ISSN:0975-9646
Chitla Arathi / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012,3644-3647

A Semi Fragile Image Watermarking Technique Using Block Based SVD

Chitla Arathi
Department of Computer Science & Engineering, Telangana University,
Dichpally, Nizamabad, Andhra Pradesh, Pin, No. 503 322, India

Abstract: This paper summarizes the overview of singular value decomposition (SVD) technique and its properties. It also presents a semi-fragile watermarking technique based on block based SVD. Semi-fragile watermark fragile to malicious modifications while robust to incidental manipulations is drawing many attentions in image authentication. The scheme can extract the watermark without the original image. SVD transformation preserves both one-way and non-symmetric properties, usually not obtainable in DCT and DFT transformations. Experimental results show that the quality of the watermarked image is good and that there is strong resistance against general image processing. Furthermore, it can locate alterations made on the image.

Keywords: ***Image authentication,*** *Semi-fragile watermarking, Singular value decomposition (SVD).*

1. INTRODUCTION

The rapid expansion of the internet and the advancement of digital technology in the past decade have increased numerous applications in the areas of multimedia communications. The ease with which digital content can be exchange over the internet has lead to illegal and unauthorized manipulation of multimedia products. In order to protect the interest of the content providers, those digital contents can be watermarked. Watermarking is used for content protection, content authentication, copyright management and tamper detection. In the past couple of years, several digital watermarking schemes have been proposed are based on DCT, DFT, and DWT transformations. This paper presents semi fragile block based watermarking technique using singular value decomposition (SVD) which allow JPEG lossy compression but prevent malicious manipulations. This technique can also detect tamper made on the image.

In the last few years, a SVD based watermarking technique and its variations are mostly encountered in the literature [6,7,8,9,10**]**. SVD is a mathematical technique used to extract algebraic features from an image. The core idea behind SVD based approaches is to apply the SVD to the whole cover image or alternatively to small blocks of it, and then modify the singular value to embed the water mark. Use of SVD in digital image processing has some advantages. First, the size of the matrices from SVD transformation is not fixed. It can be a square or rectangular. Secondly, singular values in a digital image are less affected if general image processing is performed. Finally, singular values contain intrinsic algebraic image properties. All the properties of SVD are summarized as follows.

- Stability: when a small perturbation is added to the matrix, large variance of its singular values does not occur.
- Singular values represent algebraic properties of an image.
- To some extent, singular values possess algebraic and geometric invariance.
- Rotation: given an image I and its rotated (with arbitrary angle) I^r, both have the same singular values.
- Translation: given an image I and its translated I^t. both have the same singular values.
- Scaling: given an image I and its scale I^s. if I has the singular values σ_i then I^s has the singular values $\sigma_i * \sqrt{L_R L_C}$ where L_R and L_C are the scaling factor of rows and columns respectively. If rows (columns) are mutually scaled, I^s has the singular values $\sigma_i * \sqrt{L_R}(\sigma_i * \sqrt{L_C})$
- Transpose: given an image I and its transposed I^T, both have the same singular values.
- Flip: given an image I and its row and column filled I_{rf} and I_{cf} transposed I^T, all have the same singular values.

The rest of this paper is organised as follows. In Section 2 classification of digital watermarking techniques are briefly discussed. Overview of SVD based watermarking is discussed in Section 3. Next, the proposed block based watermarking scheme is introduced in Section 4.In Section 5, the experimental results of the proposed scheme are shown. Finally, the conclusions are given in Section 6.

2. CLASSIFICATIONS OF DIGITAL WATERMARKING TECHNIQUES

The classification of watermarking algorithms can be done based on several criteria. According to the domain of the watermarking insertion, these techniques are divided into two broad categories: Spatial domain and Transform or Frequency domain algorithms. Spatial domain techniques [1] embed the data by directly modifying the pixel values of the host image, while transform domain techniques [2] embed the data by modifying the transform domain coefficients. Transform domain techniques are more robust enough to common image distortions.

According to the ability of watermark to resist attack, watermarking techniques are divided into fragile watermarking, semi fragile watermarking. A fragile watermark is a watermark that is readily altered or destroyed when the host image is modified through a linear or non linear transformation. The sensitivity of fragile watermarks to modification leads to their being used in image authentication [11]. Semi-fragile watermark fragile to malicious modifications while robust to incidental manipulations is drawing many attentions in image authentication. As a trade off of robustness and fragility, semi-fragile watermark that can resist "content preserving" operations (such as JPEG compression) and be sensitive to "content altering" transforms (such as feature replacement) is more practicable than fragile watermark in image authentication.

According to watermark detection and extraction they are divided into two types: Blind watermarking and Non blind water marking. Sometimes it is impossible to avail original

image so Blind watermarking requires extraction of watermark from watermarked image without original image, Whereas the Non Blind watermarking requires the original image to exist for detection and extraction.

2.1 Factors to determine quality of watermarking scheme

There are a set of essential factors that are evaluated to determine the quality of watermarking schemes. These factors can be organized and described as follows.

(i) Robustness: Robustness is a measure of immunity of watermark against attempts to image manipulations and modifications like compression, filtering, rotation, scaling, collision attacks, cropping, resizing etc.,

(ii) Imperceptibility: Means quality of the host image should not be destroyed by the presence of watermark i.e., the difference between the watermarked image and the original image cannot be distinguished by the human eye.

(iii) Capacity: The original image should embed maximum of information as watermark and it should successfully detect during extraction by using latest available techniques.

(iv) Unambiguous: An embedded watermark extracted from a watermark image cannot be distorted to such an extent that the original water mark cannot be identified.

(v) Blindness: To validate the existence of the watermark, either the original object is used to compare and find out the watermark signal (Non blind watermarking) or a correlation measure is used to detect the strength of the watermark signal from the extracted watermark (Blind watermarking) without original image is preferred.

2.2 Performance Evaluation of Digital Image Watermarking Algorithms:

Digital watermark performance can be measured with two metrics. They are

(i) Perceptual transparency: Means perceived quality of the image should not be destroyed by the presence of watermark. Quality of watermarked image is measured by Peak Signal to Noise Ratio (PSNR).Bigger is PSNR, better is quality of watermarked image.

PSNR for image with size M ×N is given by

$$PSNR = 10\log_{10}\frac{(max_I)^2}{MSE}$$

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{i,j} - y_{i,j})^2$$

MSE is the mean square error between the original image and the corresponding watermarked image pixels. max_I is the maximum pixel value of image which is equal to 255 for gray scale image where pixels are represented with 8 bits. Watermarked images with PSNR more than 28 are acceptable.

(ii) Robustness: Robustness is a measure of immunity of watermark against attempts to image manipulations and modifications like compression, filtering, rotation, scaling, collision attacks, cropping, resizing etc. This is measured in terms of Correlation factor. The correlation factor measures the similarity and difference between original watermark and extracted watermark. Its value is generally in between 0 to 1. Ideally it should be 1, but the value 0.75 is acceptable.

$$\rho(W, \hat{W}) = \frac{\sum w_i \hat{w}_i}{\sqrt{\sum w_i^2}\sqrt{\sum \hat{w}_i^2}}$$

Where W_i and $\hat{W}_i$ are original and extracted watermarks.

3. OVERVIEW OF SVD BASED WATERMARKING

The Singular Value Decomposition is one of a number of effective numerical analysis tools used to analyse matrices. It is a general liner algebra technique for a variety of applications including the solution of least squares problem, computing pseudo-inverse of a matrix and multivariate analysis. In addition SVD has been used in image processing applications such as image coding [4], noise estimation [5] and more recently in image watermarking [3].

From the perspective of image processing, an image can be viewed as a matrix with non negative scalar entries. In SVD transformation, a matrix can be decomposed into three matrices that are the same size as the original matrix. Given an image A with size n X n can be transformed into three components U, D, V respectively. The SVD of A is given by

$$[U \quad D \quad V] = SVD(A), \quad A' = UDV^T$$

$$\begin{bmatrix} u_{1,1}, \ldots, u_{1,n} \\ u_{2,1}, \ldots, u_{2,n} \\ \vdots \\ u_{n,1}, \ldots, u_{n,n} \end{bmatrix} \begin{bmatrix} \sigma_{1,1}, 0, \ldots, 0 \\ 0, \sigma_{2,2}, \ldots, 0 \\ \vdots \\ 0, 0, \ldots, \sigma_{n,n} \end{bmatrix} \begin{bmatrix} v_{1,1}, \ldots, v_{1,n} \\ v_{2,1}, \ldots, v_{2,n} \\ \vdots \\ v_{n,1}, \ldots, v_{n,n} \end{bmatrix}^T =$$

$$\sum_{i=1}^{n} \sigma_i u_i v_i^T$$

Where the U and V components are n X n real unitary matrices with small singular values, and the D component is an n X n diagonal matrix with large singular values which satisfy

$\sigma_{1,1} \geq \sigma_{2,2} \ldots \geq \sigma_{r,r} > \sigma_{r+1,r+1} = \ldots = \sigma_{n,n} = 0$. A' is the reconstructed matrix after the inverse SVD transformation. The U and V are orthogonal matrices where the columns of U are left singular vectors and the columns of V are the right singular vectors of the image A. The left singular vectors of A are the Eigen vectors of AA^T and the right singular vectors are the Eigen vectors of A^TA. It is important to note that the singular value specify the luminance of the image, whereas the corresponding pair of singular vectors specify the geometry of the image. The relationship between A and the three matrices U, D and V satisfy $Av_i = \sigma_i \mu_i$, and $\mu_i^T A = \sigma_i v_i^T$.

Using SVD in digital image processing has some advantages.

(i) The size of the matrices from SVD transformation is not fixed and can be a square or a rectangle.

(ii) Singular values in the digital images are less affected if general image processing is performed.

(iii) Singular values contain intrinsic algebraic image properties.

(iv) The SVD is an optimal matrix D composition technique in a least square sense that it packs the maximum signal energy into as few coefficients as possible.

(v) It has the ability to adapt to the variations in local statistics of an image.

However, SVD is image adaptive; the transform itself needs to be represented in order to recover the data.

4. BLOCK BASED SVD WATERMARKING TECHNIQUE

The basic idea behind the Block based SVD watermarking technique is, dividing the image into sub blocks and applying the SVD on each sub block so that the embedding and extraction process will be decentralized. Tamper localization will become easier with this process.

4.1 Watermark embedding process

1. Divide the M X N image X into sub blocks X_B. Perform SVD on each sub block X_B.
$$X_B = U \Sigma_X V^T$$
2. Perform SVD of watermark W, which is a two dimensional array of size P × Q, where M≥N and P≥Q.
$$W = U_w \Sigma_w V_w^T$$
3. Let Σ_B and Σ_W represent the diagonal matrices with singular values for the sub block X_B and watermark W respectively.
4. Extract the largest coefficient D (1, 1) from each Σ_B component and quantize it by using a pre defined quantization coefficient Q (Quality of the watermarked image can be determined by the quantization). Let Z=D (1,1) mod Q

Q is used for adjusting embedding strength and is chosen so as to maintain perceptual fidelity of the watermarked image. The smaller coefficient Q, The weaker is the robustness of embedded watermark. The bigger coefficient Q, The lower is the quality of the original image. So, coefficient Q should be cheesed according to concrete application situation.

5. Embed a bit, W_B of the watermark into Σ_B. After quantizing the D (1, 1)
   (i) For W_B=0, then D (1, 1) modified to
   D′ (1, 1) = D (1, 1)+Q/4-Z if Z□3Q/4
   D′ (1, 1)= D (1, 1)+5Q/4-Z otherwise
   (ii) For WB=1, then D (1, 1) modified to
   D′ (1, 1) = D (1, 1)-Q/4+Z if Z□Q/4
   D′ (1, 1) = D (1, 1)+3Q/4-Z otherwise
6. Let Σy_B represent the modified sub block. Apply reverse SVD transformation to re construct the watermarked sub image blocks Y_B and watermarked image Y
$$Y = U \Sigma_y V^T$$

If we embed the watermark into other singular values i.e other than largest singular value, the watermark information will not be extracted after JPEG lossy compression. Because the largest coefficients in the D component can resist general image processing, the embedded watermark was not greatly affected.

4.2 Watermark extraction procedure

Watermark extraction is the process of recovering or obtaining an estimate of the original watermark from a possibly distorted version of the watermarked image Y□. The extraction process requires the knowledge of the watermark and the original image, specifically the matrices Σ_x, U_w V_w.

Apply the block SVD procedure to the possibly distorted version of the watermarked image i.e.

(i) Partition the watermarked image into blocks.

(ii) Perform the SVD transformation on each block
$$Y_B = U \Sigma_{Y_B} V^T$$

(iii) Extract the largest coefficient D' (1, 1) from each D component Σ_{Y_B} and quantize it using the predefined quantization coefficient Q. Let Z= D' (1, 1) mod Q

(iv) If Z□Q/2, the extracted watermark has a bit value of 0. Otherwise, the extracted watermark has a bit value 1.
$$\Sigma_{w_B} = \frac{(\Sigma_{Y_B} - \Sigma_{X_B})}{\alpha}$$
$$\hat{W} = U_W \Sigma_{w_B} V_W^T$$

Where α is a scaling parameter which determines the embedding strength and is chosen so as to maintain perceptual fidelity of watermarked image.

4.3 To assess the extent of Tampering

To assess the extent of tampering, compute the tamper assessment function
$$T_{AF}(w, \hat{w}) = \frac{1}{M_1 M_2} \sum \sum \hat{w} \oplus w$$

Where w is the original watermark, $\hat{w}$ is the extracted watermark, M_1 and M_2 are their respective sizes of the watermarks, $\oplus$ is exclusive OR operation.

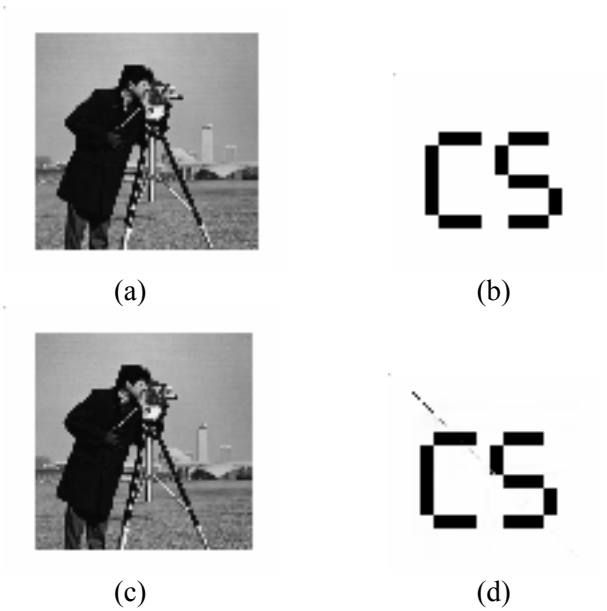
The value of $T_{AF} \in [0, 1]$.

The presence of tampering is determined if $T_{AF} \geq \tau$, where $0 \leq \tau \leq 1$ is pre specified threshold. If T_{AF} □ τ, then the modifications on the image is consider to be incidental and negligible. For higher security applications τ can be set to be smaller. The magnitude of T_{AF} can be used to assess the extent of tampering.

5. EXPERIMENTAL RESULTS

In this section, some experiments are carried out to demonstrate the effect of the proposed semi-fragile watermarking technique.

Figure 1 shows the original image, the watermark of the same size as the original image, the watermarked image, and the extracted watermark without any attacks. A single watermark is used and the correlation coefficient ρ between the extracted watermark and the original one is 0.8308. Figure 2 shows the original image, the watermark added to each block, the watermarked image, the correlation co efficient between the original watermark and the watermarks extracted from each block. Figure 3 shows the watermarked images with some attacks.



(a) (b)

(c) (d)

Figure1. (a) Original image. (b) Watermark. (c) Watermarked image without attacks. (d) Extracted watermark with $\rho(W, \hat{W})$ =0.8308.

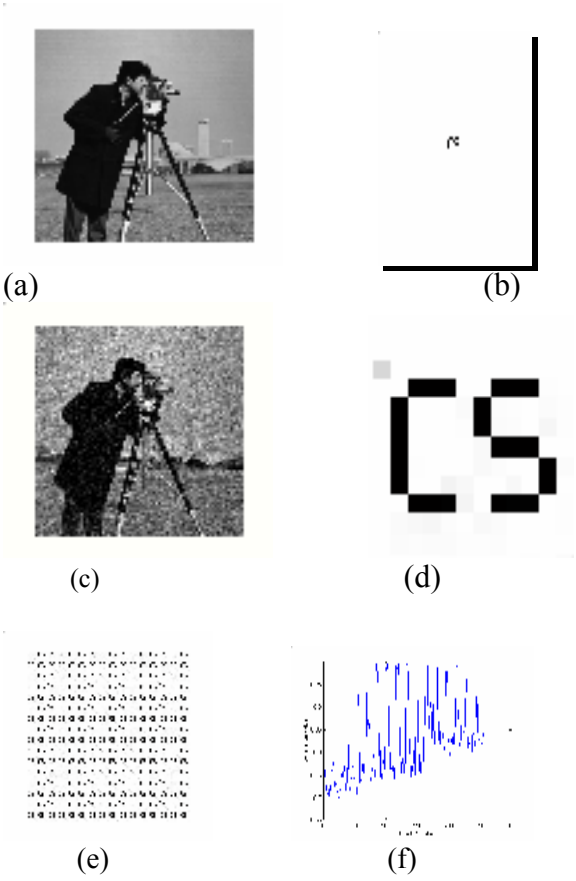


Figure2. (a) Original image. (b) Watermark embedded in each block. (c) Watermarked image without attacks. (d) Extracted watermarks from each block. (e) Zooming of extracted watermark (f) Correlation coefficient between each extracted Watermark and the original one.

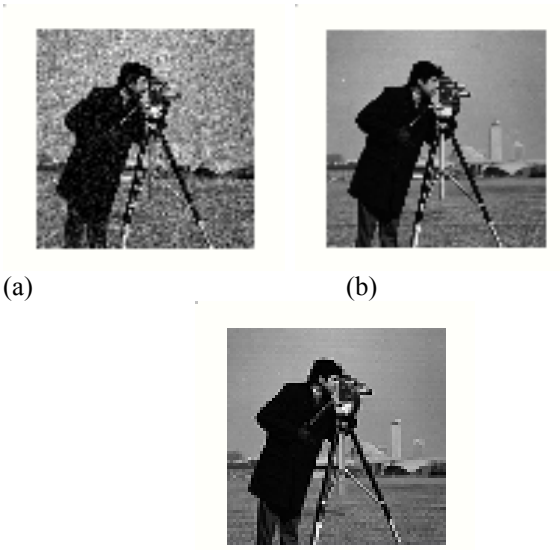


Figure 3. Attacks on the image watermarked by the proposed method. (a) Gaussian noise 0.01 (b) Resizing 256-128-256 (c) JPEG compression

6. CONCLUSION

This paper presents a visually undetectable, robust watermarking algorithm. This algorithm depends on embedding the watermark into the singular values of the original image after dividing it into blocks. The experimental results show that the proposed Block-by-Block SVD-watermarking algorithm has a high fidelity and robustness in the presence of different types of attacks. The results reveal also the superiority of the proposed algorithm to the traditional SVD watermarking algorithm.

REFERENCES

[1] C-H. Lee, and Y-K. Lee, ·An Adaptive Digital Watermarking Technique for Copyright Protection," IEEE Trans. Consumer Electronics, vol.45, pp. 1005-io15, NOV. 1999.

[2] I. J. Cox, M.Miller, and J.A. Bloom, Digital Watermarking, Morgan Kaufmann, 2002.

[3] V.I. Gorodetski, L.J. Popyack, V. Samoilov, and V.A.Skormin,"SVD-Based Approach to transparent Embedding Data into Digital Images,"Proc.Int.Workshop on Mathematical methods, models and Architecture for Computer Network

[4] J.F.Yang and C.L.Lu "combined Techniques of Singular Value Decomposition and Vector Quantization for Image Coding," IEEE Trans. Image Processing, pp. 1141 - 1146, Aug. 1995.

[5] K. Konstantinides, B. Natarajan, and G.S.Yovanof, "Noise Estimation and Filtering Us-ing Block-Based Singular Value Decomposition," IEEE Trans. Image Processing, vol. 6, pp. 479-483, March 1997.

[6] C.-C. Chang, P. Tsai, C.-C. Lin, Pattern Recogn. Lett. 26 (2005) 1577.

[7] K.-L. Chung, W.-N. Yang, Y.-H. Huang, S.-T. Wu, Y.-C. Hsu, Appl. Math. Comput.188(2007)54

[8] M.-Q. Fan, H.-X. Wang, S.-K. Li, Appl. Math. Comput. 203 (2008) 926.

[9] E. Ganic, N. Zubair, A.M. Eskicioglu, Proc. The IASTED Int. Conf. on Communication, Network, and Information Security, New York, USA, 2003, p. 85.

[10] R. Liu, T. Tan, IEEE Trans. Multimedia 40 (2002) 121.

[11]Zaho Y.,"Dual Domain Semi-Fragile Watermarking for image Authentication",Master Thesis,University of Toronto,2003