

ROBUST DIGITAL WATERMARKING FOR DIGITAL IMAGES BASED ON DWT-SVD

Jyoti Bala (Research Scholar)¹

Dr. Shweta Rai (Professor), Department of Computer Science²

Swami Vivekanand University, Sagar (M.P.)^{1,2}

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 facilitates 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.

Keyword: Digital Watermarking, Digital Images, DWT-SVD.

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 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. The 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]. A brief introduction to DWT-SVD based watermarking has been presented in this paper. The performance of implanted algorithm in this work has been analyzed in terms of MSE, PSNR and SSIM. And provides results obtained on simulation to show the performance of the algorithm.

RELATED WORK

The literature is reviewed to examine available methods that could be used in watermarking. A good number of research work is conducted for contemporary watermarking methods.

Zhang et al. [2] suggested a robust color image watermarking algorithm. This algorithm converts the host color image watermarking into YUV and SVD is utilized to Y component. However, the watermark is embedded into the host image followed by the modification through Arnold transform and DWT. This method claimed robustness against geometric attacks, but it is seen that the PSNR value is very low compare to other watermark-related schemes.

Singh et al. [5] proposed a block-based DWT-SVD image watermarking approach where QR (quick response code) code is considered as a watermark image. Both the original image and watermark image are decomposed by 2-level DWT on a low-frequency band and the corresponding frequency band is separated into $m \times n$ block size. As the color image is used

here as a host image, SVD had to apply on each RGB component of a block to find the singular values of the watermarking. This method claims robustness against Gaussian noise and salt and pepper noise.

Similar work also has been pursued by others [6] in which a hybrid (DWT–SVD) watermarking scheme and a mathematical tool known as PSO (particle swarm optimization) are used for the efficient and secured watermarked image. RGB components of the host image are separated, and three-level DWT is performed on the R component. Then, SVD is applied on the approximate co-efficient of the R component. On the other hand, the watermark image is scrambled using Arnold transform and SVD is also used here to find the singular value of the watermark. The scaling factor is obtained from PSO to embed into the watermark image. This technique asserted good PSNR values adjacent to different attacks.

This issue was explored by Naik et al. [7], who introduced a robust watermarking technique based on DWT and SVD, which decomposed the host image by 2-level DWT and SVD is applied into the HL sub-band. The same working principle is performed on the watermark image and then the SVD of both images is embedded with a scaling factor to form a watermarked image.

Conceptually similar work has also been carried out by [8, 9] in which the cover image is divided by first-level Haar DWT and the SVD is added to the LH and HL sub-bands. Besides, the watermark is split into equal halves and LH and HL are modified before being inserted in the host image. The watermark is extracted from the reverse process. It is noted that this approach only demonstrates robustness for histogram equalization.

Harjito and Suryani [10] developed their watermarking scheme where white Gaussian is added to the scaling factor. But this technique is not resistant to some attacks like rotating, cropping, and blurring.

In the study [11], both the host and watermark are converted into the grayscale and the watermark is encrypted before the embedding procedure. Host image is decomposed by 2-D DWT and SVD is applied on lower-level frequency region. Encrypted watermark is then embedded into this LL sub-band of the host image.

A hybrid watermarking algorithm based on DWT–DCT is suggested by Akter et al. [3]. The authors applied 4th-level DWT into the original image and select HL₄ and LH₄ sub-bands. The properties of DCT are performed to the co-efficient of these said sub-bands. Concurrently, the watermark image is reformed and scramble it. The scrambled watermark

image is then transformed into DCT. The duo of these modified host image and watermark is embedded to form the watermarked image. The reverse process is used to extract the watermark. This algorithm is tested through PSNR and MSE to evaluate the performance and compared the existing method. It can be seen the PSNR value is found 36.52 dB of the watermarked image before the attack and it is 30.21 dB after the attack. This method only used Additive White Gaussian Noise (AWGN) to prove the performance, but other significant attacks were not tested here.

This method [12] presented a unique technique that showed a comprehensive rise of PSNR value. The host image and the watermark image are split into R, G, and B channels, and the single-level 2D DWT is applied to the selected frequency sub-bands. Increased levels of host image and watermark have been associated with 2D DFT and DCT respectfully. The SVD is performed on both images before the embedding. But this method is not being tested by a variety of attacks.

Another method is approached by [13], where DCT is used in host images and a watermark is embedded by a slightly modified version of Cox's formula. This system provides robustness upon adding a watermark in the low-frequency regions compare with high-frequency regions.

It is noted that some methods provide good PSNR values in terms of watermarked images, but the robustness is low for the watermark extraction procedure. The grayscale image works well in some approaches while several techniques produce better results in color images. Fewer algorithms show robustness upon geometric attacks where some other is applicable only for lean attacks. Considering the above-mentioned difficulties discussed in the literature review, a novel hybrid watermarking procedure is approached in the presented work. This mechanism is developed to consider the grayscale and color images. Watermark embedding and extraction are evaluated in both types of images and robustness is examined in various types of attacks. This scheme is allowed an acceptable imperceptibility rate along with security issues.

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. In the process of DWT, the image under consideration gets 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 (highhigh). Any of the sub band can further be subdivided by implying 2-D DWT again. Fig. 1 and Fig.2 illustrates the process of 2-D DWT decomposition and I level decomposition of an image respectively [10].



Fig.1 The process of 2-D DWT decomposition



Fig. 2 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 $M \times N$ sized image as a 2-D $M \times N$ matrix after this SVD is applied over this $M \times N$ matrix to acquire three matrices namely U , S and V [13, 14]. Fig. 3 illustrates factoring of image A into three SVD matrices as:

$$A = USV^T$$

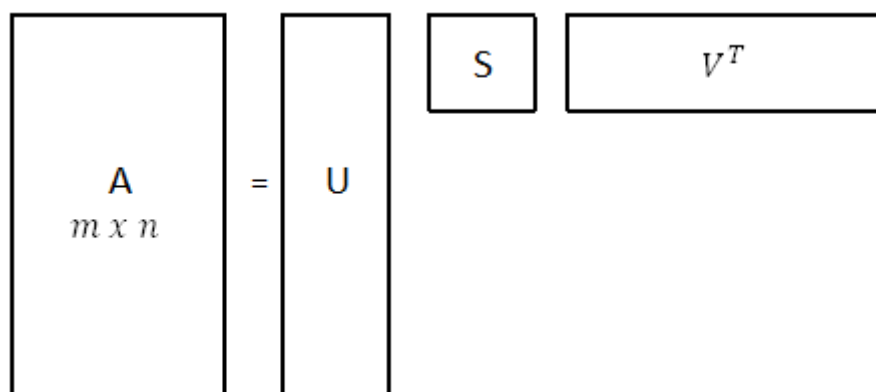


Fig. 3 Matrix division in SVD process

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. 4(a-b) is presenting the block diagram of DWT- SVD watermarking that has been implemented.

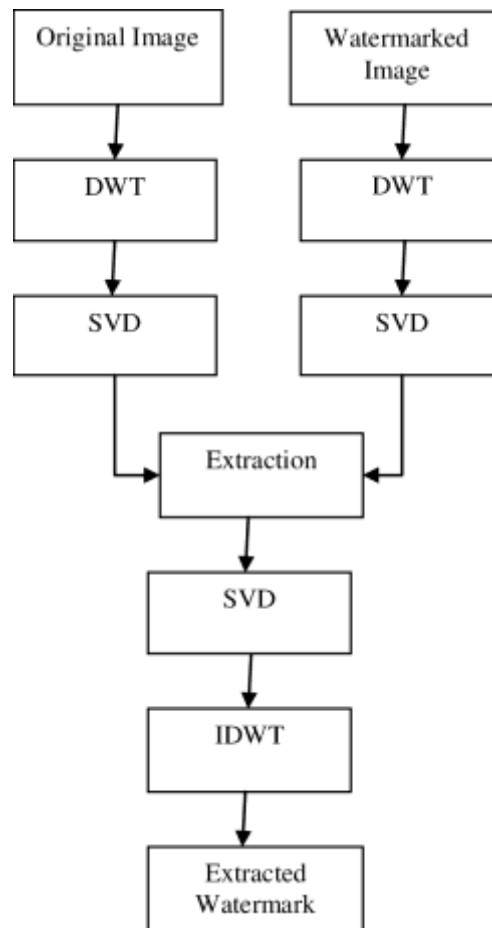


Fig. 4(a-b) Block Diagram of embedding and extraction process of DWT-SVD watermarking algorithm

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. 5 whereas Fig. 6 shows corresponding watermarked images.



Fig. 5 (a) Original images of MRI (b) Original images of Circuit (c) Original images of Pout (d) Original images of Cameraman

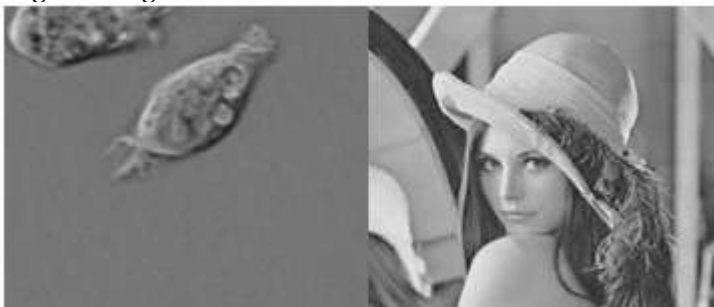
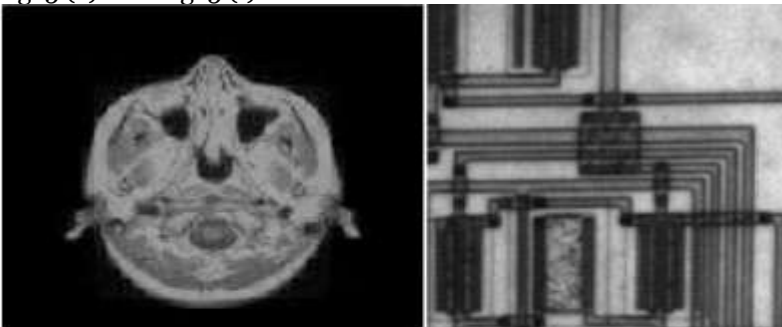


Fig. 5 (e) Cell Fig. 5 (f) Lena as watermark



6(a). Watermarked Images of MRI 6(b). Watermarked Images of Circuit



6 (c). Watermarked Images of Pout 6(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,

$$MSE = \frac{\sum_{x=1}^M \sum_{y=1}^N (I(x,y) - I'(x,y))^2}{M \times N}$$

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

$$SSIM = [l(I, I')]^\alpha \cdot [c(I, I')]^\beta \cdot [s(I, I')]^\gamma$$

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, gaussian 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, gaussian 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

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. Tarhouni N, Charfeddine M, Amar CB. Novel and robust image watermarking for copyright protection and integrity control. *Circuits Syst Signal Process.* 2020;39(10):5059–103.
2. Zhang L, Xiao JW, Luo JY. A robust color image watermarking based on SVD and DWT. *Int J Commun (IJC).* 2014;3:62.
3. Akter A, Nur-E-Tajnina, Ullah MA. Digital image watermarking based on DWT-DCT: evaluate for a new embedding algorithm. In: 3rd International conference on informatics, electronics and vision (ICIEV), Dhaka, p. 1–6, 2014.
4. Kumar S, Dutta A. Performance analysis of spatial domain digital watermarking techniques. In: International conference on information communication and embedded system (ICICES). Chennai, p. 1–4, 2016.
5. Singh RK, Shaw DK, Sahoo J. A secure and robust block-based DWT–SVD image watermarking approach. *J Inf Optim Sci.* 2017;38:11–925.
6. Sanku D, Kiran S, Takore TT, Kumar PR. Digital image watermarking in RGB host using DWT, SVD, and PSO techniques. In: Proceedings of 2nd international conference on micro-electronics, electromagnetics and telecommunications (Springer Nature), p. 333–342, 2018.
7. Naik NS, Naveena N, Manikantan K. Robust digital image watermarking using DWT+SVD approach. In: IEEE International conference on computational intelligence and computing research, Madurai, p. 1–6, 2015.
8. Wang B, Zhao P. An adaptive image watermarking method combining SVD and Wang-Landau sampling in DWT domain. *Mathematics.* 2020;8:691.

9. Shahrezaee M, Razmjoooy N. Image watermarking based on DWT–SVD. In: Proceedings of the 2nd international conference on combinatorics, cryptography and computation, p. 62–67, 2017.
10. Harjito B, Suryani E. Robust image watermarking using DWT and SVD for copyright protection. In: AIP Conference proceedings, 2017.
11. Gonge SS, Ghatol A. A robust and secure DWT–SVD digital image watermarking using encrypted watermark for copyright protection of cheque image. In: International symposium on security in computing and communications, p. 290–303, 2015.
12. Kallianpur AK, Bharath MV, Manikantan K. Digital image watermarking using optimized transform-domain approach. In: IEEE UP section conference on electrical computer and electronics (UPCON), Allahabad, p. 1–6, 2015.
- 13.** Parah SA, Ashraf S, Asharf A. Robustness analysis of a digital image watermarking technique for various frequency bands in DCT domain. In: IEEE International symposium on nanoelectronic and information systems, Indore, 2015. p. 57–62.