(1,2)}{\alpha} - \frac{1-\alpha}{\alpha} * BC_i(1,2) \\ \\ WC_j + 1 = \frac{WI_{j+1}(2,1)}{\alpha} - \frac{1-\alpha}{\alpha} * BC_i(2,1) \end{cases} \tag{4}$$

*Step 11.* If not all the watermark blocks are extracted go back to step 10 with i+1 and j+2. Else Apply $\mathrm{DFT}^{-1}$ on the extracted watermark coefficients to get the extracted scrambled watermark block then apply the Arnold chaotic map inverse using the same key used in embedding to get the watermark image.

## 4 Experimental Results and Discussion

In order to evaluate the performances of the proposed technique in terms of imperceptibility and robustness, a data set of DICOM images of size 256x256 is used (from [17, 18].), while the watermark image of size 128x128. Fig. 3 and Fig. 4 show, respectively, the watermark image and gives a sample of medical images used in experimentations. In the following, we use a scaling factor of value 0.98.

### 4.1 Performances metrics

*a) Peak Signal To Noise Ration (PSNR):* This metric is used to evaluate the imperceptibility performance. A higher PSNR value indicates higher imperceptibility [19]. The PSNR is calculated as follow:

$$PSNR(_dB) = 10log_{10}(\frac{255^2}{MSE}) \tag{5}$$

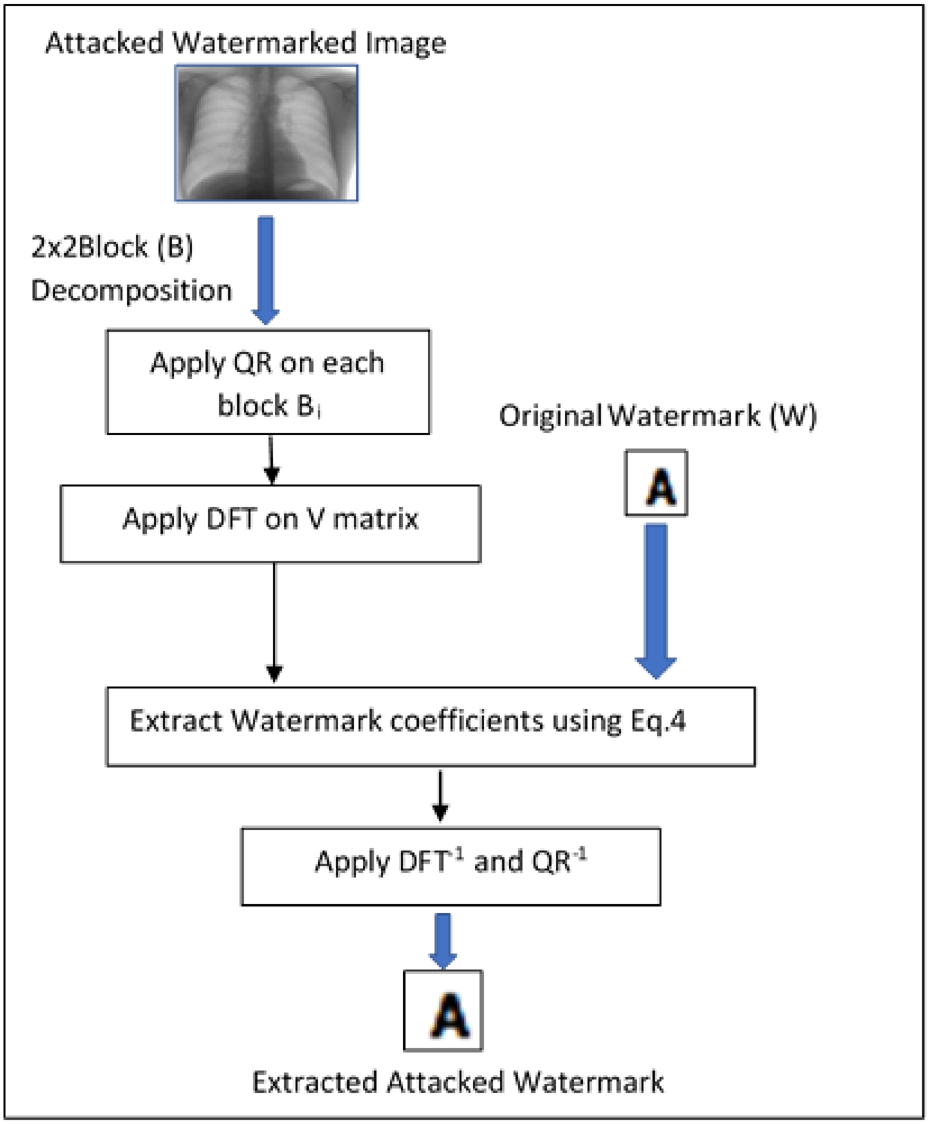


**Fig. 2.** Watermark extracting process.

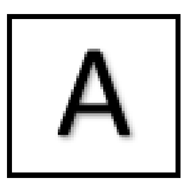


**Fig. 3.** Watermark image used in experimentation.

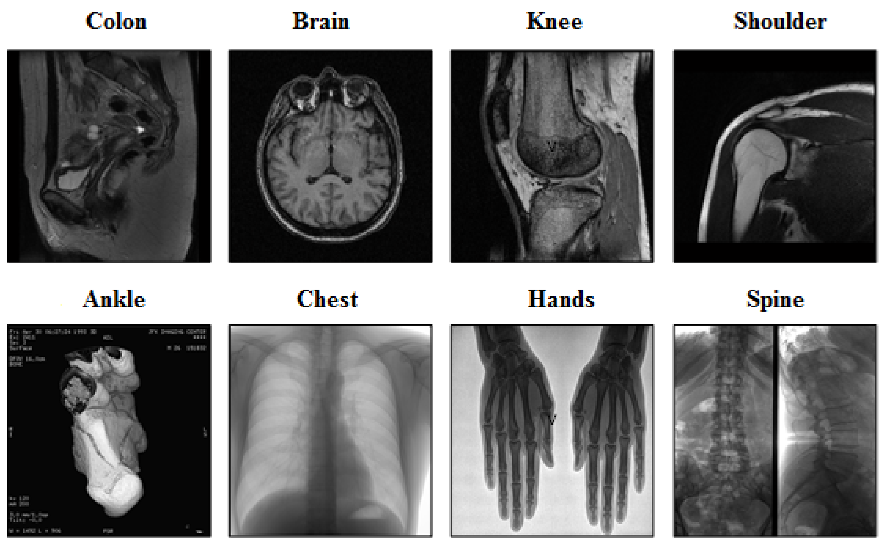


**Fig. 4.** Sample of images used in experimentation.

with

$$MSE = \frac{1}{NxM} \sum_{k=0}^{k=N-1} \sum_{l=0}^{l=M-1} (I1(k,l) - I2(k,l)) \tag{6}$$

Where I1 and I2 are the original image and the watermarked one respectively, N and M are the images' sizes.

*b) Normalized Correlation(NC):* This metric is used to compare the original watermark with the extracted one [11], A higher NC value means the good robustness of the watermarking method.

$$NC = \sum_{u=0}^{u=W_N-1} \sum_{v=0}^{v=W_M-1} (W_1(u,v) - W_2(u,v)) \tag{7}$$

Where $W_N$ x $W_M$ are the watermark size and $W_1, W_2$ are the original watermark and the extracted one respectively.

### 4.2 Imperceptibility Evaluation

The imperceptibility is the similarity degree between the original image and the watermarked one. Imperceptibility is an important factor in the context of medical images. A mediocre imperceptibility degree means the impracticability of the watermarking method. To this end, we use PSNR to evaluate the imperceptibility. Table 1 gives the imperceptibility degrees in terms of PSNR(dB) using medical images.

**Table 1.** PSNR average values (dB) using the proposed watermarking method.

| Images | Colon | Knee | Hands | Spine |
|---|---|---|---|---|
| **PSNR(dB)** | 43.18 | 43.39 | 44.61 | 44.62 |

Table 2 gives the imperceptibility comparison results among various techniques described in in [12–14, 16]. and the proposed approach in terms of PSNR (dB).

**Table 2.** Imperceptibility comparison among the proposed and method in [12–14, 16].

| Methods | [12] | [13] | [14] | [16] | Proposed method |
|---|---|---|---|---|---|
| **PSNR(dB)** | 40.48 | 39 | 36.49 | 44 | **44.62** |

As shown in Table 1 and Table 2, the proposed method achieves better imperceptibility. The reason is that the embedding of a watermark DFT coefficient necessitates a small change in the QR-DFT coefficients of the cover image blocks. To this end, the watermarked images keep the good imperceptibility comparing to the original one.

### 4.3 Robustness Evaluation

The robustness is the resistance degree of the embedded watermark after any attacks applied to remove it or confuse the image authentication.

**Table 3.** NC values Of the extracted watermark from attacked watermarked images.

| Attacks | Colon | Knee | Hands | Spine |
|---|---|---|---|---|
| **Salt and pepper noise v=0.05** | 0.918 | 0.91 | 0.91 | 0.91 |
| **White noise v=0.05** | 0.891 | 0.88 | 0.89 | 0.89 |
| **DICOM JPEG compression attacks QF=50** | 0.99 | 0.99 | 0.99 | 0.99 |
| **Rotation 45** | 0.99 | 0.99 | 0.99 | 0.99 |
| **Cropping 10** | 0.99 | 0.99 | 0.99 | 0.99 |
| **Shearing** | 0.99 | 0.99 | 0.99 | 0.99 |

In order to evalaute the robustness of the proposed method, we use a metric called Normalized Correlation (NC) [8, 7, 20, 5].

We apply some attacks to the watermarked image, and then evaluate the extracted watermark image using NC measure between the original watermark and the extracted one. Table 3 gives the NC values of the extracted watermarks from the attacked watermarked images. Table 4 shows the robustness comparison results between the proposed method and the approaches described in [15,

**Table 4.** Robustness comparisons under NC values.

| Attacks | [14] | [15] | Proposed method |
|---|---|---|---|
| **Salt and pepper noise v=0.01** | 0.97 | 0.794 | **1** |
| **Salt and pepper noise v=0.05** | 0.911 | Not found | **0.98** |
| **White noise v=0.01** | 0.939 | 0.794 | **0.99** |
| **Rotation 5** | - | 0.81 | **1** |
| **Rotation 45** | 0.91 | 0.519 | **0.99** |

14]. The results show that our approach is more robust against different kinds of attacks than the existing approaches.

From Table 3 and Table 4 its obvious that the proposed technique offers good robustness; the reason is that the NC values are very close to 1. This means that the proposed method allows full robustness for the watermark image.

## 5 Conclusion

This paper presents a new robust medical image watermarking method, which benefits from the good features of QR decomposition and DFT. The main idea is to embed the watermark data into the DFT-QR coefficients of the host image blocks. Experimental results prove that the proposed technique offers better performance in terms of robustness, imperceptibility and data payload. A comparison with some related methods reveals that the proposed approach is better when we talk about imperceptible and robustness. However, the computational complexity required for embedding and extracting must be improved in future works. In future works, we will focus mainly on the robust blind watermarking methods to be adopted to real-time e-Health applications.

## References

1. Su, Q., Niu, Y., Wang, Q., Sheng, G.: A blind color image watermarking based on DC component in the spatial domain. Optik- International Journal for Light and Electron Optics, **124** (23), 6255-6260 (2013)
2. Ortiz, A. M., Uribe, C. F., Beltran, R .H, Hernandez, J. J. G.: A survey on reversible watermarking for multimedia content: A robustness overview. IEEE Access, pp. 121 (2019)
3. Rahmani, H., Mortezaei, R., Moghaddam, M.E.: A New Robust Watermarking Scheme to Increase Image Security. EURASIP Journal on Advances in Signal Processing **2010** (1), 428183 (2010)
4. Su,Q., Wang, G., Zhang, X. F., Lv, G., Chen, B.: An improved color image watermarking algorithm based on QR decomposition. Multimedia Tools and Applications **76** , 707729 (2017)
5. Panchal, U. H., Srivastava, R.: A Comprehensive Survey on Digital Image Watermarking Techniques. In proceeding of the Fifth International Conference on Communication Systems and Network Technologies (CSNT), pp. 591-595. IEEE, (2015)

6. Das, C., Panigrahi,.S, Sharma, V., Mahapatra, K.: A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. AEU - International Journal of Electronics and Communications **68** (3), 244-253 (2014)
7. Ernawan, F., Kabir, M. N.: An Improved Watermarking Technique for Copyright Protection based on Tchebichef Moments. IEEE Access, 1-20 (2019)
8. Agarwal, H., Raman, B., Venkat, I.: Blind reliable invisible watermarking method in wavelet domain for face image watermark. Multimedia Tools and Applications,**74** (17), 6897-6935 (2014)
9. Lagzian, S., Soryani, M., Fathi, M.: A New Robust Watermarking Scheme Based on RDWT-SVD. International Journal of Intelligent Information Processing, **2** (1), 22-29 (2011)
10. Han, B., Li, J., Zong, L.: A New Robust Zero-watermarking Algorithm for Medical Volume Data. International Journal of Signal Processing, Image Processing and Pattern Recognition **6** (6), 245-258 (2013)
11. Kabra, R. G., Agrawal, S. S.: Robust Embedding of Image Watermark using LWT and SVD. In: proceeding of the International Conference on Communication and Signal Processing, pp. 1968-1972. IEEE, India (2016)
12. Singh, A., Dave, M., Mohan, A.: Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimedia Tools and Applications, **75** (14), 8381-8401 (2015)
13. Liu, X.L., Lin, C. C., Yuan, S.M.: Blind dual watermarking for color images authentication and copyright protection . IEEE Transactions on Circuits and Systems for Video Technology, 1-9 (2016)
14. S,P., C. R, P. V. S. S.: A robust semi-blind watermarking for color images based on multiple decompositions. Multimedia Tools and Applications, pp. 1-17 (2017)
15. Singh, N., Joshi, S., Birla, S.: Color Image Watermarking with Watermark Authentication against False Positive Detection using SVD .In: Proceeding of the International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur, India (2019)
16. Kumar, S., Jha, R. K.: FD-based detector for medical image watermarking. IET Image Proces, **13** (10), 1773-1782 (2019)
17. sample images http://deanvaughan.org/wordpress/2013/07/dicom-sample-images/ . Last accessed 03 Dec 2018
18. sample images http://dicom.nema.org. Last accessed 15 Dec 2018
19. Agarwal, N., Singh, A. K., Singh, P. K.: Survey of robust and imperceptible watermarking. Multimedia Tools and Applications, 131 (2019)
20. AL-Nabhani, Y., Jalab, H., Wahid, A., Noor, R.: Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network. Journal of King Saud University - Computer and Information Sciences, **27** (4), 393-401 (2015)