International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 3, No.3 (Sep-2014)

Reversible Combined R-DWT-DCT-SVD Watermarking Schema

Bekkouche Souad and Faraoun Kamel Mohamed

Computer sciences department

DjillaliLiabes University, SidiBel Abbes 22000, Algeria

Received 25Apr.2014, Revised 31May. 2014, Accepted 15Jun. 2014, Published 1Sep. 2014

Abstract: This paper presents a secure and robust image watermarking scheme based on the reversible DWT-DCT-SVD transformations to increase both integrity authentication and confidentiality. The proposed approach uses two types of watermarks image: a reversible watermark W_1 used for verification (integrity and authentication aspects), and a second watermark W_2 (a logo image) to verify the confidentiality. Performances of proposed method are evaluated with respect to the PSNR (Peak Signal to Noise Ratio), SNR (Signal noise to ratio), and NCC (Normalized Correlation) and to the running time. A comparative study is also provided to show robustness of the technique against different attacks including compression attack and Salt & Pepper.

Keywords: Watermarking, R-DWT-DCT-SVD, Images security.

1. Introduction

Today, network technologies have improved so that people gain more access to remote facilities and send or receive different types of digital data via the net. However, the Internet is a good public, but non-secure data transmission channel. Thus, important information must be manipulated to be concealed while provided via the Internet so that only the authorized receiver can get it. For this reason, several methods are developed to hide a secret message in the data content to verify security properties (authentication, confidentiality and integrity). Digital watermarking, which is the act of hiding a signal (watermark) into an image, is one of such proposed techniques, used to protect the rights of owners. Watermarking techniques are classified into two classes according to domain of embedding: spatial techniques that are implemented in spatial domain by directly modifying pixel values, and frequency techniques applied in frequency domain when the watermark is embedded by modifying transform domain coefficients carried out after decomposition such as Discrete Cosine Transform (DCT) [1, 2], Discrete Wavelet Transform(DWT) [2, 3], Discrete Fourier Transform (DFT)[4] or Singular Value Decomposition (SVD)[5,6].

The main properties that a watermarking technique must provide to be effective are imperceptibility and robustness. The former imply that the embedded mark should be perceptually invisible to assure a best image quality after the embedding step. The later property is satisfied if the inserted mark is difficult to remove and can be recovered even if the image is modified or altered by the attacks (image modification and manipulation). More precisely, Cox et al [7] define robustness as the ability to detect watermark after modifying operations (treatments), for example, more quality information in the image increases, the signature will be visible or perceptible and therefore the robustness decreases. Furthermore, A watermarking system can be reversible or irreversible: the reversible watermarking can extract or restore the original data from the watermarked one by applying an inverse transformation without producing any changes and avoids all irreversible distortion into an original image using techniques capable to extracting the watermark, while the irreversible watermarking, there is no way to extract the original image from the watermarked image [8].The aim of this paper is to propose a reversible watermarking algorithm R-DWT-DCT-SVD based on the insertion two marks: W_1 and W_2 in three different domains DWT, DCT and SVD. The remaining of the paper is organized as follows: Section 1 presents an introduction to watermarking systems, section 2 discus related works, and

Email:sbekkouche2008@gmail.com; kamel_mh@yahoo.fr

section 3 present the proposed technique. In section 4 the experimental results are presented, when performances of the proposed method are evaluated and compared to those of existing methods using the PSNR, the NCC coefficient of correlation between original watermark and extracted watermark, SNR and Elapsed time. We test the robustness of watermarking according to Salt & pepper noise, Gaussian noise and JPEG compression attack. Finally conclusions are drawn in section 5.

2. RELATED WORK

The transform domain after a DCT is similar to the discrete Fourier transform (DFT) that allows an image to be divided into different frequency bands: high, middle and low frequency band. The technique based on DCT has a great advantage: robust compression operations with a reduced computation time. Cox and al. [19] apply the DCT on the host image among the low frequency; they modify the n coefficients of the highest amplitude of the transform, and the original image is required to extract the watermark. In [9],Piva and al. describes the same principle of embedding process but the extraction the watermark is performed by a correlation approach without the need for original image.

The DWT transform is a modern mathematical tools and has been widely studied in signal processing in general and image compression in particular, based on the separation the original image into four non-overlapping multi-resolution sub bands: lower resolution approximation image (LL), a horizontal high frequency band (HL), vertical high frequency band (LH) and diagonal high frequency band (HH). In general, most of the image energy is situated at the lower frequency sub-bands LL and therefore hiding watermarks in lower frequency sub-bands (LL) may degrade the quality of the host image even if it could increase the robustness significantly. Tao and Eskicioglu [10] proposed a watermarking technique based on the insertion of the watermark as a binary logo in the four sub bands. The quality of the extract watermark is determined by the similarity rate.

The SVD transformation is another mathematical tool used in digital image processing. Recently, this transform is used for watermarking because of its algebraic proprieties. It is generally used to compute two orthogonal matrices U, V and a diagonal matrix S [11]. In [12], Chandra computed SVD of both the original and watermark images and then singular values of the watermark images are added to those of the host image, the watermark W is added to the matrix S. Then, a new SVD process is performed on the new matrix: D=S+k*W, to getU_w, $S_w$andV_w , where k is a scale factor that controls the strength of the watermark embedded into the original image. The watermarked image $I_w$is then obtained by multiplying the matrices U,S_W, and V.

3. DESCRIPTION OF THE PROPOSED SCHEMA(R-DWT-DCT-SVD)

Watermarking schemes that uses the frequency domain as a workspace are advantageous for compression operations since the same domain is used to encode the image, and hence provides faster processing time. In the proposed method, the DWT transformation is used firstly to decompose the image into the four sub bands namely LL, LH, HL and HH described above. The watermark images are then embedded on the HL detail of the host image and the DCT is applied on LL and HH to give D and D_3 that will undergo each one the SVD transform to give three matrices respectively : Diagonal S and S_3 and the two orthogonal ones U,V for D and U_3,V_3 for D_3.

The first step of embedding is generating both the watermark W_1 and W_2. A transformed DWT is applied to the two watermarks which gives respectively four levels (LL_1, HL_1, LH_1, and HH1) and (LL_2, HL_2, LH_2, HH_2). We then perform the DCT on LH_1 and LH_2 to give D_2 and D_1, and the SVD transform applied to D_2 and D_1 to give (U_2, S_2, V_2) and (U_1, S_1, V_1) respectively. The embedding of the watermark W_1 is performed by the addition of the two diagonals matrices S and S_2 multiplied by a factor α to obtain S_{55} and the embedding the watermark W_2 is performed by the addition of two diagonals matrices S_2 and S_3 multiplied by the same factor α to obtain S_{32}, the SVD is performed on S_{32} to obtain W_{img}, to reconstruct the watermarked image $I_w$the inverse IDCT is applied to W_{img}.

In the following, we present the process of embedding and extraction of proposed watermarking approach that uses the DCT, DWT and the SVD transformations in a same schema.

3.1. Watermark embedding process

In order to ensure the main aspects of security that are authenticity, Integrity and confidentiality, we propose a new hybrid watermarking approach R-DCT-DWT-SVD that performs the embedding of two different kinds of watermarks:

- A reversible watermark W_1 used to verify data authentication and integrity of the image, defined by the RSA enciphering of a data block composed by: the SHA-512 hash of the most significant bits (MSB) and the RLE compression of the least significant bits (LSB) compressed.
- A second watermark W_2 that is created by the generating of pseudorandom binary sequence using a secret key that allows you to check the confidentiality and also the integrity of images. The watermarking process has as input the cover image I and the two generated watermarks W1 and W2, and gives as output the watermarked image I_w. Details of different steps are presented in follow, and a complete diagram of the approach is illustrated by figures 3 and 4.

- **Generation of the matrix S_1 representing the Watermark W_1:**

1. Extract of the MSB of the cover image and calculate the corresponding Message authentication code(MAC) using the SHA-512 algorithm;
2. Concatenate the obtained MAC with the patient information and encrypt the resulting string; (as shown in the figure 1) .
3. Select the LSBs of all pixels and compress the resulting string using RLE;
4. Concatenate the compressed string and the encrypted one.
5. Converts the characters of string to their decimal ASCII codes d ;
6. Converts a nonnegative decimal integer vector d to a binary matrix A;
7. Apply the DWT on the resulting matrix A to obtain: LL_1, HL_1,LH_1 and HH_1;
8. Apply the DCT transform on LH_1 obtain a new matrix D_1;
9. Perform the SVD on the D1 to obtain the SVs decomposition : $U_1.S_1.V_1'$;

Only the obtained matrix S_1 represent the watermark W_1 to be inserted as watermarking information in the host image I. The watermark W_1 is computed from the host image and will serve for integrity and authentication (As shown in the figure 1).

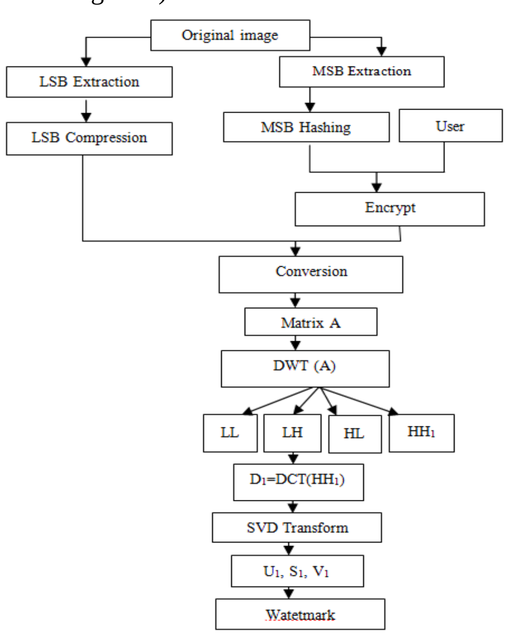


Fig.1. Generation the Watermark W1.

- **Generating the matrix S_2 representing the watermark W_2**

1. Read in the watermark message and reshape it into a vector;
2. For a pseudorandom sequence is then generated from the watermark message used as a seed.
3. Apply DWT on the generated random sequence reshaped as a matrix to obtain: LL_2, HL_2, LH_2 and HH_2;
4. Apply the DCT to sub bands LH_2 to give the new matrix D_2;
5. Decompose D_2 in singular values to obtain the SVs:

$$SVD\ (D_2)=U_2.S_2.V_2^t;$$

Only the obtained matrix S_2 represent the watermark W_2 to be inserted as watermarking information in the host image I. The watermark W_2 is computed from the host image and will serve for confidentiality (As shown in the figure 2).

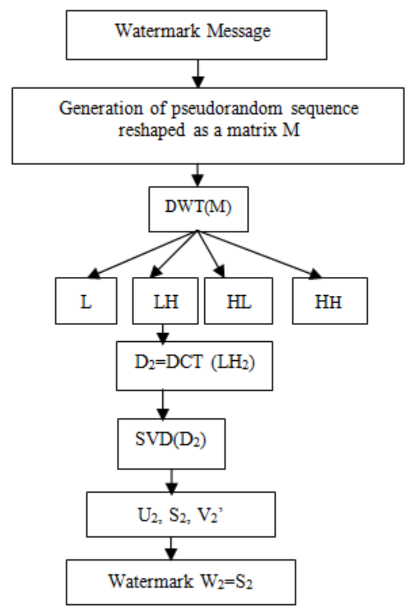


Fig.2. Generation the Watermark W_2

- ***Embedding process of watermark W_1:***

1. Apply the DWT transform to decompose the cover image into four sub-bands;
2. Perform the SVD on the sub-band LL to obtain the SVs : SVD(LL)=U.S.V';
3. Insert the singular values of the watermark S_1 in the matrix S of LL to obtain : $S_{33}=S + \alpha * S_1$;
4. Perform the SVD on S_{33} to obtain the SVs: $SVD(S_{33})=U_6.S_6.V_6'$;
5. Finally, Calculate the watermarked matrix using U, V and S_6: $W_{img2} = U \times S_6 \times V'$.

- ***Embedding process of watermark W_2***

1. Take the sub-band HH of the cover image ;
2. Apply the DCT to sub-band HH to get the new matrix D_3;
3. Perform the SVD on D_3 : $SVD\ (D_3)=U_3.S_3.V_3^t$;

4. Add the S_2 of the watermark W_2 to the matrix diagonal S_3: $S_{32} = S_3 + {}_{\alpha} x\ s_2$;
5. Perform the SVD on S_{32} to obtain U_5, V5', S5and reconstruct the W_{img} matrix using S_5, U3 and V_3: $W_{img} = U_3 . S_5 . V_3^{\,t}$;
6. Apply the inverse DCT to Reconstruct B_1 using W_{img} ;
7. Obtain the watermarked image I_W by performing the inverse DWT using $B_2$and three sets of DWT coefficients: HL_2, B_1 and HH_2.The detailed process of watermark embedding is illustrated in the figure 3.

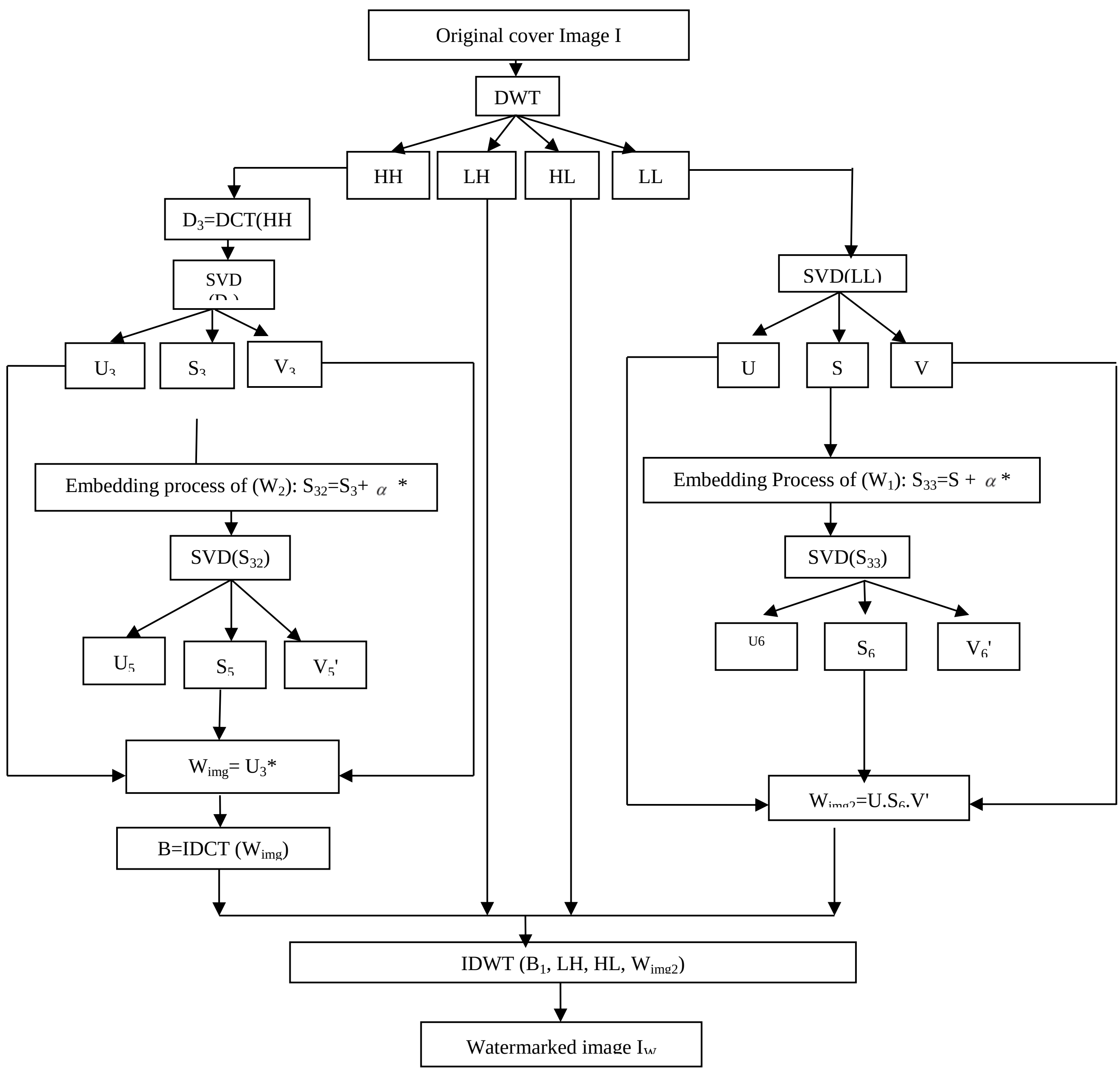


Fig.3. Watermark embedding process.

3.2. Watermark extraction process Fig

The extraction phase based on the extraction of watermark W1 and watermark extraction W2,the first step is applying the decomposition DWT to decompose the watermarked image I_W which gives us four details: LL_w*, HL_w*, LH_w*and HH_w*(possibly corrupted), the detail LL_w* is used for the extraction watermark w_1 and the HH_w*is used for extraction the watermark w_2.The transformed SVD is applied to LL_w*which gives the three matrices U_w*,S_w*,V_w*, after we find the matrix $S_r$using the diagonal matrix S (obtained by the SVD transform which is applied on the original detail LL of the original image) and the matrices S_W , then we calculate the new matrix D^* using the matrices U_1 , V_1 obtained during embedding process, then applying the inverse DCT on the new matrix D^* Which gives G. Finally to extract the watermarkW1, we calculate the inverse DWT of original detail LL_1, LH1, HL1 and G.For extraction the second watermark W2, the DCT transform is applied to HH_w* gives us T_W after the SVD transform is applied on T_W which gives us three Matrices: U_{ww}, V_{ww} and S_{ww} , afterto find the matrix Sr_1 using the original matrix S_3 obtained during process of embedding and S_{WW}, then we calculate the new matrix D22* using the matrices: U_2,V_2 of original Watermark W2 and S_r1, then applying the inverse DCT on the new matrix D22* Which gives the new matrix B .Finally to extract the watermark W2, we calculate the inverse DWT of original detail LL_2,HL_2,LH_2 and B.

3.2.1. Extraction of Watermark W_1

- Decompose the watermarked image I_W* (possibly attacked) in four sets coefficients: LL_W*,HL_w*,LH_w* and HH_w*;
- Perform the SVD on LL_w*to obtain: SVD(LL_w*)=U_w* x S_W* x V_W*' ;
- The corrupted watermark is obtained by : S_r=(S-S_w*)/4 ;
- The matrix that contains the watermark is computed: D*=U_1xS_rxV_1';
- Obtain the extract watermark $W1^*$by performing the inverse DWT using the sets coefficients of original watermark W1:LL_1, HL1, LH1 and D*.

3.2.2. Extraction of Watermark W_2

- Apply the DCT on HH_w*to obtain T_w ;
- Apply the SVD on T_w to obtain:

$$SVD(T_w) = U_{ww} \times S_{ww} x V_{ww}' ;$$

- The corrupted watermark is obtained:Sr_1 = (S_3 –S_{ww})/4;
- The matrix that contains the watermark is computed: $D22^*$ =U_2xSr_1xV_2' ;
- Then perform the inverse DCT on D22*;
- Obtain the extract watermark W2* by performing the inverse DWT using the sets coefficients of the original watermark W2: LL2, HL2, LH2 and D22*.The detailed process of watermark extracting is illustrated in the figure 4.

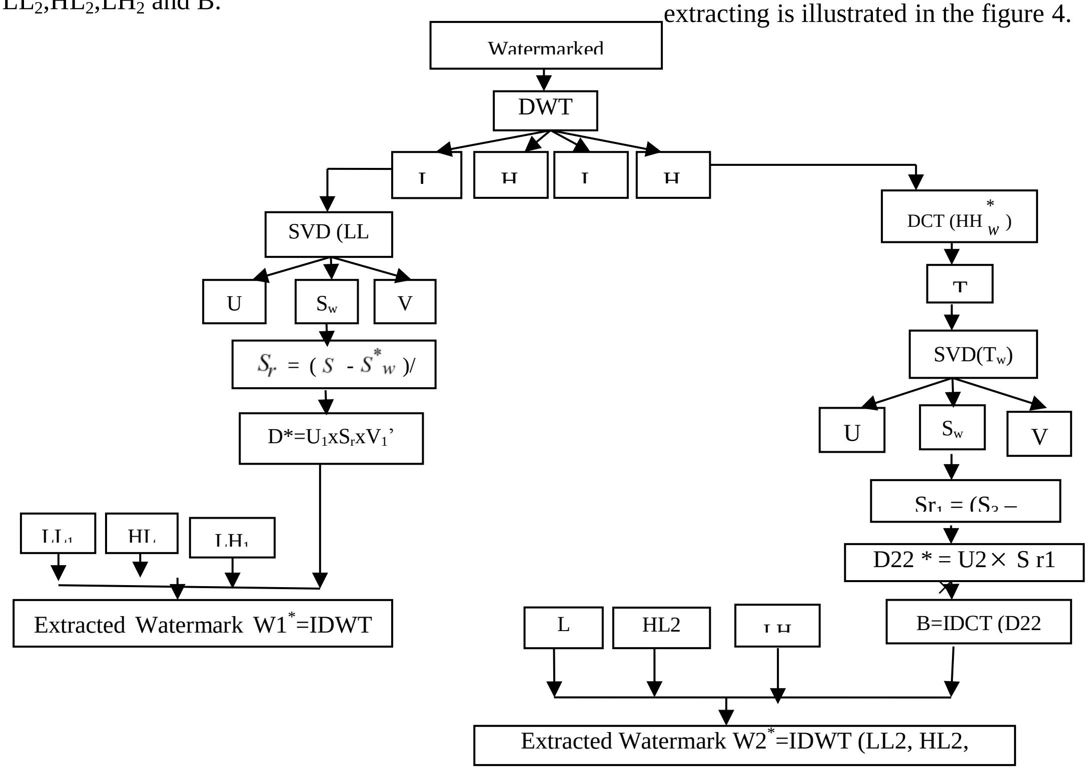


Fig. 4. Watermark extraction Process

4. EXPERIMENTAL RESULTS

4.1. Discussion

The performance of the proposed method (watermarked image) is simulated by the metric NCC ('Normalized cross co relation') which is the quality of Extracted Watermark between watermark image and Extracted Watermark image and also was used to measure the similarity between original watermarks W and the extracted watermarks W' that is defined as below:[14].

$$NCC = \frac{\sum_i \sum_j W(i,j).W^*(i,j)}{\sum_i \sum_j W(i,j)^2} \qquad (1)$$

Where $W\,(i,j)$ is the pixel values at the position (i, j) of the original image and $W^*\,(i,j)$ is the pixel values at the position (i, j) of the watermarked or image to which it is to be compared with original one, respectively. The Peak Signal to Noise Ratio (PSNR) and SNR (signal noise to ratio) [13] between Original Image and Watermarked Image which are defined as below:

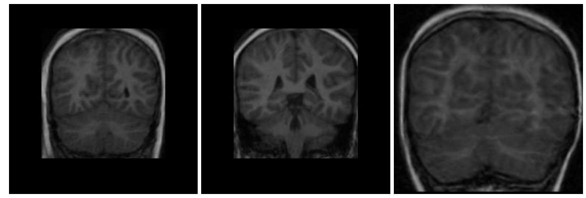
$$PSNR = 10.\log_{10}\frac{X\max^2}{MSE} = \frac{255^2}{MSE} \qquad (2)$$

$$SNR = \frac{\sum_1^M \sum_1^N I^2}{\sum_1^M \sum_1^N (I_w - I)^2} \qquad (3)$$

Where M and N are the height and width of the image. I Is the Original Image and I_w is the Watermarked Image and X is the peak signal value of the original image. Images having high PSNR value are preferable. For a good image the SNR value must be high.

4.2. Results

To evaluate the proposed method we use three medical images IRM_31, IRM_32 and IRM_33 256×256 gray scale (as shown in Figure 5 (a), (b), (c)).The original watermark image W1 of sizes 1 × 206 and the original watermark image W2 of 106 ×143 size are shown in figure 6.The figure7 shows the results after watermarking process of the Original image. Original watermark and extracted watermark are shown in figure 8.To estimate the watermark imperceptibility between cover image and watermarked image for proposed technique, we used two parameters SNR and PSNR .To estimate the similarity between the original watermark and the extracted watermark using normalized correlation (NCC).The bigger the value of correlation coefficient better is the robustness of watermark. Table 1 shows the SNR, PSNR between original and watermarked images without attacks and shows the NCC [14] between the original and extracted watermark and their comparison between DWT-DCT-SVD method [20][21].



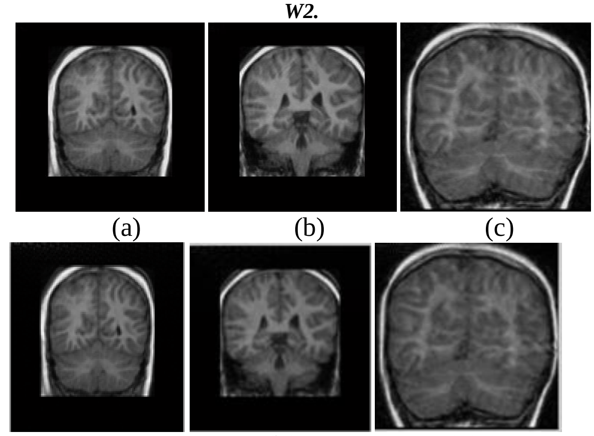
(a) (b) (c)

Fig. 5. Original image: IRM_31, (b) IRM_32, (c) IRM_33.

(a)

(b)

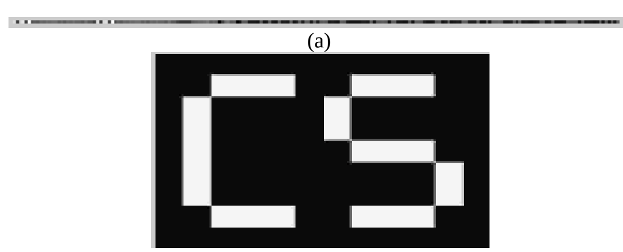
Fig. 6. *Original* Watermark image: (a) *Watermark W1, (b) Watermark W2.*



(a) (b) (c)

(a') (b') (c')

Fig.7. Watermarked image:(a) watermarked image_31,(b) watermarked image_32, watermarked image_33 after DWT-DCT-SVD method , (a') watermarked image_31,(b') watermarked image_32, (c') watermarked image_33 after Proposed approach.



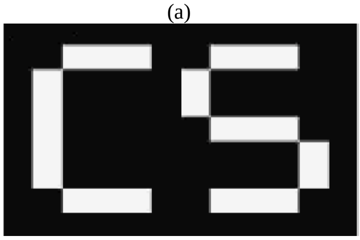
(a)

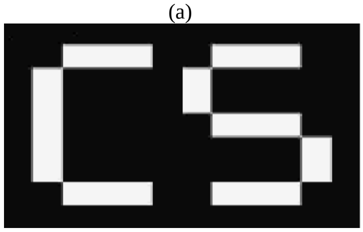
(b)

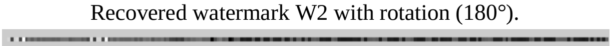
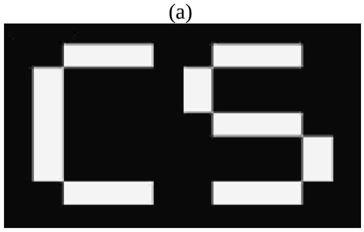
Fig.8. (a) Recovered watermark W1 without attack, (b) Recovered watermark W2 without attack.

TABLE 1: Comparison of the proposed watermarking method and the method of DWT-DCT-SVD.

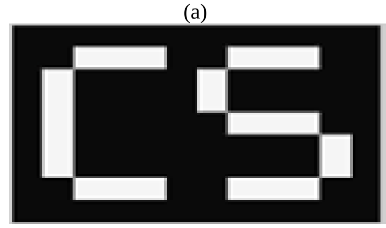
	DWT-DCT-SVD				Proposed method				
	PSNR	**SNR**	**NCC**	**Elapsed_time**	**PSNR**	**SNR**	**NCC1**	**NCC2**	**Elapsed_ time**
Image_31	36.2465	20.1769	0.99972	8.42	**44.012395**	**27.93996334**	**0.9964422**	**0.9998849**	**23.6653517**
Image_32	36.4044	19.6194	0.99970	8.72	**45.587506**	**28.802519257**	**.9983543**	**0.9998865**	**21.5749383**
Image_33	35.6121	21.8558	0.99953	8.81	**47.309064**	**33.552824960**	**0.9984433**	**0.9998873**	**25.8181655**

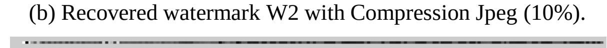
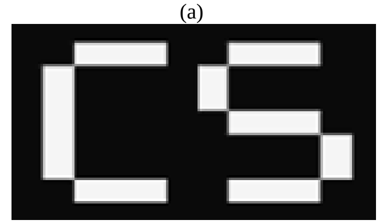
(a)

(b)
Fig.9-(a) Recovered watermark W1 with rotation (270°), (b) Recovered watermark W2 with rotation (270°).

(a)

(b)
Fig.10-(a) Recovered watermark W1 with rotation (180°), (b) Recovered watermark W2 with rotation (180°).


(a)

(b)
Fig.11-(a) Recovered watermark W1 with, (b) Recovered watermark W2 with rotation (90°).

To investigate the robustness of the algorithm, the watermarked image was attacked by applying JPEG compression, with a quality factor varying 10%, salt & pepper (with a quality factor 0.006) and rotation(90°,180°and 270°).(As shown in Table 2 and Table 3).

(a)

(b)
Fig.12. (a) Recovered watermark W1 with Compression Jpeg (10%), (b) Recovered watermark W2 with Compression Jpeg (10%).


(a)

(b)
Fig.13. (a) Recovered watermark W1 with Cropping (5%), (b) Recovered watermark W2 with Cropping (5%).

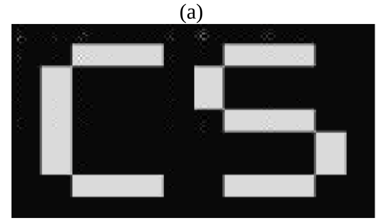

(a)

(b)
Fig.14-(a) Recovered watermark W1 with salt &pepper (QF=0.006), (b) Recovered watermark W2 with salt &pepper (QF=0.006).

TABLE 2. Comparison by PSNR of the performance of the proposed watermarking method and DWT-DCT-SVD method under attack.

	DWT-DCT-SVD					
	PSNR					
	Rotation (90°)	**Rotation (180°)**	**Rotation (270°)**	**Compression JPEG**	**Cropping**	**Salt &pepper**
Image_ 31	18.6791903168599	20.0564984662468	18.6791903168599	33.8306983532844	24.17784929562	35.4115
Image_ 32	20.5777902121331	19.6281556359074	20.5777902121331	33.7794615863222	25.5352332830523	35.6817718442444
Image_ 33	18.6698847681474	17.4615227438526	18.6698847681474	32.0680913939687	22.9118584346561	37.1613376942075
Proposed method						
PSNR						
	Rotation (90°)	**Rotation (180°)**	**Rotation (270°)**	**Compression JPEG**	**Cropping(5%)**	**Salt &pepper**
Image_31	18.9962456832509	20.3373351441839	18.9962456832509	34.7142194111571	24.3955771708494	35.3604895478714
Image_32	20.7581026666703	19.8251416713788	20.7581026666703	34.8785942110533	25.681125248267	35.7208019063138
Image_33	18.8570642594712	17.6066427025262	18.8570642594712	33.3593458765117	23.2107087756612	37.2122757046533

The NCC values of the extracted watermarks after applying various attacks are shown in the Table 3.

TABLE 3. Comparison by NCC of the performance of the proposed watermarking method and the method of DWT-DCT-SVD under attack.

	DWT-DCT-SVD	**Proposed method**	
	NCC	**NCC1**	**NCC2**
Image_31			
Rotation (90°)	0.999720888784919	**0.999599838782352**	**0.999884918680135**
Rotation (180°)	0.999720888784919	**0.999599838782352**	**0.999884918680135**
Rotation (270°)	0.999720888784919	**0.999408843332659**	**0.999890632419953**
Compression	0.999719256849283	**0.998908759051357**	**0.999895529917262**
Cropping	0.999769847913107	**0.986982464519914**	**0.999884918606083**
Salt &Pepper	0.9998	**0.973743920943171**	**0.997738935832268**
Image_32			
Rotation (90°)	0.999701307643859	**0.998966780552113**	**0.999886551234541**
Rotation (180°)	0.999701307643859	**0.998966780552113**	**0.999886551234541**
Rotation (270°)	0.999701307643859	**0.998966780552113**	**0.999886551234541**
Compression	0.999672757176938	**0.998103521905205**	**0.999895529917262**
Cropping	0.999739655639425	**0.963868295435495**	**0.999885734692596**
Salt &Pepper	0.9999	**0.971845120308229**	**0.997689098174895**
Image_33			
Rotation (90°)	0.999538578187655	**0.999255813625857**	**0.999887367364161**
Rotation (180°)	0.999538578187655	**0.999312393160696**	**0.999889000081144**
Rotation (270°)	0.999538578187655	**0.999255813625857**	**0.999887367364161**
Compression	0.999594854575909	**0.998617390792195**	**0.999895529917262**
Cropping	0.999656438568911	**0.988773019014099**	**0.999889815974136**
Salt &pepper	0.9999	**0.987920074441603**	**0.998071056547793**

The PSNR values and the NCC in table 2 show that the proposed watermarking technique is having the greatest value of the PSNR than DWT-DCT-SVD. Experimental values of table III shows that the proposed algorithm more robust against the salt & pepper noise than the compression JEPG, cropping and rotation attack.

5. CONCLUSIONS

In this paper, we presented a novel watermarking scheme R-DWT-DCT-SVD to insert two types of watermarks into digital medical image IRM images check for the purpose of increasing the security of data hiding which can be applied both in the copyright protection and the content authentication domain; we use the frequency transformations DWT, SVD and DCT.

Even though we obtained satisfying results, the R-DWT-DCT-SVD based method is offered better capacityand imperceptibility for IRM_33 than IRM_34 and IRM_31 than the DWT-DCT-SVD method and show that our system can resist against differenttypes of image processing attacks like geometric distortions such as compression JPEG, we cannot prove that it will resist all attacks. Our future work is to use color image watermarking by inserting two different watermarks (reversible watermark W1 and watermakW2) image into RGB image and test the robustness against other attacks.

REFERENCES

[1] Xu Yan-ping, Jia Li-qin,"Research of a Digital Watermarking Algorithm Based on Discrete Cosine Transform", Proceedings of the Third International Symposium on Electronic Commerce and Security Workshop (ISECS ’10) Guangzhou P R China, pp. 373-375, 29-31 July 2010.

[2] Chi-Man Pun and Ioi-Tun Lam," Fingerprint Watermark Embedding by Discrete Cosine Transform for Copyright wnershipAuthentication",INTERNATIONAL JOURNAL OF COMMUNICATIONs, Volume 3, Issue 1, 2009.

[3] Y.I. Khamlichi, M. Machkour, K. Afdel, A. Moudden, "Medical Image Watermarked by Simultaneous Moment Invariants and Content-Based for Privacy and Tamper Detection", Proceedings of the 6th WSEAS International Conference on Multimedia Systems & Signal Processing, Hangzhou, China, April 16-18, pp.109-113, 2006.

[4] Pranab Kumar Dhar, Mohammad Ibrahim Khan, and Jong Myon Kim1. "A New Audio Watermarking System using Discrete Fourier Transform for Copyright Protection", IJCSNS International Journal of Computer Science and Network Security, Vol. 10 Number 6, June 2010.

[5] Chin-Chen Chang, Piyu Tsai and Chia-Chen Lin, "SVD based digital image watermarking scheme. Pattern Recognition Letters 26, pp.1577-1586, 2005.

[6] Hasan Demirel, CagriOzcinar, and GholamrezaAnbarjafari, "Satellite Image Contrast Enhancement Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Geoscience and remote sensing letters, VOL. 7, N°. 2, April 2010.

[8] Osamah M. Al-Qershi, Khoo Bee Ee. Authentications and Data HidingUsing a Reversible ROI-based Watermarking Scheme for DICOM Images, World Academy of Science, Engineering and Technology 50, 2009.

[7] I. Cox, M. Miller, and J. Bloom. Digital Watermarking Principles & Practices. Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.

[9] A.Piva , M.Barni,F.Bartolini,andV.Cappelini.DCTbased watermark recovering without resorting to the uncorrupted original image.Inproc.ICIP,pages 520-523,1997.

[10] Tao, P&Eskicioglu, AM 2004,"A robust Multi Discrete wavelet Transform Domain", in Symposium Management SystemsV,Philadelphia,PA.

[11] Dan Kalman. A Singularly Valuable Decomposition: The SVD of a Matrix, February 13, 2002. [12] Liu, R. and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. On Multimedia, Vol. 4, No. 1 March 2002.

[12 D.V. Chandra. Digital Image Watermarking using Singular Value Decomposition. In 45th IEEE Midwest Symposium on Circuit and Systems, Tulsa, volume 3, pages 264–267, 2002. .

[13] B. Aiazzi, L. Alparone and S. Baronti. "Nearlosslessompression of 3-D optical data". IEEE Transactions on Geosciences and Remote Sensing, vol. 39, no 11, pp. 2547–2557, 2001.

[14] Ming-Shing Hsieh, "Wavelet-based Image Watermarking and Compression", Ph.D Thesis, Institute of Computer Science and Information Engineering National Central University,Taiwan, Dec. 2001.

[15] T. Cox, J. Killian, T. Leighton, and T. Shamoon. Secure Spread Spectrum Watermarking for Multimedia, 1997.

[16] Navas K A, Ajay Mathews Cheriyan,Lekshmi.M, ArchanaTampy.S, Sasikumar M. DWT-DCT-SVD Based Watermarking,” Electronics and Communication Engineering Dept. College of Engineering Trivandrum, Keral, 2008.

[17] MayankAwasthi, HimanshiLodhi .Robust Image Watermarking based on Discrete Wavelet Transform, Discrete Cosine Transform & Singular Value Decomposition, Advance in Electronic and Electric Engineering. ISSN 2231-1297, Volume 3, Number 8 (2013), pp. 971-976,2013.

Bekkouche Souad She was born in 1981; she is a MAB in computer science at the computer science department Mascara Algeria, she is PhD student in computer engineering, Research Interest in image watermarking technique

A K.M. Faraoun was born in Sidi Bel abbes, Algeria, in February 23, 1978. He received his master’s degree in computer science at the computer science department of Djilali Liabbes University- Sidi-Bel-abbes – Algeria in 2002, and his PHD in computer sciences in the field of artificial intelligence application for computer security. His current research areas include computer safety systems; genetic algorithms, dynamical systems, chaotic behavior, numbers theory and their applications for cryptography. He is currently a teacher at the computer sciences Institute of Djilali Liabess University, he teaches cryptography, information theory, operational researches and information security. He has published several papers in international journals. Dr. Faraoun is a member of the Evolutionary Engineering and Distributed Information Systems Laboratory, EEDIS