

A Robust Semi-Blind Image Watermarking Technique

Iti Saxena¹, Praful Saxena²

¹(Computer Science Department, Shri Venkateshwara University, Gajraula, India)

²(Computer Science Department, Asst. Prof. KIMT, Moradabad, India)

Abstract: Day by day the increase in networked multimedia systems has created an urgent need for copyright enforcement technologies that can protect copyright ownership of multimedia contents. Digital Image Watermarking is one such technology that has been developed to protect digital images from illegal manipulations. Watermarking is used to protect the ownership of content service provider is a crucial area of research. Robustness against geometric distortions is crucial issue in watermarking. In this paper, a new SVD-DWT semi-blind composite image watermarking algorithm that is robust against various attacks is presented. I used DWT and IDWT transform to obtain four different frequency images. Watermark is embedded in high-frequency band by SVD. The imperceptibility and robustness are the properties that are evaluated for the proposed scheme. Image is evaluated using peak-signal-to-noise ratio (PSNR) which is used to evaluate the difference between original image and the watermarked image.

Keywords: Copyright protection, Discrete wavelet transform (DWT), Multi frequency image, Singular value decomposition (SVD)

I. Introduction

The copyright of digital images in the internet can be easily violated by cropping and graphical modifications. Some parts of an image can be cropped and applied to other images without permission. Commercial potential of offering multimedia resources through Internet by entertainment industry has also created a need to protect intellectual property rights of copy-righted material.

The Watermarking is the process of embedding data into a multimedia element such as image, audio or video[1]. A digital Watermarking is a process to embed certain special and confidential information (watermark) directly into digital media which makes the information become unitary with the original data to achieve covert transmission, storage, multimedia authentication, digital copyright protection[2]. The process of digital watermarking involves the modification of the original multimedia data to embed a watermark containing key information such as authentication or copyright codes[3]. A watermarking algorithm consists of the watermark structure, an embedding algorithm and an extraction or a detection algorithm. Suppose that a watermark is defined as W , D is the host data, and K is the security key. In watermarking, an embedding function $e(\cdot)$ takes the watermark W , the host data D , and the security K , as the input parameters, and outputs the watermarked data D' [4]:

$$D' = e(D, W, K) \quad (1)$$

The watermark is considered to be robust if it is embedded in a way such that the watermark can remain unaffected even if the watermarked data D' go through different attacks. The watermark detection procedure is stated as follows:

$$W' = d(D', K, \dots), \quad (2)$$

Where $d(\cdot)$ is the detection function. D and W are the optional inputs for the detection function. An important criterion for classifying watermarking schemes is the type of information needed by the detector:

- Non-blind schemes: Both the original image and the secret key(s) for watermark embedding.
- Semi-blind schemes: The secret key(s) and the watermark bit sequence.
- Blind schemes: Only the secret key(s).

II. Background And Theory

1. Singular Value Decomposition (SVD)

Every real matrix A can be decomposed into a product of 3 matrices $A = U\Sigma V^T$, where U and V are orthogonal matrices,

$$U^T U = I, V^T V = I \quad \text{and} \quad (3)$$

$$\Sigma = \text{diag}(\lambda_1, \lambda_2 \dots) \quad (4)$$

The diagonal entries of Σ are called the singular values of A , the columns of U are called the left singular vectors of A , and the columns of V are called the right singular vectors of A . This decomposition is known as the Singular Value Decomposition (SVD) of A , and can be written as

$$A = \lambda_1 U_1 V_1^T + \lambda_2 U_2 V_2^T + \dots + \lambda_r U_r V_r^T \quad (5)$$

where r is the rank of matrix A .

Generally a real matrix A has many SVs, some of which are very small, and the number of SVs which are non-zero equals the rank of matrix A [5]. SVD has many good mathematical characteristics. Using SVD in digital image processing has some advantages [6,7].

- The size of the matrices from SVD transformation is not fixed and can be a square or a rectangle.
- The SVs (Singular Values) of an image have very good stability, i.e. when a small perturbation is added to an image, its SVs do not vary rapidly.
- SVs represent algebraic image properties which are intrinsic and not visual.
- Each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image [2].

2. Discrete Wavelet Transform (DWT)

Discrete Wavelet transform (DWT) is a mathematical tool for hierarchically decomposing an image. It is useful for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides both frequency and spatial description of an image. Unlike conventional Fourier transform, temporal information is retained in this transformation process. Wavelets are created by translations and dilations of a fixed function called mother wavelet. This section analyses suitability of DWT for image watermarking and gives advantages of using DWT as against other transforms. Fig. 1 shows DWT decomposition of an image using three level pyramid.

LL3	HL3	HL2	
LH3	HH3		
LH2		HH2	HL1
LH1			HH1

Fig 3.1 Pyramid after three decomposition steps

- Wavelet Transform is computationally efficient and can be implemented by using simple filter convolution.
- With multi-resolution analysis, image can be represented at more than one resolution level. Wavelets allow image to be described in terms of coarse overall shape and details ranging from broad to narrow.
- Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, HL).
- The larger the magnitude of wavelet coefficient, the more significant it is.
- Watermark detection at lower resolutions is computationally effective because at every successive resolution level, less no. of frequency bands are involved.
- High resolution sub bands help to easily locate edge and textures patterns in an image.

III. Literature Review

Ganic and Eskicioglu [3] presented DWT-SVD based digital image watermarking scheme. This method is robust against different attacks because of using all bands in embedding process, but it is a non-blind method and the transparency of the watermarked image is not good. Kapre and Joshi [8] proposed same DWT-SVD scheme but embeds data in high frequency band which is much more robust to geometric attack. The approach they too used was a non blind scheme.

IV. Proposed Method

4.1 Watermark Embedding

- Using DWT, decompose the original image I into 4 subbands: LL, HL, LH and HH
- Apply IDWT to HH and get high frequency image I^h .
- Apply SVD to high frequency image I^h

$$I^h = U^h S^h V^h$$

- Apply SVD to visual watermark W :

$$W = U^w S^w V^w$$

- Modify $S^{*h} : S^h = \alpha S^w$ where α is scaling factor.

- Obtain the modified high frequency image I^{*h}

$$I^{*h} = U^h S^{*h} V^h$$

- Apply DWT to I^{*h} and get modified HH^* :

$$HH^* = DWT(I^{*h})$$

- Using HH^*, HL, LH and LH apply IDWT to obtain the watermarked image I^* .

4.2 Watermark Extraction

- Using DWT, decompose the watermarked image I^* into 4 subbands: LL, HL, LH , and HH^*

- Apply IDWT to HH^* and get modified high frequency image I^{*h}

- Apply SVD to I^{*h} :

$$I^{*h} = U^{*h} S^{*h} V^{*h}$$

- Apply SVD to watermark W :

$$W = U^w S^w V^w$$

- Extract the singular values of watermark:

$$S^{*w} = S^{*h} / \alpha$$

- Where S^{*h} are the singulars of origin image.

- Recover the watermark from HH band:

$$\hat{W} = U^w S^{*w} V^w$$

V. Performance Evaluation

5.1 PSNR

PSNR evaluates the difference between original image and the attacked watermarked image.

$$PSNR = 20 * \log_{10} (255 / \sqrt{MSE}) \quad (6)$$

Mean absolute error (mse) measures the mean of the square of the original watermark and the extracted watermark from the attacked image. PSNR lies between 20db to 50db. This is used in used in Pattern reorganization and image processing methods. It is used to compare the two images taken at different times.

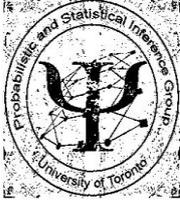
5.2 Correlation Coefficient

The correlation coefficient r has the value, $r = 1$, if the two images are absolutely identical, $r = 0$ if the two images are completely uncorrelated, $r = -1$ if they are anti-correlated.

VI. Experiment

The proposed watermarking scheme was tested using ordinarily image processing: Gaussian noise, rotation, median filter, histogram equalization and salt & pepper. The correlated coefficient of the original watermark, psnr and extracted watermark is shown in the Table 1. In this we observe that this scheme is robust against various attacks

TABLE 7.1: ATTACKS, EXTRACTED WATERMARK, PSNR AND CORRELATED COEFFICIENT OF THE ORIGINAL WATERMARK

Attacks	Extracted Watermark	PSNR	Correlated Coefficient	
Rotation			34.41	0.7761
Median Filter			36.21	0.8215
Gaussian Noise			33.53	0.7922
Histogram Equalization			30.45	0.7248
Salt & Pepper			35.77	0.7966

VII. Conclusion

- In our scheme, the most difference from traditional scheme is that the watermark is embedded in high frequency. It has good performance in a variety of image processing.
- SVD decomposition belongs to spatial domain transform and has robustness to geometrical attack. For considering this, we use DWT and IDWT transformation to obtain the high frequency image. Accordingly the scheme has robustness to geometrical attack.
- We notice there are three frequency image (low frequency image, middle-low frequency image, middle-high frequency image) are not used. Different watermarks can be embedded in them.

- The PSNR value is between 20db-50db which shows that the extracted watermark from the attacked image is closer to the original watermark.

References

- [1]. Dazhi Zhang, Wu, Sun and Huang, "A New Robust Watermarking Algorithm Based on DWT" Image and Signal processing 2009, CISP'09
- [2]. Rowayda A. Sadek, "Blind Synthesis Attack on SVD Based watermarking Technique", Computational Intelligence for modeling Control :2008 pp 140-145.
- [3]. E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, September 20-21, 2004.
- [4]. Zheng, D., Liu, Y., Zhao, J., and El Saddik, A. "A survey of RST invariant image watermarking algorithms", ACM Computing Surveys, Volume 39, No. 2, Article 5, June 2007.
- [5]. H. C. Andrews and C. L. Patterson, "Singular value decomposition (SVD) image coding," IEEE Transactions on Communication, vol. COM-24, pp. 425-432, Apr. 1976.
- [6]. Zude Zhou, Bing Tang and Xinhua Liu, "A Block-SVD Based Image Watermarking Method", Proceedings of the 6th World Congress on Intelligent Control and Automation, June 21 - 23, 2006, Dalian, China
- [7]. Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin, "SVD-based digital image watermarking scheme", Pattern Recognition Letters, Volume 26, Issue 10, July 2005, pp. 1577-1586
- [8]. Kapre and Joshi, "Robust Image Watermarking based on Singular Value Decomposition and Discrete Wavelet Transform", Nanded ©2010 IEEE