SVD based Image Watermarking Scheme

Deepa Mathew K
Karunya University
Coimbatore, India

ABSTRACT
To embed watermark is a way to increase the robustness of the image. In this paper the singular value decomposition (SVD) based image watermarking scheme is proposed. The output result of SVD is more secure and robust. In the proposed scheme D and U components are used for embedding watermark. Unlike other transforms which uses fixed orthogonal bases, SVD uses non fixed orthogonal bases. The result of SVD gives good accuracy, good robustness and good imperceptibility in resolving rightful ownership of watermarked image. With the increased use of SVD watermarking scheme, the watermarking technology in the transform domain has been greatly developed.

Keywords
Watermark, Singular value decomposition (SVD), extracting, embedding

1. INTRODUCTION
From the dawn of civilization, to the highly networked societies that we live in today communication has always been an integral part of our existence. Methods of communication today include radio communication, telephonic communication, network communication and mobile communication. All these methods and means of communication have played an important role in our lives, but in the past few years, network communication, especially over internet has emerged as one of the most powerful communication with an over whelming impact in our lives. With the advance in the technology, illegal operations in digital media have become easy. Therefore, the copy right protection has become an important issue. One of the solutions for this problem is the embedding of digital watermark into the data.

Watermarking is the process of embedding a watermark into an object. This object may be audio, video or image. To get more effective output, the water should be perceptually invisible, difficult to remove without seriously affecting the image quality and should robustly resist to image distortions caused by attacks such as common image processing operations and lossy image compression.[1]. Several watermarking techniques have been proposed. These techniques can be classified into two: spatial domain techniques and frequency domain techniques. In spatial domain technique which embed the data directly by modifying the pixel values of the original image. In frequency domain technique which embeds the data by modulating the coefficients of a properly chosen transform [2, 3].

Watermarking techniques covers a wide area. Many other techniques also proposed. Example cryptography, security through quantization [4,5],discrete cosine transform[6,7,8].A new method of watermark detecting is proposed in [9]. In this a Gaussian distribution is assumed in DCT and DWT domains. Most commonly used methods of watermarking are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT). These transform domain technique always give more robust output [10].
SVD and DCT based watermarking scheme is explained in[11]. SVD is a powerful numerical analysis tool for matrices [12] which give minimum least square truncation error. This is because the total potential degrees of freedom of three matrices are equal to the input host image [13]. In [14] also explaining about SVD based image watermarking scheme, which give secure and robust owner identification. The main properties of SVD image processing are i. The singular values of an image have good stability ii. Singular values represent intrinsic algebraic image properties.
In this paper, we propose an improved SVD based image watermarking scheme. Unlike other transforms which uses fixed orthogonal bases, SVD uses non fixed orthogonal bases. The result of SVD gives good accuracy, good robustness and good imperceptibility in resolving rightful ownership of watermarked image.

2. THE PROPOSED WATERMARKING SCHEME
SVD is one of the effective tool to analysis the matrices. While using the SVD transformation a matrix is decomposed into three matrices U, D, V. U and V are the unitary matrices and D is a diagonal matrix. There are two steps in the proposed watermarking scheme. The first step is watermark embedding procedure and the next step is watermark extracting procedure.

2.1 The Watermark Embedding Procedure
In the proposed watermarking scheme the input image is gray scale.

Step1: Partition the image into blocks of n×n pixels

Step2: Apply SVD transformation to each partitioned block

Step3: Calculate the number of non-zero co-efficient in the D component of each block. This is calculated to determine the complexity of the block.

Step4: Select greater complexity blocks using PRNG [pseudo random number generator] and also using the feature of D component.

Step5: For each selected greater complexity block, in the first column of U, magnitude difference between the neighboring coefficients is calculated.
Step6: First, if the magnitude difference matches the embedding watermark (e.g. positive relationship matching a bit value of 1 or negative relationship matching a bit value of 0), the coefficients are retained. Second, if the magnitude difference does not match the embedding watermark, the coefficient must be modified.
Step7: To retain the image quality and provide a stronger robustness of a watermarking scheme, the difference value is first checked to be above certain threshold.

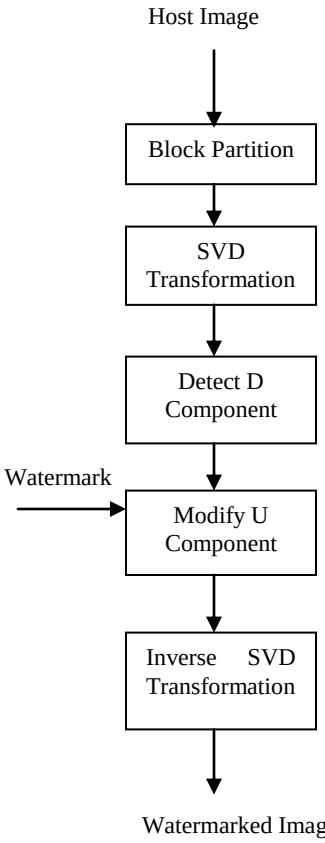

Fig.1 The watermark embedding procedure

If there is only less modification in the U component means the image quality is higher, but the resistance is weaker. But if the more modification in the U component implies the less quality image and it gives more robust output.

2.2 The watermark extracting procedure

The watermark extracting procedure is similar to the watermark embedding procedure.

Step1: Block partitioned the watermarked image

Step2: Apply SVD transformation to these block partitioned pixels

Step3: Calculate the number of non-zero co-efficient in the D component of each block. This is calculated to determine the complexity of the block.

Step4: Using the feature of D component and PRNG, the relationship of U component is calculated

Step5: If a positive relationship is detected, the extracted watermark is assigned a bit value of 1. Otherwise, the extracted watermark is given a bit value of 0.

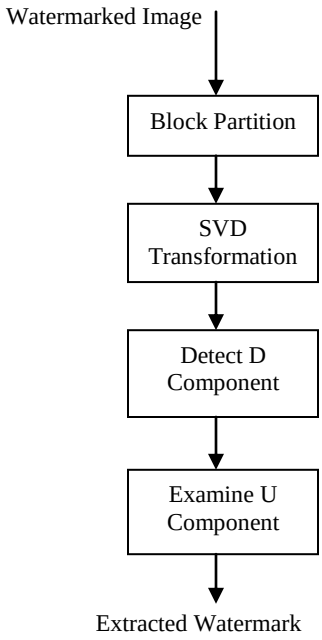

Fig. 2 The Watermark extracting procedure

3. EXPERIMENTAL RESULTS

A set of gray scale images of size 512×512 are chosen as input images. Here we are using Barbara, Lena and Liftingbody images as input host image. 32x32 jpeg image is used as a watermark.

First the images are partitioned into 8x8 pixels. Then SVD transformation is applied to each block partitioned image. Number of non zero coefficients of D components is calculated. Also the greater complexity block also calculated using PRNG. The magnitude difference is calculated in U component and it is modified according to the watermark added. The peak signals to noise ratio (PSNR) between the input and output image is calculated and it is more than 45dB. Therefore the proposed watermarking scheme will cause only a slight distortion in the image. The host image, watermarked image, the watermark embedded and the watermark extracted is shown in figure.3, 4, 5&6.

(a)Barbara

(b)Lena

(c)Liftingbody

Fig.3 The host images (a) Barbara (b) Lena (c) Liftingbody

Fig.4 Watermark added to host image

(a)Watermarked Barbara

(b)Watermarked Lena

(c)Watermarked Liftingbody

Fig.4 The watermarked images (a) Barbara (b) Lena
(c) Liftingbody

Fig.5 Watermark extracted

Table1: PSNR between input and output images

Barbara	Lena	Liftingbody
46.11	47.66	47.51

4. REFERENCES

[1] Liang-Hua Chen, Jyh-Jiun Lin, 2003. "Mean Quantization Based Image Watermarking", Proceedings Of The Image Vision And Computing 21, pp 717-727

[2] R.B. Wolfgang, E.J. Delp, 1996. "A Watermark For Digital Images", Proceedings Of The International Conference On Image Processing 3

[3] N. Nikolaidis, I. Pitas, 1998. "Robust Image Watermarking In The Spatial Domain", Signal Processing 66 (3) pp 385–403.

[4] P.W. Wong, N. Memon, 2001. "Secret And Public Key Image Watermarking Schemes For Image Authentication And Ownership Verification", IEEE Trans. Image Process. 10 (10) pp 1593–1601.

[5] T.H. Chen, D.S. Tsai, 2006. "Owner–Customer Right Protection Mechanism Using A Watermarking Scheme And A Watermarking Protocol", Pattern Recogn. 39 (8) pp 1530–1541.

[6] C.Y. Lin, S.F. Chang, 2001. "A Robust Image Authentication Method Distinguishing JPEG Compression From Malicious Manipulation", IEEE Trans. Circuits Systems Video Technol. 11 (2) 153–168.

[7] C.T. Hsu, J.L. Wu, 1999. "Hidden Digital Watermarks In Images", IEEE Trans. Image Process. 8 (1) pp 58–68.

[8] M. Barni, F. Bartolini, V. Cappellini, .A. Piva, 1997." A DCT-Domain System For Robust Image Watermarking", Signal Process. 66 pp357–372.

[9] Athanasios Nikolaidis and Ioannis Pitas, 2003*."* Asymptotically Optimal Detection For Additive Watermarking In The DCT And DWT Domains", IEEE Transactions On Image Processing, Vol. 12, No. 5

[10] Ben Wang, Jinkou Ding, Qiaoyan Wen, Xin Liao, Cuixiang Liu, 2009. "An Image Watermarking Algorithm Based On DWT DCT And SVD", Proceedings of IC-NIDC

[11] Feng Liu, Yangguang Liu, 2008. "A Watermarking Algorithm for Digital Image Based on DCT and SVD". Congress on Image and Signal Processing

[12] LIU Rui-zhen, Tan Tie-niu.2001. "SVD Based Digital Watermarking Method". Acta Electronica Sinica, Vol.29, No.2.

[13] H.C. Andrews and C.L. Patterson,1976. "Singular Value Decomposition (SVD) Image Coding",IEEE Trans. On Communications, Nol. COM-24, No. 4, pp. 425– 432

[14] R.Z. Liu and T.N. Tan,2002. "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE Trans. On Multimedia, Vol. 4, No. 1, pp. 121–128.