PSNR and Robustness Comparison Between DCT and SVD Based Digital Image Watermarking Against Different Noise and Attacks

Tarun Rathi[1(✉)], Rudra P. Maheshwari[2], Manoj Tripathy[3], and Vikas Chaudhary[4]

[1] Department of Electrical and Computer Engineering, Maddawalabu University, Bale Robe, Ethiopia
rathi.tarun@gmail.com
[2] Raj Kumar Goel Institute of Technology, Ghaziabad, India
rpmaheshwari@hotmail.com
[3] Department of Electrical Engineering, Indian Institute of Technology Roorkee, Roorkee, India
tripathy.manoj@gmail.com
[4] Department of Computer Science and Engineering, KIET Ghaziabad, Ghaziabad, India
Vikas.chaudhary@kiet.edu

Abstract. This paper presents a comparison of extracted watermark image quality and robustness between DCT and SVD based digital watermarking techniques. Here two transform domain DCT and SVD based watermarking algorithms are implemented. For better comparison purpose original host image and watermark image are kept same in both algorithms. Before extracting watermark, different image processing attacks and noise are inserted in watermarked image then DCT and SVD based watermark extraction are performed to check PSNR and robustness against those image processing attacks and noise. Obtained experimental results show that between these two algorithms, robustness, and quality of extracted watermark images are better in SVD based watermarking method.

Keywords: Discrete cosine transform (DCT) · Singular value decomposition (SVD) · Pseudo random noise sequence (PN sequence) · Peak signal to noise ratio (PSNR) · Normalized correlation (NC)

1 Introduction

With the rapid growth of multimedia and internet technology the data communication has been very fast [1]. But these also create the problems of data copyright protection and data security. In order to overcome these issues digital image watermarking is used [2]. Earlier spatial domain based watermarking algorithms were having the problems like quality, security and robustness of extracted watermark. The new transform based

F. A. Zimale et al. (Eds.): ICAST 2018, LNICST 274, pp. 315–321, 2019.
https://doi.org/10.1007/978-3-030-15357-1_26

algorithms are being introduced to reduce the impact of these problems. The transform domain watermarking method is much better than the spatial domain algorithms with respect to different features of watermarking algorithm. In these techniques the message bits are inserted after transforming the host image by using transform based method like discrete cosine transform (DCT), and singular value decomposing (SVD) based algorithm. It is very difficult to detect the hidden contents from the watermarked image in transform based algorithm. If the coefficients of large values are taken to embed the message bits than extracted watermark image will be more robust [3].

There are many features of digital image watermarking like security, capacity, imperceptibility, robustness, etc. but there is a trade-off between three features imperceptibility capacity, and robustness. In recent years more work has been done to find the best tradeoff between the imperceptibility, capacity and robustness [4].

2 Evaluation Parameters

PSNR is peak signal to noise ratio, which represents the quality of the watermark image. Mean square error (MSE) is to be evaluated to compute the PSNR between extracted and original watermark image [5]. PSNR and mean square error (MSE) can be expressed as follows.

$$PSNR = 10 \times \log(\frac{255^2}{MSE}) \tag{1}$$

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{N} \sum_{i=2}^{M} [I(i,j) - I^*(i,j)]^2 \tag{2}$$

Where I(i, j) and I*(i, j) respectively are the pixel values of the original images and watermarked images. Image matrix size is denoted by M × N [6]. Robustness is the ability of the watermark image to preserve the information even after different noise and malicious attacks. This is measured by the normalized correlation (NC) used for similarity measurement between the original watermark and extracted watermark. Normalized correlation (NC) can be expressed as follows.

$$NC = \frac{\sum_i w_i w_i^*}{\sum_i w_i^2} \tag{3}$$

Here w_i is the original watermark and w_i^* is the extracted watermark [7]. Bigger the NC value means better similarity between two images.

3 Transform Domain Algorithm

3.1 DCT Based Digital Image Watermarking

This is a transform based algorithm which is more robust than spatial domain method. A discrete cosine transform (DCT) changes the host image in terms of a sum of cosine function oscillating at different frequencies [8]. In blind DCT watermarking the host image is segmented into blocks of same size [9]. DCT based algorithm transforms every block into its transformed coefficients. For single image embedding two coefficients are modified. For better result, we choose mid frequencies because higher frequency coefficients are highly sensitive to different image processing attacks and low frequency coefficients are having the feature of visual effect so mid frequency coefficients are selected for inserting the watermark message which improves the robustness of extracted watermark. Selected particular coefficients work as secret key at extracting algorithm [10]. Without knowing this watermark extraction can not be done. After changing coefficients the inverse DCT is taken and combining all blocks to produce the watermarked image.

3.2 SVD Based Digital Image Watermarking

Singular value decomposition is an algorithm to analyze the image matrix. It converts image in to three different metrics [11]. It is a kind of orthogonal transform used for matrix analysis. The SVD of image Im can be described as

$$\mathrm{Im} = \mathrm{HSVT} \tag{4}$$

$$\mathrm{Im} = \mathrm{I_m} = [\,h1 \quad h2 \quad . \quad . \quad . \quad hN\,] \begin{bmatrix} s1 & & & & & \\ & s2 & & & & \\ & & . & & & \\ & & & . & & \\ & & & & . & \\ & & & & & sN \end{bmatrix} \begin{bmatrix} v1 \\ v2 \\ . \\ . \\ . \\ \mathrm{vN} \end{bmatrix}^T \tag{5}$$

Im is the image matrix. H and V are two M × 1 and 1 × N unitary orthogonal matrices, and S is an N × N diagonal matrix [12]. Where the horizontal detail component of image Im is represented by H matrix and vertical detail component of the image Im is represented by V. Both H and V are orthogonal matrices and S is a singular matrix which consists of singular values. Singular values in S matrix are arranged diagonally and in decreasing order. The important feature of SVD is stability, which means small changes in the singular values do not affect the watermark image [13]. This makes the SVD algorithm more robust than other transform based algorithm. After dividing the host image into blocks, each block of host image is transformed using the SVD based algorithm. Singular values of diagonal matrix are modified according to the message bits. Two pseudo random sequences for two binary digits '1' and '0' are added to singular values with a gain factor. After changing singular values we take the inverse process of the SVD to produce a watermarked image. At the extraction algorithm correlation between stored singular value and changed singular values are found. Using this, message bits are recovered, and then reshaped into the watermark image.

4 Experimental Results

To compare both algorithms (discussed above) we extract the watermark from the noisy/attacked watermarked image. For this purpose different noise like Salt and Pepper, Gaussian, Poisson, Speckle, Median filter noise and different geometrical attacks like image rotation and cropping are inserted in the watermarked image before extraction then with the help of DCT and SVD extraction process watermark is extracted. Values of PSNR and normalized correlation of each extracted watermark are measured in DCT and SVD based algorithms and written on watermark images which

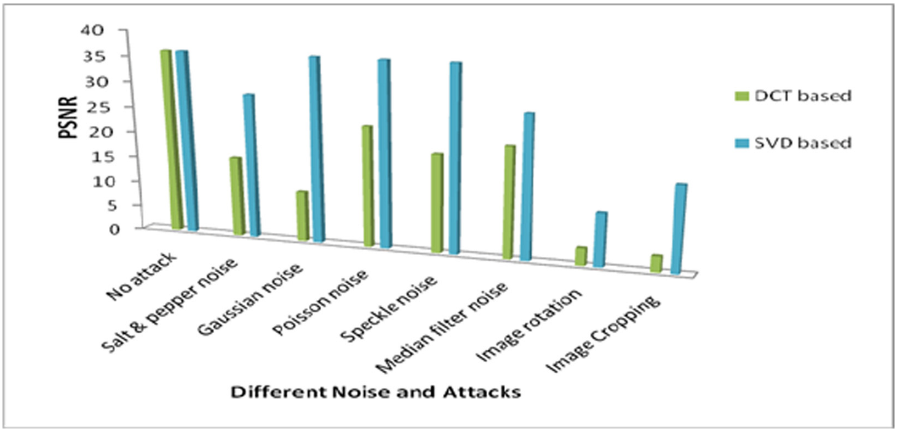


Fig. 1. PSNR of watermark images with respect of different attacks

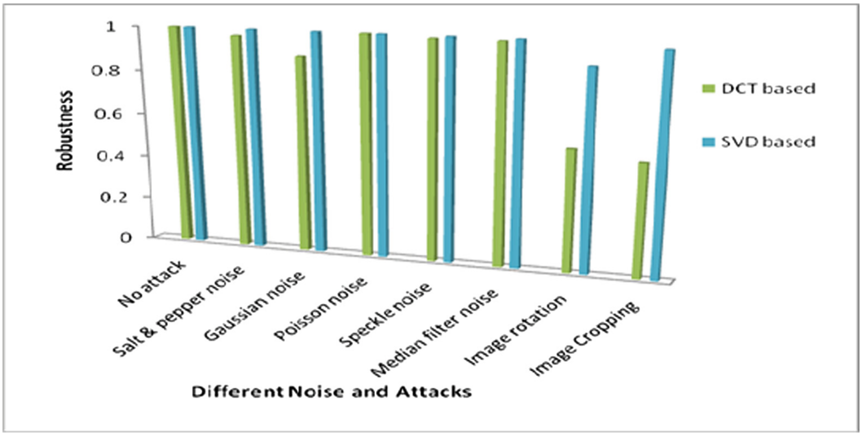
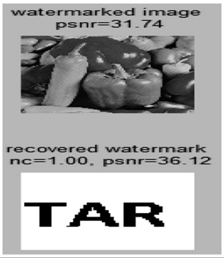
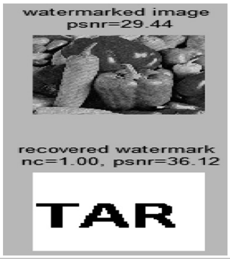
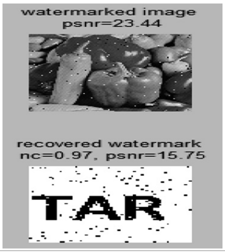
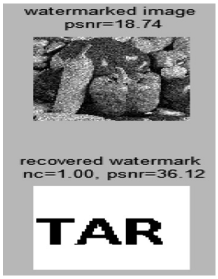
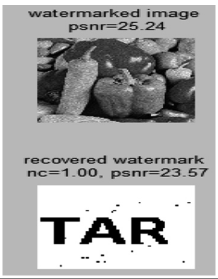
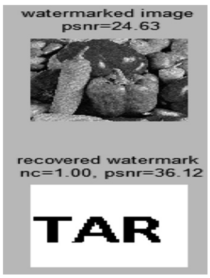


Fig. 2. Robustness of watermark images with respect of different attacks

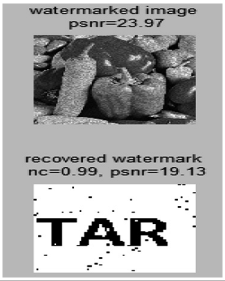
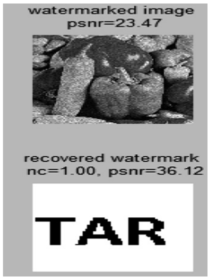
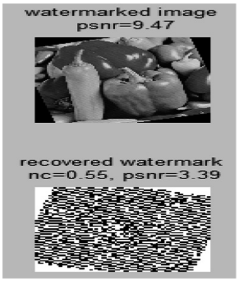
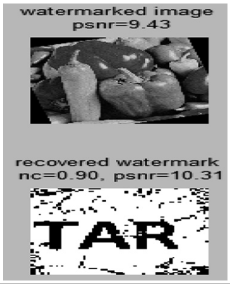
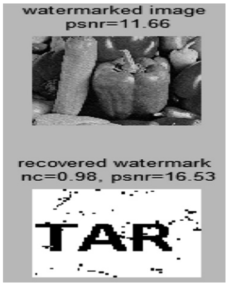
are shown in Table 1. In two watermarking algorithm, variation in PSNR and robustness against different noise and attacks are shown by the chart in Figs. 1 and 2 respectively where it is clearly visible that extracted watermark image from the SVD based algorithm is of higher PSNR and better robustness then the DCT based algorithm.

Table 1. Comparison of extracted watermark image

SN	Type of noise/attack	DCT based watermarking	SVD based watermarking
1.	No attack		
2.	Salt & Pepper attack		
3.	Gaussian noise		
4.	Poisson noise		

(*continued*)

Table 1. (*continued*)

SN	Type of noise/attack	DCT based watermarking	SVD based watermarking
5.	Speckle noise		
6.	Median filter noise		
7.	Image rotation		
8.	Image cropping		

5 Conclusions

In this paper, DCT and SVD based digital image watermarking algorithms are implemented using MATLAB. Host and watermark image are kept same for comparison purpose. These algorithms are examined after inserting the different types of noise and attacks in watermarked image at extraction algorithm. SVD based algorithm extracts more robust and better quality watermark image than DCT based algorithm which can be seen through charts in Figs. 1 and 2 respectively. In case of geometric attacks like image cropping and rotation, SVD algorithm is also able to extract watermark image unlike DCT algorithms as shown in Table 1. This is because of the stability, flipping and transpose etc. properties of SVD. A hybrid algorithm using SVD and other transform based watermarking algorithm can also be used to extract much better watermark image.

References

1. Potdar, V.M., Han, S., Chang, E.: A survey of digital image watermarking techniques. In: Proceedings of the IEEE International Conference on Industrial Informatics, pp. 709–716 (2005)
2. Lu, Z.-M., Zheng, H.-Y., Huang, J.-W.: A digital watermarking scheme based on DCT and SVD. In: Proceeding of IIHMSP 2007 Conference, Kaohsiung, pp. 241–244 (2007)
3. Xiao, M.M., Yu, L.X., Liu, C.J.: A comparative research of robustness for image watermarking. In: IEEE International Conference on Computer Science and Software Engineering, pp. 700–703 (2008)
4. Lee, G.-J., Yoon, E.-J., Yoo, K.-Y.: A new LSB based digital watermarking scheme with random mapping function. In: IEEE International Conference on Ubiquitous Multimedia Computing, pp. 130–134 (2008)
5. Na, W., Yunjin, W., Xia, L.: A novel robust watermarking algorithm based on DWT and DCT. In: International Conference on Computational Intelligence and Security, vol. 1, pp. 437–441 (2009)
6. Himanshu, H., Rawat, S., Raman, B., Bhatnagar, G.: DCT and SVD based new watermarking scheme. In: 3rd International Conference on Emerging Trends in Engineering and Technology, pp. 146–151 (2010)
7. Rafigh, M., Moghaddam, M.E.: A robust evolutionary based digital image watermarking technique in DCT domain. In: Proceedings of IEEE Seventh International Conference on Computer Graphics, Imaging and Visualization, pp. 105–109 (2010)
8. Dehkordi, A.B., Esfahani, S.N., Avanaki, N.: Robust LSB watermarking optimized for local structural similarity. In: 19th Iranian IEEE International Conference on Electrical Engineering (ICEE), pp. 1–6 (2011)
9. Run, R.-S., Horng, S.-J., Lai, J.-L., Kao, T.-W., Chen, R.-J.: An improved SVD-based watermarking technique for copyright protection. Expert Syst. Appl. **39**(1), 673–689 (2012)
10. Parashar, P., Singh, R.K.: A survey : digital image watermarking. In: 3rd IEEE International Conference on Industrial Informatics Techniques, pp. 111–124 (2014)
11. Furqan, A., Kumar, M.: Study and analysis of robust DWT-SVD domain based digital image watermarking technique using MATLAB. In: IEEE International Conference on Computational Intelligence & Communication Technology, pp. 638–644 (2015)
12. Bhuyan, T., Srivastava, V.K., Thakkar, F.: Shuffled SVD based robust and secure digital image watermarking. In: International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT, pp. 1229–1233 (2016)
13. Nana, Z.: Watermarking algorithm of spatial domain image based on SVD. In: ICALIP International Conference on Audio, Language and Image Processing – Proceedings, no. 4, pp. 361–365 (2017)