Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 132 (2018) 1441–1448

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Computational Intelligence and Data Science (ICCIDS 2018)

A DWT-SVD based Robust Digital Watermarking for Digital Images

Poonam[1], Shaifali M. Arora[2]

[1]*Research Scholar, GD Goenka University, Haryana*
Assistant Professor, Maharaja Surajmal Institute of Technology, Janakpuri, New Delhi
[2]*Associate Professor, Maharaja Surajmal Institute of Technology, Janakpuri, New Delhi*

Abstract

The rapid increase in usage of personal computers, internet and digital multimedia technology leads to easily sharing of digital data/ media. However, availability of numerous image processing tools facilitate unauthorized use of such data. Unauthorized users/ attackers can easily copy, delete or modify digital data. This problem of illegal modification/ reproduction of digital data, leads to innovation of some techniques which can protect intellectual property rights of digital data/ media. Recently, watermarking has been identified as a major tool to attain copyright protection/ authentication. A digital watermark can be embedded in host data in spatial domain as well as in frequency domain. In this work a hybridized technique incorporating Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) has been presented.

© 2018 The Authors. Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/3.0/)
Peer-review under responsibility of the scientific committee of the International Conference on Computational Intelligence and Data Science (ICCIDS 2018).

Keywords: *Digital watermarking; DWT; robust watermarking; SVD; copyright protection; multimedia security; hybridized digital watermarking*

Corresponding author: poonamdsk@gmail.com

1. Introduction

In the literature, researchers have introduced numerous techniques that address to the issue of illegally modification/ reproduction of data- information hiding techniques are one among them. The Information hiding techniques can be categorized as: steganography, cryptography and watermarking. Among the three mentioned techniques watermarking has proven to be a better method of hiding information. This is due to the fact that in Steganography

1877-0509 © 2018 The Authors. Published by Elsevier Ltd.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/3.0/)
Peer-review under responsibility of the scientific committee of the International Conference on Computational Intelligence and Data Science (ICCIDS 2018).
10.1016/j.procs.2018.05.076

the information is hidden such that only the intended recipient knows about the existence of message. In cryptography the data is converted into a secret code before transmission. This owes to the limitation that the user always require encryption key to decode the message.

Watermarks first appeared during the 13th century in Italy as marks of recognition embedded during manufacturing of paper. Charles Osborne and Andrew Tirkel in year 1992 first coined the term digital watermarking. The process of digital watermarking is to insert certain data (image, text, logo) known as watermark inside the host digital data (audio, image, video) without severely affecting the visible quality of host data. The watermark may be in the form of- binary logo, a randomly generated sequence, digital signature, some biometric traits. The main perseverance of digital watermarking is to offer copyright authentication and copyright protection. he applications where copyright protection is required robust watermarking is incorporated and for the application of copyright authentication fragile watermarking is done. Robust watermark exhibits the property of sustainability in host data even after intended/ unintended attacks, on the other hand fragile watermarks are such that the watermark vanishes when it is exposed to some intended/ unintended attacks [14]. The process of watermarking includes two main steps: watermark embedding to the cover image and watermark extraction from the watermarked image. During the process of embedding of watermark there are two inputs- one is the watermark to be embedded and the other is host data in which the watermark is to be embedded. In the extraction process, watermark is extracted from the received data with the help of detector and it is determined whether the watermark is present or not [1-2]. This paper is organized as- A brief introduction to characteristics of digital watermarking and general framework of digital watermarking system has been presented in section 2, overview of the existing frequency domain based watermarking techniques has been reviewed in section 3. A brief introduction to DWT-SVD based watermarking has been presented in section 4. The performance of implanted algorithm in this work has been analyzed in terms of MSE, PSNR and SSIM. Section 5 provides results obtained on simulation to show the performance of the algorithm. Finally, section 6 concludes the paper.

2. Characteristics and general framework of a digital watermark

2.1. Characteristics of digital watermark

The important characteristics for general watermarking system are discussed below.

a. Data Payload

It is an important characteristic of any digital watermarking system. Data payload denotes to the number of bits encoded by digital watermark within a specified time. For example a watermark that is capable of encoding M bits in a unit time is referred to as an M-bit watermarking system. Different data payloads are required in different applications [4].

b. Robustness

The robustness of watermarking scheme refers to survival of embedded watermark against any image processing and geometric attacks. These attacks may include spatial filtering, copying, cropping, scaling, translation, compressing and rotation either intentionally or unintentionally [3-4].

c. Security

It is desired that watermark must remain a secret and is undetectable to unauthorized parties. Security of the watermark defines ability of watermark to be undetectable to unauthorized parties. Security of watermark also decides its resistance against attacks [2, 5].

d. Imperceptibility

The term imperceptibility refers to amount of likeness between the message image and the image that is watermarked [2-4]. Perceptual transparency is the main requirement of any watermarking system. In all applications of digital watermarking, watermark is inserted in the cover image, so the perceptual quality of host image gets affected. It is always desired that watermark is implanted in the message image in such a manner that the perceptual quality of message image don't get degraded after some extent.

e. Cost

The cost here refers to the computational cost involved in the entire watermarking process which includes embedding of watermark to host image and extraction of watermark.

f. Fragility

A watermark is fragile if it is sensitive to any slightest modification attempted by unauthorized users. A fragile watermark becomes undetectable on slightest modification attempted. This category of watermark is used in applications where copyright protection is required [14].

2.2 General Framework of Digital watermarking

Fig.1 shows the general working layout of digital watermarking process.

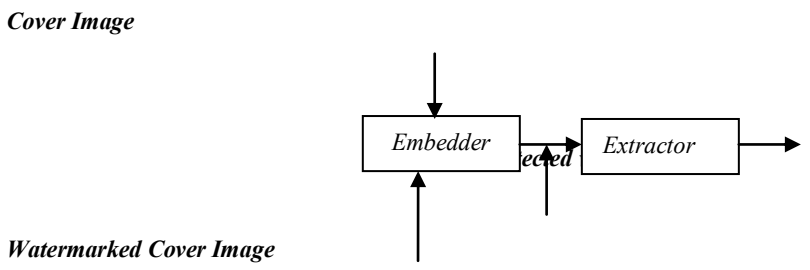


Fig. 1 General framework of digital watermarking system

The process of digital watermarking can be achieved in two main steps-

1. Embedding of data to be used as watermark on host image
2. Extraction of embedded watermark in first step from the watermarked cover image

There are mainly two inputs to the embedder unit- one is the cover message image and another is the message to be used as watermark that we want to encode in the host image. A watermark message used to be inserted on to the host message image can be a randomly generated sequence, a digital signature, some extracted features of the host image, biometric traits, combination of bits, logo or some text [2-3, 9]. The watermarked image is then transmitted or recorded. The implanted message can be retrieved from the watermarked cover image by using the extractor unit that will check for the presence of watermark.

3. A brief survey on transform domain watermarking

A non-blind digital watermarking algorithm in DCT domain was introduced by I.J. Cox *et al.* (1997) [1]. In this, the watermark has been implanted into highest magnitude DCT quantities of an image. The simulation results shows high robustness as these DCT coefficients are capable to show resistance against various image processing attacks. However, as the proposed algorithm is non-blind it is inappropriate for many applications. Wen-Nung Lie *et al.* (2000) [6] proposed 2- DCT domain techniques that embed single or multiple watermarks. To achieve a balanceamong robustness and visible quality the watermarks have been rooted in the middle band. Their presented technique has proven its robustness against various introduced geometric as well as non-geometric attacks. M. Barni et al. (2001) [7] has introduced a wavelet based algorithm. In this the authors has considered HVS (Human Visual System) characteristics. Pixel by pixel masking has been performed by keeping into consideration of texture in addition with luminance values of each sub band. The authors have used a pseudo random sequence as watermark that has been embedded adaptively into DWT sub band coefficients. The simulation results of proposed scheme has shown that this algorithm provides a watermarking system that is highly robust against different image processing attacks. V.S. Verma*et al.* (2013) [8] introduced a highly invisible and robust watermarking scheme that is based on significant difference of LWT coefficients. In this proposed technique, blocks of CH3 sub band have been shuffled randomly and then a watermark has been embedded into the largest coefficient of this shuffled sub block. This algorithm has been tested with the help of simulating the algorithm by imposing numerous attacks. The simulation results have shown high robustness against the imposed image processing attacks along with good imperceptibility.

D. Singh et al. (2016) [9] presented a perceptually invisible and robust method for protection of copyrights. The authors have also incorporated DCT and Arnold Cat Map method to achieve encryption. The authors have addressed to the most frequently faced security problem of unauthorized reading and false positive detection with SVD. The authors have tested their proposed scheme for different attacks and the results have shown that the system is imperceptible as well as secure to different signal processing attacks. Falgun N. Thakkar et al. (2017) [11] introduced DWT-SVD based perceptually invisible image watermarking scheme intended for medical purposes. In this technique different frequency sub bands are evaluated by decomposing the medical image by applying DWT on region of interest of medical image. Block- SVD is then smeared on the low frequency sub band LL of ROI. Authors have tested their algorithm on various medical images such as X-Ray, mammography and CT scan. The proposed method provides high imperceptibility of watermarked image. The authors have also analyzed the method for robustness by implying various checkmark attacks. The analysis has shown that this scheme is highly robust against the imposed attacks.

4. DWT-SVD based digital watermark

Discrete wavelet transform (DWT) has proven to provide better robustness and visible transparency as compared to other techniques such as Discrete Cosine Transform (DCT) along with Discrete Fourier transform (DFT) among others [15]. In the process of DWT, the image under considerationgets decomposed into four frequency sub bands. The 2-D DWT can be interpreted as two 1-D transformations from which one 1-D transformation is accomplished over the rows of image array dividing the image into two halves vertically. The columns of the image array are divided into two halves horizontally by using another 1-D transformation process. This process of decomposition of image array results in four frequency subbands namely LL (low-low), LH (low-high), HL (high-low) and HH (high-high). Any of the sub band can further be subdivided by implying 2-D DWT again. Fig. 2 and Fig.3 illustrates the process of 2-D DWT decomposition and I level decomposition of an image respectively [10].

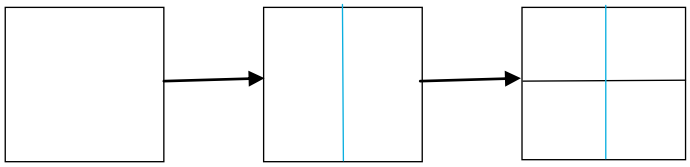


Fig.2 The process of 2-D DWT decomposition

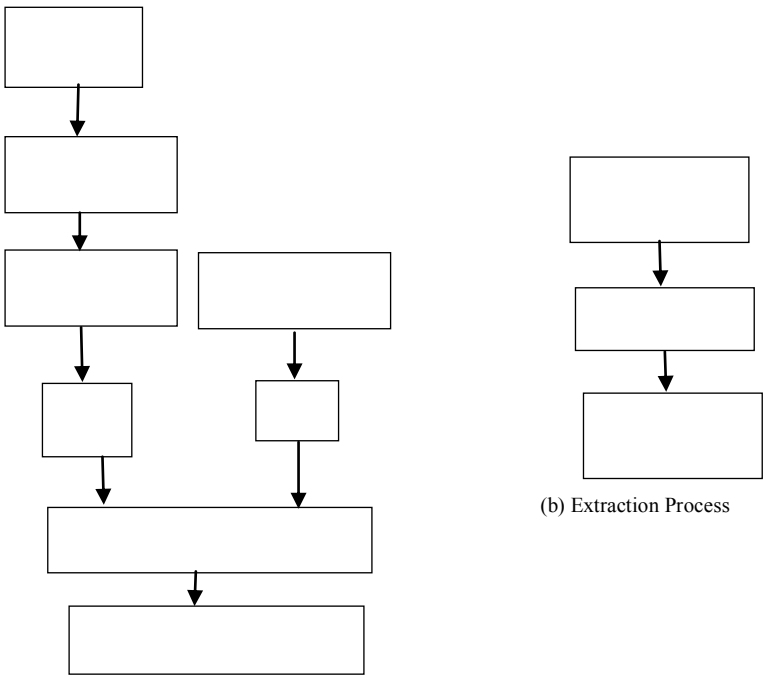
Fig. 3 An I- level 2-D DWT decomposition of Cameraman image

Singular Value Decomposition (SVD) can be interpreted as a matrix transformation procedure. This transformation first decomposes an MxN sized image as a 2-D MxN matrix after this SVD is applied over this MxN matrix to acquire three matrices namely U, S and V [13, 14]. Fig. 4 illustrates factoring of image A into three SVD matrices as:

$A = USV^T$

Fig. 4 Matrix division in SVD process

An implementation of robust DWT- SVD algorithm has been presented in this paper. For comparative analysis five different input images and one watermark image is considered. The values of MSE, PSNR, SSIM and BCR are calculated to make comparison. Fig. 5(a-b) is presenting the block diagram of DWT- SVD watermarking that has been implemented.



(b) Extraction Process

(a) Embedding Process

Fig. 5(a-b) Block Diagram of embedding and extraction process ofDWT-SVDwatermarking algorithm

5. Experimental results

Experiments have been conducted to test robustness against image processing and geometric attacks. Cameraman, Cell, Circuit, MRI and Pout images are used as input host test images and lena image has been used as a watermark for all the host images. MATLAB R2017b version 9.3.0.713579 has been used to perform the simulation on Windows10 platform over a Personal computer.

The original images and the image that has been used as watermark are shown in Fig. 6 whereas Fig. 7 shows corresponding watermarked images.

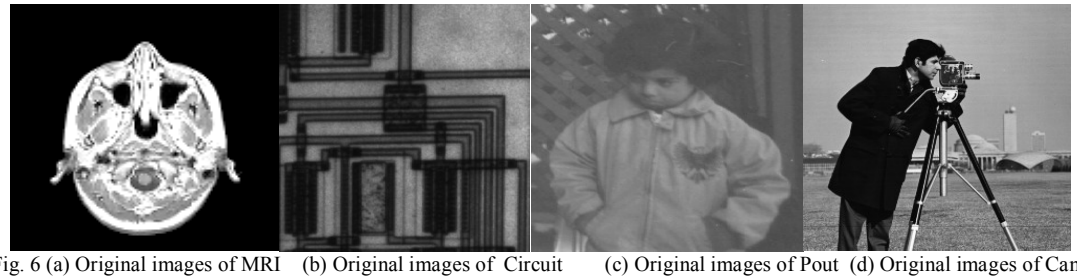


Fig. 6 (a) Original images of MRI (b) Original images of Circuit (c) Original images of Pout (d) Original images of Cameraman

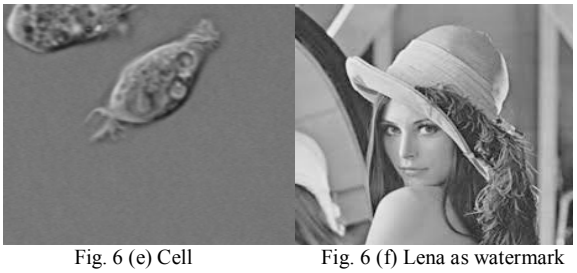
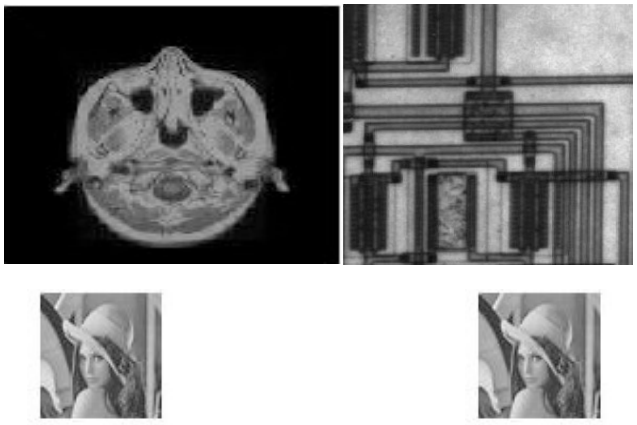


Fig. 6 (e) Cell Fig. 6 (f) Lena as watermark



7(a). Watermarked Images of MRI 7(b). Watermarked Images of Circuit

7 (c). Watermarked Images of Pout 7 (d).Watermarked Images of Cameraman 7 (e). Watermarked Images of Circuit

To assess the robustness of the implemented algorithm MSE, PSNR and SSIM has been calculated. Where,

$$MSE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I(x,y)-I'(x,y)\right)}{M \times N} \quad (1)$$

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \text{ (dB)} \quad (2)$$

$$SSIM = \left[l(I,I')\right]^{\alpha}.\left[c(I,I')\right]^{\beta}.\left[s(I,I')\right]^{\gamma} \quad (3)$$

Table 1 lists the simulation results for MSE, the results for PSNR, and SSIM are tabulated in Table 2 and 3 respectively. First column of these tables show the results achieved for an attack free watermarking system whereas the rest of columns depicts the values after imposing various attacks like-blurring, sharpening, resize, guassian noise, cropping,salt and pepper noise, along with rotation.

Table 1 Comparison of attained MSE values (attack free and with attacks) for different images

Attacks/Images	Camera man	Cell	Circuit	MRI	Pout
Attack free	1.75	0.2	0.01	0.21	1.25
Blurring	111.75	82.64	89.02	57.62	52.99
Sharpening	88.9	103.9	84.85	74.02	100.94
Resize	25.17	12.08	17.27	3.82	10.29
Gaussian Noise (10%)	25.21	1.53	19.17	8.32	4.67
Salt & Pepper Noise	58.55	36.21	21.21	38.91	31.71
Cropping	253.49	100.42	206.33	0.01	192.68
Rotation	226.78	199.21	227.35	79.47	213.49

Table 2 Comparison of attained PSNR values (attack free and with attacks) for different images

Attacks/Images	Cameraman	Cell	Circuit	MRI	Pout
Attack free	45.73	55.15	69.14	54.98	47.21
Blurring	27.68	28.99	28.67	30.56	30.92
Sharpening	28.67	27.99	28.88	29.47	28.12
Resize	34.15	37.34	35.79	42.35	38.04
Gaussian Noise (10%)	34.12	46.13	35.23	38.75	41.78
Salt & Pepper Noise	30.57	32.54	34.99	32.36	33.22
Cropping	24.12	28.15	25.02	68.72	25.32
Rotation	24.61	25.17	24.59	29.16	24.87

The first row of each table is presenting the results for MSE, PSNR and SSIM respectively, when the image is not exposed to any kind of image processing/ signal processing attack. Rest of the rows in table 1, 2 and 3 shows the simulation results achieved after imposing attacks like blurring, sharpening, resizing, guassian noise (10%), salt and pepper noise, cropping along with rotation on five different images.

Table 3 Comparison of attained SSIM values (attack free and with attacks) for different images

Attacks/Images	Cameraman	Cell	Circuit	MRI	Pout
Attack free	0.9977	0.9998	1	0.9997	0.9983
Blurring	0.1971	0.5182	0.6442	0.3524	0.7087
Sharpening	0.5771	0.6512	0.5667	0.5901	0.6098
Resize	0.9436	0.9855	0.9728	0.9964	0.9809
Gaussian Noise (10%)	0.9434	0.9964	0.9463	0.9838	0.9887
Salt & Pepper Noise	0.9417	0.9534	0.9144	0.9273	0.9383
Cropping	0.0452	0.6012	0.1346	0.9071	0.1411
Rotation	0.2011	0.3318	0.3141	0.8952	0.366

6. Conclusion

This paper presents a robust digital watermarking method incorporating two transformation techniques DWT and SVD. The watermark has been inserted over the singular values of the cover image's sub bands. Simulation results have shown that this technique is able to attain good imperceptibility, as the perceptual quality has not been degraded. Experiment results presented in table 3 illustrates that there are noteworthy improvements in terms of imperceptibility. The attained values of MSE, PSNR and SSIM demonstrates that DWT-SVD provide significant robustness when subjected to different image/signal processing attacks.

References

[1] Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamoon. "Secure spread spectrum watermarking for multimedia." *IEEE transactions on image processing* 6, no. 12 (1997): 1673-1687.

[2] Kutter, Martin, and Fabien AP Petitcolas. "Fair benchmark for image watermarking systems." *Security and Watermarking of Multimedia Contents* 3657 (1999): 226-239.

[3] Cox, Ingemar J., and Matt L. Miller. "The first 50 years of electronic watermarking." *EURASIP Journal on Advances in Signal Processing* 2002, no. 2 (2002): 820936.

[4] Cox, I. J., and M. L. Miller. "J. A, Bloom,"Digital watermarking," Chapter 5—Watermarking with Side Information." (2001).

[5] Poonam, S.M. arora, "Digital Watermarking: An Introduction" *International Journal of Applied Research* 3(4), 2017 128-131.

[6] Lie, Wen-Nung, Guo-Shiang Lin, Chih-Liang Wu, and Ta-Chun Wang. "Robust image watermarking on the DCT domain." In *Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on*, vol. 1, pp. 228-231. IEEE, 2000.

[7] Barni, Mauro, Franco Bartolini, and Alessandro Piva. "Improved wavelet-based watermarking through pixel-wise masking." *IEEE transactions on image processing* 10, no. 5 (2001): 783-791.

[8] Verma, Vivek Singh, and Rajib Kumar Jha. "Improved watermarking technique based on significant difference of lifting wavelet coefficients." *Signal, Image and Video Processing* 9, no. 6 (2015): 1443-1450.

[9] Singh, D. and Singh, S.K., 2017. DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimedia Tools and Applications*, *76*(11), pp.13001-13024.

[10] Ganic, Emir, and Ahmet M. Eskicioglu. "Robust DWT-SVD domain image watermarking: embedding data in all frequencies." In *Proceedings of the 2004 Workshop on Multimedia and Security*, pp. 166-174. ACM, 2004.

[11] Thakkar, F.N. and Srivastava, V.K., 2017. A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. *Multimedia Tools and Applications*, *76*(3), pp.3669-3697.

[12] Bhatnagar, Gaurav, and Balasubramanian Raman. "A new robust reference watermarking scheme based on DWT-SVD." *Computer Standards & Interfaces* 31, no. 5 (2009): 1002-1013.

[13] Sadek, Rowayda A. "SVD based image processing applications: state of the art, contributions and research challenges." *arXiv preprint arXiv:1211.7102* (2012).

[14] Honsinger, Chris. "Digital watermarking." *Journal of Electronic Imaging* 11, no. 3 (2002): 414.

[15] Kang, Xiangui, Jiwu Huang, Yun Q. Shi, and Yan Lin. "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression." *IEEE transactions on circuits and systems for video technology* 13, no. 8 (2003): 776-786.