A Robust Data Hiding Scheme Using Singular Value Decomposition and Wavelet Transform

Sudhir Singh(✉) and Buddha Singh

School of Computer and Systems Sciences, Jawaharlal Nehru University Delhi, Delhi, India
sidsingh73@gmail.com

Abstract. Due to latest development in computing and communication technologies, there are various kinds of digital contents on the internet in terms of audio, video, and images. Also, there are many freely available softwares that can modify a given digital object. These softwares have created a challenge for the owners of the original contents. Digital image watermarking secret data hiding may be helpful in addressing this problem digital contents. This chapter discusses a data hiding scheme by using the singular value decomposition (SVD) and digital wavelet transform (DWT). Our scheme performs better than the recent methods for the quality and the extracted watermark image.

Keywords: Data hiding · DWT · SVD · Frequency band · PSNR

1 Introduction

Latest developments in computational and communication technologies have made multimedia contents over the internet quite rich and easily accessible [1]. These contents can be easily copied and distributed, reducing the control of their ownership by the freely available softwares. To protect this ownership of a digital content, secret data hiding or digital watermarking schemes can be useful. A watermark may be considered as a secret data/code, which consists of the identification information for the creator/owner of the original contents that can be used to prove the ownership of contents, if required. A watermark must be unobtrusive, that is, it should not degrade the visual quality of an image in a perceptible manner, and should be robust, that is, it should be resistant to the intentional as well as unintentional attacks, specifically geometric distortions, collusion attacks, and compression distortion. Watermarking can be blind and non-blind. The hybrid form of these two is semi-blind watermarking in which some extra information is to be provided to help a detector in the detection process. The watermark can be visible as well as invisible. An invisible watermark is an image that cannot be seen but can be detected algorithmically, whereas a visible watermark is a transparent picture that is placed on the cover image. In this chapter, we go over a method for watermarking that is both invisible and semi-blind. Typically, a watermarking technique is used in the transform (frequency) and spatial domains. Some of the bits of the pre-specified pixels are adjusted in the spatial domain-based approaches, such as the last two bits of high pixel values.

R. N. Shaw et al. (Eds.): ICACIS 2022, CCIS 1749, pp. 81–88, 2023.
https://doi.org/10.1007/978-3-031-25088-0_6

The spatial domain techniques are simpler to use and easier to construct, but they have less capacity and are more vulnerable to the attacks. In [2, 3] some of the watermarking techniques in spatial domain are discussed. For transform domain, the unitary transforms are applied on the blocks of the intended cover image and the pre-specified frequency coefficients are modified. A watermarking technique is mainly assessed based on the perceptibility, robustness, and security parameters [4, 5]. Perceptibility signifies the visibility and invisibility of the watermark. Robustness refers to the strength of the technique, and the security to resist various attacks. Another important parameter is time needed for embedding the watermark and its detection process. In this chapter, we present a 2-D DWT and SVD-based method for digitally watermarking images. The matrix is essentially divided into 4 bands by the DWT: LL, LH, HL, and HH. The LL band maintains the most of the image's information, while the HH band maintains the most of its details. In-between details about the image are contained in the final two bands. A matrix of dimension (m x n) is factorised into three matrices (U, S, and V) using the singular value decomposition method. U is a matrix of dimension (m x r), S is of dimension (r x r), and V is of dimension (r x n), where r is the rank of the original matrix. S is a diagonal matrix, U and V are the unitary transform matrices. Compared to the approaches [2, 6], our scheme performs better.

2 Related Work

With its first academic conference held in the year 1996, digital watermarking is considered relatively a young research area. Since then a large number of watermarking techniques have been proposed. Recently, SVD based techniques [1, 2] have become popular. The basic reason for using SVD is that the diagonal matrix obtained after decomposition of the original matrix governs different luminous levels. The modification done on this diagonal matrix has very little effect on the perceptibility of the image. Based on the combination of DCT, SVD, and CNT Tian [5] has proposed a method. In this, the host image is created using a one level CNT and the embedding process uses its low frequency coefficients. It offers imperceptibility 42.77 dB and strengthens resistance to numerous threats. Zhang et al. [2] have discussed a data hiding scheme on the basis of SVD by exploring horizontal variation in the image intensity, that is U matrix, for hiding the watermark. It modifies the absolute variation of two consecutive rows of U matrix to preserve positive relationships between its rows even after performing JPEG encoding. But, this method does not provide error-free watermark extraction. Another issue with this method is complex block selection.

Salehnia et.al. [6] proposed an algorithm by using SVD and lifting wavelet transform (LWT). The LWT gives 4 sub-images, namely LL, LH, HL, HH, when applied on an image. Three LH, HL, and HH sub-bands have lower resolution than the LL subband. This method solves both the issues of method [2]. The first issue is addressed by considering the diagonal matrix using LWT and Three Module Redundancy (TMR) technique. The second one is addressed by considering the complex blocks on the basis of the number of edges. But this algorithm has a disadvantage that it does not work correctly when all the edges are confined to one particular area of the image. Therefore, there is a need to resolve this problem. Our scheme resolves this issue by using the watermark made of a binary image and embedding it in the high-high frequency region of the DWT coefficients. Our proposed method is highly robust and has better perceptibility as compared to the methods discussed in [2, 6]. The proposed method is introduced in Sect. 3 and Sect. 4 provides its experimental results. The chapter is concluded in Sect. 5.

3 Proposed Scheme

Before introducing our proposed method, we briefly discuss SVD and DWT as these are the basic concepts used to develop our proposed scheme.

3.1 Singular Value Decomposition (SVD)

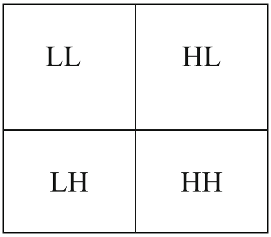
The singular value decomposition (SVD) factorizes a rectangular matrix, which can be real or complex into tree matrices. Consider a matrix X of dimension *mxn*. On applying SVD on X, we get three matrices as shown below.

$$X = USV^T \tag{1}$$

The matrix U refers to horizontal variation in intensity in X, S is a diagonal matrix that contains singular values of X, and V refers to vertical variation in intensity in X.

3.2 Discrete Wavelet Transform

The discrete wavelet transform (DWT) splits a 1-dim signal into two parts: low and high frequency components. The low frequency component consists of maximum information of the signal, whereas the detailed information such as edges is confined to the high frequency component. On applying DWT on an image (2-dim signal), we get for components, denoted as low-low (LL) frequency band, low-high (LH) frequency band, high-low (HL) frequency band, and high-high (HH) frequency band as shown in Fig. 1. Generally LL sub-image is used to hide the secret data.



LL	HL
LH	HH

Fig. 1. Various bands into which image is decomposed.

We now discuss our proposed scheme. We first apply the DWT to the cover image and then apply SVD to LL sub-image. We use diagonal matrix for hiding the secret data that is obtained by SVD from LL sub-image. For maintaining the perceptibility of the resultant image, we select the complex blocks of the LL sub-image for embedding. The algorithm for embedding the watermark in an image is given below.

1. *Load image to be watermarked (Fig. 2).*
2. *Take its discrete wavelet transformation.*
3. *Choose LL band to work upon.*
4. *Take a 32 × 32 block (for 512 × 512 image) watermark image and convert it into binary image.*
5. *Reshape binary image to 1x1024.*
6. *Group 256 × 256 pixels of LL matrix obtained, into 32 × 32 groups of 8 × 8 each.*
7. *On each 8 × 8 block, apply SVD and store S(1, 1) element/coefficients in an array (denoted by b(i)).*
8. *Store indices of min(b(i)) and max(b(i)) respectively as j and k and set jth and kth bit in 1 × 1024 (W) to either 0 or 1.*
9. *Group the intervals of b(i) within min and max values with 1024 intervals as max(b(i))-min(b(i))/1024.*
10. *Modify the values of S(1, 1) by adding 1/4 from lower bound if watermark bit is '1' and by subtracting 1/4 from upper bound if watermark bit is '0'.*
11. *Replace them in b(i) array and take SVD inverse with new SVD(1, 1) values to form the watermarked LL.*
12. *Take inverse dwt with this changed LL and previous HH, HL, LH to get the watermarked image.*

The algorithm for extracting the watermark from the resultant (watermarked) image is given below.

1. *Load watermarked image (Fig. 5).*
2. *Take its discrete wavelet transformation.*
3. *Choose LL band to work upon.*
4. *Since we have set jth (min value index) and kth (max value index) bits either 1 or 0, we know the deviation of the min and max values in original b(i) array.*
5. *Group 256 × 256 pixels of LL matrix obtained, into 32 × 32 groups of 8 × 8 each.*
6. *On each 8 × 8 block, apply SVD and store S(1, 1) element/coefficients in an array (denoted by b(i)).*
7. *Store the indices of min(b(i)) and max(b(i)) respectively as j and k and set jth and kth bit in 1 × 1024 (W) to either 0 or 1.*
8. *Group the intervals of b(i) within min and max value with 1024 intervals as max(b(i))-min(b(i))/1024.*
9. *The interval boundaries will be same as while embedding, so we can check which S(1, 1) or b(i) value has changed and thus we can obtain the watermark pattern.*
10. *Since we store the bit as 0 or 1 according to the shift observed in b(i) values.*
11. *After extracting the watermark and comparing with the original, the authenticity of image can be ascertained.*

Fig. 2. 512 × 512 Lena (host image)

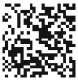


Fig. 3. Watermark image

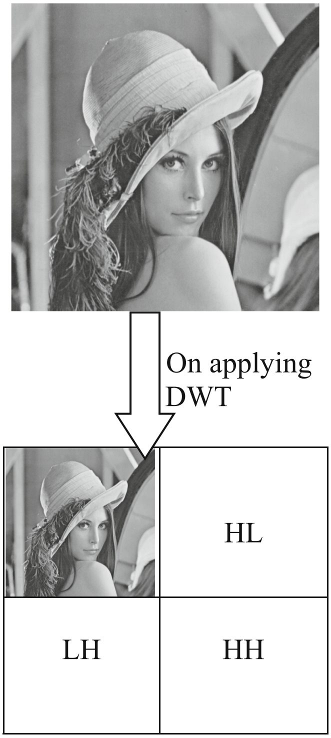


Fig. 4. Decomposition of the host image

Fig. 5. Watermarked image

4 Watermark Attacks

By conducting numerous tests, such as image attacks utilising the Lena Picture (512 × 512) as the host image—which is depicted in Fig. 2—we assess the effectiveness of our system. The watermark has a binary size of 24 × 24 and an additional two key data bits, as illustrated in Fig. 3. Figure 4 depicts the image's breakdown following the use of DWT, and Fig. 5 depicts the watermarked Lena image. The resilience of the watermark to attacks such as row-column blanking, row-column copying, rotation, low pass filtering, scaling, cropping, salt & pepper noise, and picture manipulation. With the exception of image tampering and JPEG2000 attacks, all attacks are conducted using MATLAB R2021a. The MORGAN JPEG2000 toolkit is used for the JPEG2000 attack, while PAINTBRUSH is used for picture tampering. A good PSNR of 53.36 dB is present in the watermarked image.

The watermarked image is rotated at various angles (10, 20, 30 degrees) up to which exactly the same watermark is detected with the correlation factor of 1, but the rotation attack shows great similarity. However, it maintains its strength at various angles except in the vicinity of 40 degrees. Using lossy JPEG compression the watermark image is compressed with various quality factors such as 30, 40, 60, and 100. The JPEG compression value ranges from 0 (best compression) to 100 (best quality). Our scheme stands outstanding even for high compression and has 0.9792 value for the quality factor of 30. The higher values of the quality factor show great level of similarity with the original watermark. Due to the extremely strong presence of watermark in the upper region of the image cropping attack does not show great results but for cropping in the lower region good results are obtained. A 3 × 3 mask with intensity values of 0.9 is considered for low pass filtering attack. Our scheme shows great resilience to the low pass filtering attack as can be seen in Table 1. In resizing, we first reduce the watermarked image by half in both the dimensions and then using the bicubic interpolation it is enlarged to the original size. The watermark extracted is exactly same to the embedded watermark. A certain number of rows and columns are eliminated in a row column blanking attack, including 10, 30, 40, 70, 100, 120, and 140 rows and columns. In a row-column copy attack, several rows and columns are copied to randomly chosen or relatively neighbouring locations, for example, 10th row is copied to 30th one, 40th to

70th, 100th to 120th and 140th to 160th. As can be seen from Table 1, the watermark extracted from the row column blanking and copying attacks has good similarity with the original watermark. The watermarked image is corrupted by salt & pepper noise with density of 0.001, 0.002, 0.003, and 0.004. The watermarks from the corrupted images are clearly visible, which justifies that our scheme is resilient to the noise attacks. Finally, the proposed scheme shows good results for bit plane removal and image tampering attacks. The NC (normalized cross-correlation) value helps to compare the robustness of the proposed scheme. Table 1 summarizes the performance parameters.

Table 1. Proposed scheme comparison and their performance

Parameters	Zhang et al.[2]	Salehnia et al. [6]	Proposed method
Image quality (in dB)	49.07	50.3453	53.3612
Type of attack	NC values		
Rotation (in degrees) (10, 20, 40, 60)	0.5333		1
	0.4988		1
	0.4712		0.02
	0.4856		0.9965
Low pass filtering 3 × 3 kernel	0.9386	0.9862	0.9896
Resizing 512-256-512	0.9538	0.8155	1
JPEG Compression (Quality factor) 30, 40, 60, 100	0.9295	0.9211	0.9792
	0.9793	0.9711	0.9965
	0.9986	0.9961	1.0000
	1.0000	1.0000	1.0000
JPEG2000 Compression (Quality factor) 5,10,30,50	0.3323	0.6502	1.0000
	0.2819	0.9953	1.0000
	0.8765	1.0000	1.0000
	0.8989	1.0000	1.0000
Salt & pepper Noise (Noise density) .1%,.2%,.3%,.4%	0.9923	0.9624	0.9896
	0.9566	0.9512	0.9757
	0.9255	0.9102	0.9515
	0.9148	0.9184	0.9202

(*continued*)

Table 1. (*continued*)

Parameters	Zhang et al.[2]	Salehnia et al. [6]	Proposed method
Bit plane removal 1st, 2nd and 3rd	0.9802	1.0000	1.0000
	0.9802	0.9009	0.1099
	0.4354	0.8076	0.1696
Image tampering	0.9353	0.9907	0.9688

5 Conclusion

In this chapter, we provide an SVD and DWT-based data hiding technique. It is strong and able to fend off numerous attacks. Peak-to-signal ratio, which is 53.3612, and perceptibility are both good indicators of the image's quality. Additionally, it is immune to JPEG compression, scaling, row column blanking, rotation, cropping, low pass filtering, row column copying, bit plane removal, salt and pepper noise, and tampering. The linked techniques are better for specific parameters when it comes to rotation and cropping attack. The proposed approach outperforms the existing algorithms used for comparison in all other attacks.

References

1. Altay, ŞY., Ulutaş, G.: Self-adaptive step firefly algorithm based robust watermarking method in DWTSVD domain. Multimedia Tools Appl. **80**, 23457–23484 (2021)
2. Zhang, H., Wang, C., Zhou, X.: A robust image watermarking scheme based on SVD in the spatial domain. Future Internet **9**, 45 (2017). https://doi.org/10.3390/fi9030045
3. Bartolini, F., Tefas, A., Barni, M., Pitas, I.: Image authentication techniques for surveillance applications. Proc. IEEE **89**(10), 1403–1418 (2001). https://doi.org/10.1109/5.959338
4. Kim, W.-H., Nam, S.-H., Kang, J.-H., Lee, H.-K.: Robust watermarking in curvelet domain for preserving cleanness of high-quality images. Multimedia Tools Appl. **78**(12), 16887–16906 (2019). https://doi.org/10.1007/s11042-018-6879-3
5. Tian, C., Wen, R.H., Zou, W.P., Gong, L.H.: Robust and blind watermarking algorithm based on DCT and SVD in the contourlet domain. Multimedia Tools Appl. **79**, 7515–7541 (2020). https://doi.org/10.1007/s11042-019-08530-z
6. Salehnia, T., Fathi, A.: Fault tolerance in LWT-SVD based image watermarking systems using three module redundancy technique. Expert Syst. Appl. **179** (2021). https://doi.org/10.1016/j.eswa.2021.115058