Journal of Computer Engineering
ISSN 10003428

Original Research Article
Vol 10, Issue 6, 2021 | ISSN: 1000-3428

Secure Image Watermarking via Wavelet Transform and Singular Value Decomposition

Amira El Hachim, Youssef Ziani, Mohamed Amine Benabdallah

Department of Computer Science, University of Algiers, Algeria; Laboratory of Advanced Studies and Research in Mathematics and Computer Science, Constantine 1 University, Constantine, Algeria; Department of Electrical Engineering, University of Science and Technology Houari Boumediene, Algiers, Algeria

***Abstract*—**In this paper, we present a technique of secure watermarking of grayscale and color images. This technique consists in applying the Singular Value Decomposition (SVD) in LWT (Lifting Wavelet Transform) domain in order to insert the watermark image (grayscale) in the host image (grayscale or color image). It also uses signature in the embedding and extraction steps. The technique is applied on a number of grayscale and color images. The performance of this technique is proved by the PSNR (Pick Signal to Noise Ratio), the MSE (Mean Square Error) and the SSIM (structural similarity) computations.

I. Introduction

The ways that permit to access to information have been improved thanks to the fast development of digital technologies. They permit to store, transfer and process digital data with less time, better efficiency and lower complexities. The role of internet is very important in circulation of unauthorized and illegal digital information. This causes the increase of risk of hampering authenticity of a digital data and violating owner right. One protection way of digital content against illegal distribution and reproduction consists in embedding some extra content (named watermark) into it [1]. The information has to be inserted in both robust and secure manner such that it remains resistive to malicious attempts of destruction [1], [2]. The watermark is usually the information about the digital data it intends to protect [1].

Watermarks have to be inserted in such a way that they remain detectable as long as the perceptual quality of the digital content stays at an acceptable quality [3].

Generally, in any watermarking system there are four following parts [1]: Watermark, Carrier, Encoder and Decoder.

Fig. 1 [1], [4] explains the conceptual model of the watermarking system. The host image depicts the carrier which necessitates protection. The watermark encoder inserts the watermark into the host image. The watermark can be a binary sequence or a pseudo-random number. The optional key is employed in order to improve the security of the watermarking system. Decoder permits to estimate the watermark from the received of the watermarked image with
the key help and the host image if required. On communication channel, the watermarked image is the subject of diverse forms of manipulations.

In this work, a robust, blind and secure watermarking technique is presented which is based on LWT and SVD. The rest of this paper is organized as: In Section II, we will present some recent image watermarking techniques applied in spectral domain including our proposed one based on data compression and DCT (Discrete Cosine Transform). Section III describes Digital Watermarking using DWT-SVD. Section IV deals with LWT and describes the proposed image watermarking technique. In Section V is given a detailed description of the proposed watermarking scheme. In Section VI are presented results and discussion and finally conclusions are drawn in Section VII.

II. Image Watermarking in Spectral Domain

There are different transforms that bring the image into frequency domain. Among most famous of those, we mention the FFT (Fast Fourier Transform) and the DCT. In frequency domain, coefficients are slightly modified [5]. This makes some unnoticeable modifications in the whole image which becomes more robust against attacks compared to spatial techniques [5]. Among the most popular techniques in this category, we can mention the watermarking scheme proposed by Cox et al. [6]. In this technique [6], the DCT is applied on the host image (original image) and we obtain a matrix having the same size, but with values of "double" class [6]. As illustrated in Fig. 2, the absolute values of the coefficients which correspond to the low frequencies, are higher and located in the up-left corner of the presented square in Fig. 2, though the high frequency coefficients appear in the downright with lower absolute values (Fig. 2).

To have a better concept of values, it is worth mentioning that the largest value corresponds to the DC value of the image positioned in (0,0) of the square [5]. The message is also coded into a spread spectrum sequence [5]. This step makes the watermarking message robust to some attacks like JPEG compression which aims to omit the unnoticeable details in high frequencies. Concerning the embedding process of the watermark in the cover image, it can be summarized by the flowchart presented at Fig. 3.

How to cite: Amira El Hachim, Youssef Ziani, Mohamed Amine Benabdallah (2021). Secure Image Watermarking via Wavelet Transform and Singular Value Decomposition. Journal of Computer Engineering, 10(6), 56–61. DOI: https://doi.org/10.5281/zenodo.19343197

For modifying the DCT coefficients, Cox et al. [6] have used 1000 largest coefficients to insert a watermark sequence having 1000 as length. The only exception is the DC term, positioned in (0,0) of the DCT matrix, that should not be modified due to its perceptible change in the whole picture brightness. On the other hand, high frequencies are simply
modified under common attacks such as JPEG compression. However, authors in [6] suggest not modifying some coefficients near to DC term due to their perceptible change. The suggested zone is approximately depicted in Fig. 2. Coefficients are changed according to the bits stream of the message employing (1) [6]:

$$\cdot 1 \quad \cdot \qquad (1)$$

where is the original coefficient, is watermarked, corresponds to the bit of the message data and is the watermarking strength. The formula is simply suggesting that if a coefficient is larger, it should be modified to a greater extent. The process of extraction consists in subtracting the original DCT coefficients from the watermarked image ones
(Fig. 4) [6].

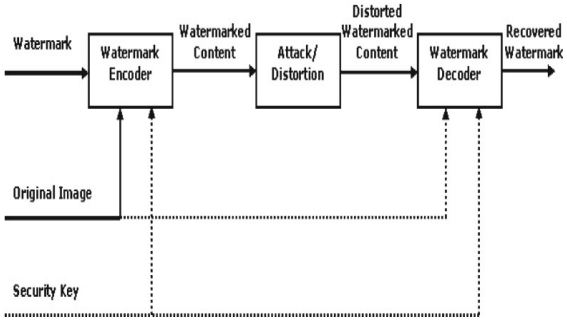


Fig. 1 Typical watermarking system

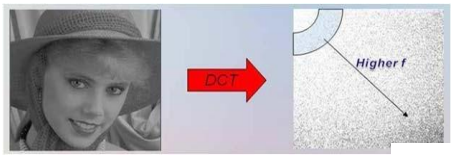
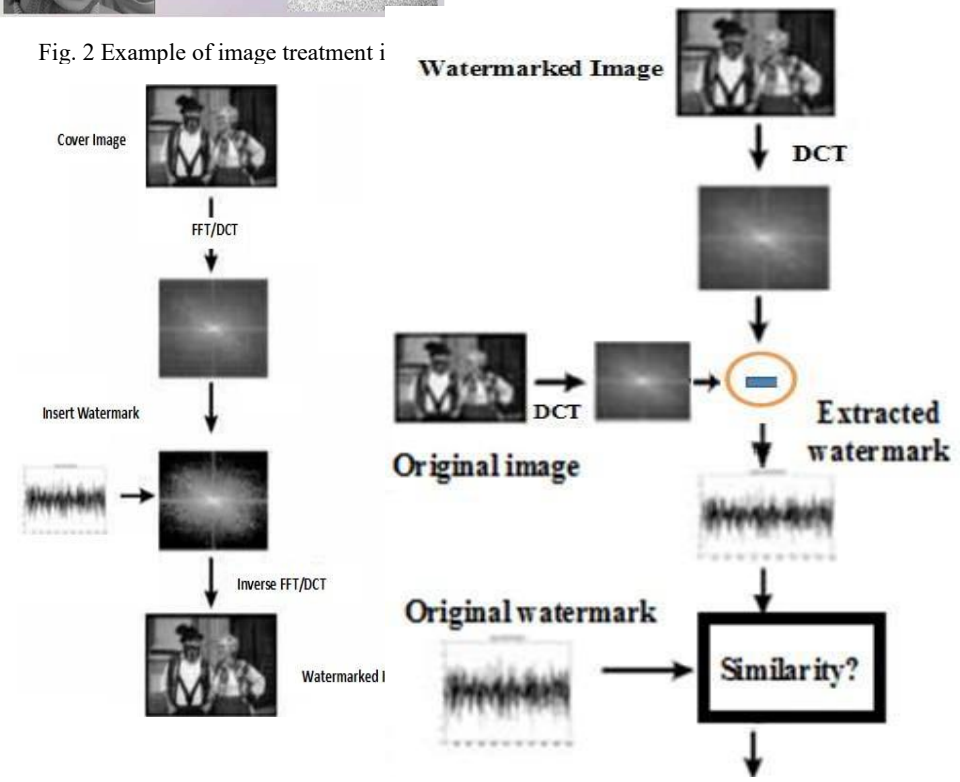


Fig. 2 Example of image treatment i

is a two dimensional matrix. Secondly, the DCT is applied to that matrix and after that, the Watermark signal is



inserted into the DCT coefficients [7]. This watermark signal is obtained after compression of the original signal which is a speech waveform signal. This compression is performed in the wavelet domain [7].

III. Digital Watermarking Using DWT-SVD

In [1] was proposed a blind image watermarking technique based on DWT (Discrete Wavelet Transform) and SVD. Singular values (SVs) of high frequency sub-image, HH, are used for optimization of perceptual transparency and robustness constraints. Though, most of the SVD-based schemes prove their robustness, little attention has been paid to their security aspect. Consequently, to improve security, in [1] was introduced a signature-based authentication mechanism at the decoder. Resulting blind watermarking scheme is secure and robust.

IV. The Proposed Technique of Image Watermarking

The technique consists at first step in applying the LWT to the cover image, I in order to obtain four sub-images or subbands which are LL, HL, LH and HH. These sub-bands are illustrated in Fig. 5.

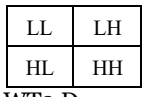


Fig. 5 LWT2 Decomposition

The LWT application to an image permits to divide it into four sub-bands which are (LL), (LH), (HL) and (HH). (LL) designates a lower resolution approximation component. (HL), (LH) and (HH) are respectively horizontal, vertical and diagonal detail components. The LL sub-band is obtained after applying the low-pass filtering to the rows and columns. It contains a rough description of the image.

The HH sub-band is high-pass filtered in both directions and contains the high-frequency components along the diagonals. After the image processing by the wavelet transform, most of the information contained in the cover image is concentrated into the LL sub-band. The LH image contains mostly the vertical details information corresponding to horizontal edges.

The second step of the technique consists in applying the SVD to both the image and the watermark image in order to obtain three matrixes Uh, Sh and Vh for HH and Uw, Sw and Vw for the watermark image. Then SVs of the HH sub-band are replaced with those of the watermark image. After that, the signature is generated [8], [9]. Then, the signature is embedded into the sub-band LL. After that the SVD is applied in order to obtain the modified HH band which now holds the SV's of watermark image. Then the LWT inverse is applied to the modified LL, the modified HH, the LH and HL in order to have the watermarked image. Here the HH band should be the one modified with SV's.

The watermarking technique can be summarized by the following steps:

Watermark Embedding

1. Apply Haar wavelet and decompose cover image into four sub-bands: LL, HL, LH, and HH,
2. Use the Haar mother wavelet for the 4th level decomposition of the sub-band LL,
3. Apply SVD to sub-band HH,
4. Apply the SVD to the Watermark logo,
5. Replace SVs of the sub-band HH with those of the watermark,
6. Generate signature,
7. Embed the signature into host image.
8. Apply SVD in order to obtain the modified sub-band, . The latter holds now the SV's of the watermark logo,
9. Apply the inverse of LWT with the modified sub-bands, and in order to obtain the watermarked image.

Watermark Extraction

1. By Using Haar mother wavelet, the noisy watermarked image is decomposed into 4 subbands: LL, HL, LH, and HH,
2. Then, LL is decomposed up to the 4th level,
3. Apply the SVD to the watermark logo,
4. Then, the signature is generated using Uw and Vw matrices,
5. Extract signature from the sub-bands LLw_4 & HHw_4 using all coefficients which are in number of 512,
6. Compare the embedded and the extracted signatures,
7. Proceed to extract the watermark when the authentication is successful,
8. Apply the SVD to the modified sub-band ,
9. Extract the SVs from ,
10. Reconstruct the watermark using the SVs and orthogonal matrices, and .

V. Evaluation Criteria

Different criteria are used to qualify the watermarking algorithm. Among them, we can mention:

- Imperceptibility: The watermark imperceptibility is tested through the comparison between the original and the watermarked images. Different tests are frequently employed in this regard.
- MSE: It is performed to test the similarity between two images. It is expressed as:

$$- \Sigma \quad * \qquad (4)$$

- PSNR: It takes into count the signal strength (not only the error). It is expressed as:

$$. \quad \text{——}) \qquad (5)$$

- SSIM: The main problem about the previous two criteria is that they are not similar to what similarity means to human visual system (HVS). SSIM is a function expressed in (6) and introduced by Wang et al. [10] for overcoming this problem to a great extent.

(6)

μ, σ and σ are respectively the mean, variance, and covariance of the images, and c , c are the stabilizing constants

- Robustness: The watermark technique robustness can be evaluated by performing attacks on the watermarked image and evaluating the similarity between the extracted message and the original one. [5]

VI. Results and Discussion

Cover image Watermarked image signed with secret key

Extracted watermark

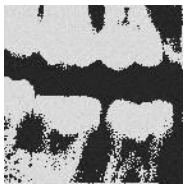


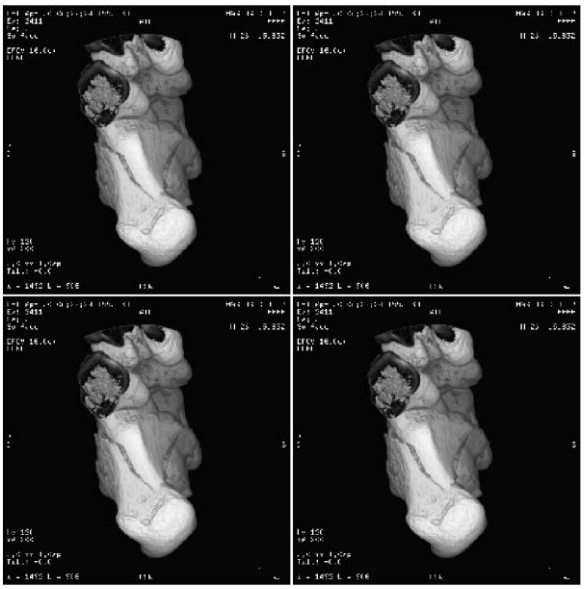
Fig. 6 Example 1 of image watermarking: The cover image (Lena) and the watermark image (tooth), psnr (cover_image, watermarked_image) = 39.6832, ssim (cover_image, watermarked_image) = 0.9596, psnr (watermark_logo, watermark_logo_extracted) = 30.5452, ssim (watermark_logo, watermark_logo_extracted) = 0.6721

Watermarked image signed with secret key

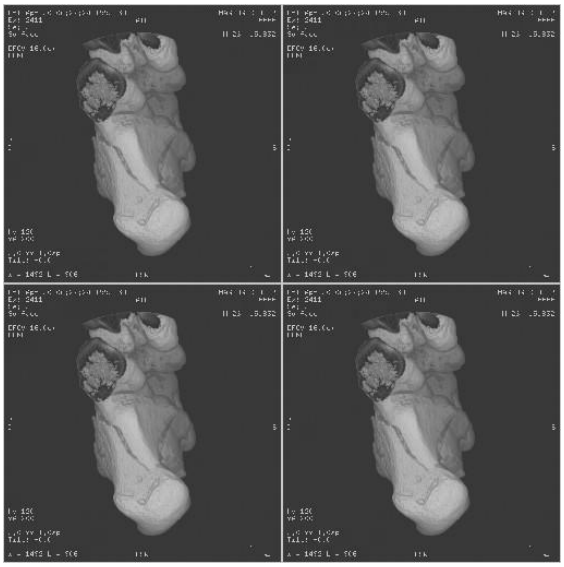
Extracted watermark

Fig. 7 Example 1 of image watermarking: The cover image (tooth) and the watermark image (copyright), psnr (cover_image, watermarked_image) = 95.95, ssim (cover_image, watermarked_image) = 0.9887, psnr(watermark_logo,watermark_logo_extracted) = 66.732. ssim(watermark_logo,watermark_logo_extracted)=0.985

In this section are given some image watermarking examples obtained from the application of the proposed technique on a number of grayscale and color images (grayscale images in Figs. 6, 7 and color images in Figs. 9, 10). In Fig. 8 is illustrated an example of medical image watermarking with a grayscale image (Woman). All these results show clearly the performance of the technique. In fact, according to the obtained values of PSNR, MSE and SSIM and also the perceptual quality; the technique permits to have good qualities of both the watermarked and watermark images.



(a)



(b)

(c) watermark logo

(d) Extracted watermark logo

Fig. 8 Example 4 of image watermarking: (a) the cover image: Dicom image anon.dcm and the (b) watermark image: woman, (c) Watermark_logo, (d) extracted watermark logo. psnr (cover image, watermarked_image) = 25.8128, ssim = 0.7809, psnr (watermark_logo, watermark_logo_extracted) = 95.6669

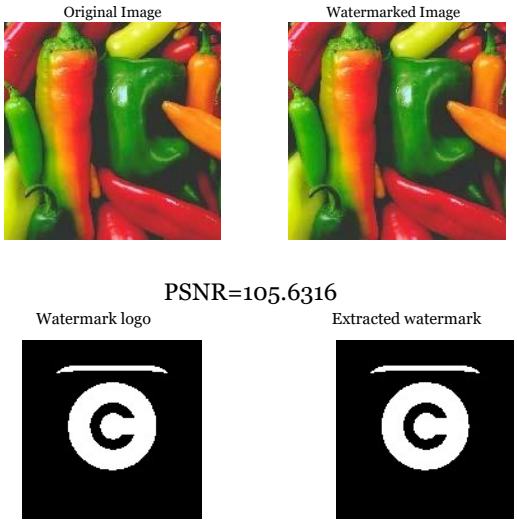


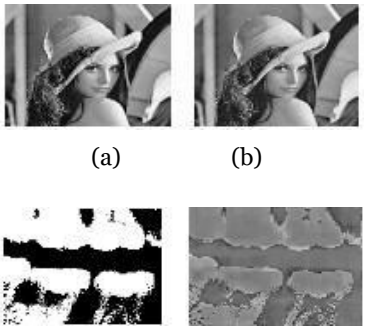
Fig. 9 Example of Color Image (peppers) watermarking using the proposed technique

Fig. 10 Example of Image (Lena) watermarking using the proposed technique

Examples 4 and 5 (Color Image Watermarking) show the performance of the technique because both the watermarked image and the extracted watermark logo are with good perceptual quality.

Figs. 9 and 10 show the performance of the technique because both the watermarked image and the extracted watermark logo are with good perceptual quality.

To test the robustness of the technique, we apply the JPEG compression attack on the watermarked image. In Fig. 11 is illustrated an example of image watermarking using the technique with JPEG compression attack.



(a) (b)

(c) (d)

Fig. 11 Example of image watermarking and watermark extraction after JPEG compression attack of the watermarked image (a) Original Image: Lena, (b) Watermarked image obtained after JPEG
Compression attack (c) Watermark, (d) extracted watermark after
JPEG Compression attack

Example 6 shows a certain robustness of the technique against JPEG Compression attack which is applied to the watermarked image.

VII. Conclusion

In this paper, we have presented grayscale and color images watermarking technique. This technique consists in applying the SVD in LWT domain in order to insert the watermark image in the cover image. It also uses signature in the
embedding and extraction procedure. The obtained results from the application of the technique on a number of images clearly show its performance. These results are obtained from PSNR, SSIM and MSE computation and they show the good perceptual quality of the watermarked image and the extracted watermark. Moreover, this technique shows its robustness against JPEG Compression attack.

References

[1] Akshya Kumar Gupta* and Mehul S Raval, "A robust and secure watermarking scheme based on singular values replacement," Sadhana¯ Vol. 37, Part 4, August 2012, pp. 425–440. © Indian Academy of Sciences.

[2] Katzenbeisser Stefan and Petitcolas Fabien A 2000 Information hiding techniques for steganography and digital watermarking. Norwood, MA, USA: Artech House, Inc.

[3] Lee Sin-Joo and Jung Sung-Hwan 2001 A survey of watermarking techniques applied to multimedia. Industrial electronics. Proceedings. ISIE 2001. IEEE International Symposium pp.272–277. Podilchuk C I and Delp E J 2001 Digital watermarking: Algorithms and applications. Signal Process. Mag. IEEE. 18(4): 33–46. Pooya Monshizadeh Naini (2011). Digital Watermarking Using MATLAB, Engineering Education and Research Using MATLAB, Dr. Ali Assi (Ed.), ISBN: 978-953-307-656-0, Intech, Available from: http://www.intechopen.com/books/engineeringeducationandre searchusin gmatlab/digital-watermarkingusing-matlab.

Cox, J.; Miller, M. L.; Bloom, J. A.; Fridrich J. & Kalker T. (2008). Digital Watermarking and Steganography, Morgan Kaufmann Pub.,
Elsevier Inc.

Mourad Talbi, Siraa Ben Ftima, Adnen Cherif, "Image watermarking using data compression," Computer Networks and Information Security
(WSCNIS), 2015 World Symposium on 19-21 Sept. 2015

R. Dhanalakshmi, K. Thaiyalnayaki, "Dual Watermarking Scheme with Encryption," International Journal of Computer Science and Information Security, Vol. 7, No. 1, pp.248-253,Jan. 2010.

http://www.ias.ac.in/sadhana/Pdf2012Aug/425.pdf,https://ww w.mathwo rks.com/matlabcentral/fileexchange/41686-dwt-svd-robust-and-securewatermarking-scheme, Vol. 37, Part 4, August 2012, pp. 425–440. §c Indian Academy of Sciences.

[10] Wang, Z.; Bovik, A. C.; Sheikh, H. R. & Simoncelli E. P. (2004).Image quality assessment: From error visibility to structural similarity. IEEE Trans. Image Processing, vol. 13, no. 4, pp. 600-612.