Advanced Research in Electrical and Electronic Engineering
Print ISSN: 2349-5804; Online ISSN: 2349-5812 Volume 2, Number 9 April-June (2015) pp. 58-62

http://www.krishisanskriti.org/areee.html

Implementation of Digital Image Watermarking using SVD

Jaiveer Tewatia[1] and Shivani Singh[2]

[1,2]Department of Electronics and Communiction Manav Rachna College of Engineering Faridabad, India
E-mail: [1]tewatia.jai10@gmail.com, [2]shivanisingh.mrce@mrei.ac.in

Abstract—*Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Copyright protection of digital information is the most widely used application of digital watermarking. It is different from the encryption in the fact that it allows the user to access, view and interpret the signal but protect the ownership of the content. In latest years, various digital watermarking techniques are presented based on discrete cosine transform (DCT), discrete wavelets transform (DWT) and discrete Fourier transform (DFT). In this paper we have proposed an algorithm for digital image watermarking technique based on singular value decomposition (SVD).The quality of the watermarked image is excellent and there is strong resistant against many geometrical attacks.*

Keywords*: Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), power signal to noise ratio (PSNR), extracting and embedding.*

1. INTRODUCTION

Digital watermarking is a technique that embeds data called watermark into a multimedia object so that watermark can be detected to make an assertion about the objects. It can be categorized as visible or invisible. Ex-ample of visible watermarking is the logo visible super-imposed on the corner of television channel in a television picture. On the other hand, invisible watermark is hidden in the object, which can be detected by an authorized person. Such watermarks are used for suit the author authentication and detecting unauthorized copying. Digital watermarking is having a variety of useful applications such as digital cameras, medical imaging, image databases, video on demand systems, and many others. In recent years, many digital image watermarking techniques have been proposed in the literature which is based on spatial domain technique and frequency domain technique. These techniques are used in watermark embedding algorithm and watermark extracting algorithm. Digital watermarking based on DWT and DCT is used to improve the performance of the DWT-based watermarking algorithms [3]. In this method, watermarking is done by embedding the watermark in first and second level of DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. The combination of these two transforms improved the watermarking performance considerably in comparison with only watermarking approaches. They showed that the quality of watermark image is very good. In 2005, Chen [4] proposed a singular value decomposition scheme based on components of D and U without using DWT, DCT and DFT transforms. They showed that quality of watermarked image is good on their schemes. In 2007, [5] introduced a novel digital watermarking method based on single key image for extracting different watermarks. In this method, they used Arnold transform technique in watermark embedding and ex-traction, which is based on DWT and DCT algorithm. With the popularity of internet and availability of large storage devices, storing and transferring an image is simple and feasible. They showed that robustness of the algorithm against many signal processing operations.

Most of the domain transformation watermarking techniques works with DCT and DWT. However singular value decomposition (SVD) is one of the most powerful numeric analysis techniques and used in various requirements. These requirements can be organized and described as follows.

Undeletable: An embedded watermark is difficult to detect and cannot be removed by an illegal person. Also the algorithm must resist different attacks.

Perceptually visible: The original images and water-marked images cannot be distinguished by the human eye. This means that there is not enough alteration of a watermarked image to prevent motivation to an illegal person.

Unambiguous: An embedded watermark selected from a watermarked image that must be clear enough for ownership to be determined. In this way, the extracted watermark cannot be distorted to such an extent that the original watermark cannot be recognized.

In this paper, we will describe a digital image water-marking algorithm based on singular value decomposition technique.

2. DIFFERENT TECHNIQUES OF DIGITAL WATERMARKING

Digital watermarking is a prominent field of research and many researchers have suggested a large number of algorithms

and compared. The main thrust on all such algorithms is to hide secrete information (watermark) in host signal in such a way that it provides good tradeoff between imperceptibility and robustness against different attacks. This section presents several types of digital watermarking techniques found in the academic literature. We do not give an exhaustive review of the area, but provide an overview of established approaches. Existing digital watermarking techniques are broadly classified into two categories depending on the domain of watermark insertion:

- Spatial Domain Technique
- Frequency Domain Technique

Earlier watermarking techniques are almost spatial based approach. In spatial domain the watermark is embedded into the host image by directly modifying the pixel values, i.e. simplest example is to embed the watermark in the least significant bits (LSBs) of image pixels. Spatial domain watermarking is easy to implement and requires no original image for watermark detection. However, it often fails under signal processing attacks such as filtering and compression and having relative low-bit capacity. A simple image cropping operation may eliminate the watermark. Besides, the fidelity of the original image data can be severely degraded since the watermark is directly applied on the pixel values. In contrast to the spatial-domain-based watermarking, frequency-domain based techniques can embed more bits of watermark and are more robust to attack; thus, they are more attractive than the spatial-domain-based methods, because the watermark information can be spread out to the entire image.

As to the frequency transform, there are DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), and DWT (Discrete Wavelet Transform).

A. Spatial Domain technique

Embedding the watermark into spatial domain component of the original is straight forward method. LSB scheme is one of the examples from spatial domain which modifies lower order bits of cover image to embed the watermark. It has the advantage of low complexity and easy implementation but problem with this scheme is low security, because it is possible to remove the watermarked image easily by setting all LSBs or pixels to zero.

B. Frequency domain technique

Compared to spatial domain techniques, frequency domain techniques are more applied. The target of this technique is to insert the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT). The discrete wavelet transforms (DWT) and the discrete cosine transforms (DCT) are implemented very effectively in numerous digital images watermarking scheme. In this new era, Singular Value Decomposition (SVD) is also implementing very effectively in the digital image watermarking scheme. A-Haj [3] presented a combined DWT-DCT digital image watermarking algorithm. Watermarking is carried out through the embedding of the watermark in the first and second level DWT sub-bands of the host image sub-sequenced by the application of DCT on the selected DWT sub-bands. The most commonly used transforms are given below:

3. DCT (DISCREATE COSINE TRANSFORM)

DCT based watermarking scheme which provides higher resistance to image processing attacks such as JPEG compression, noise, rotation, translation etc. In this approach, the watermark is embedded in the mid frequency band of the DCT blocks carrying low frequency components and the high frequency sub band components remain unused. Watermark is inserted by adjusting the DCT coefficients of the image and by using the private key. Watermark can then be extracted using the same private key without resorting to the original image. Performance analysis shows that the watermark is robust.

4. DWT (DISCREATE WAVELET TRANSFORM)

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. DWT is the multi resolution description of an image the decoding can be processed sequentially from a low resolution to the higher resolution. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. The high frequency components are usually used for watermarking since the human eye is less sensitive to changes in edges.

The Wavelet Transform, at high frequencies, gives good time resolution and poor frequency resolution, while at low frequencies; the Wavelet Transform gives good frequency resolution and poor time resolution.

5. SVD (SINGULAR VALUE DECOMOSITION)

Singular value decomposition is one of a number of valuable numerical analysis tools which is used to analyse matrices. It can be appeared from three jointly compatible points of view. On the other hand, we can see it as a method for transforming correlated variables into a set of uncorrelated ones that better expose the various relationships among the original data items. At the same time, SVD is a method for identifying and ordering the dimensions along which data points demonstrate the most variation.

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.

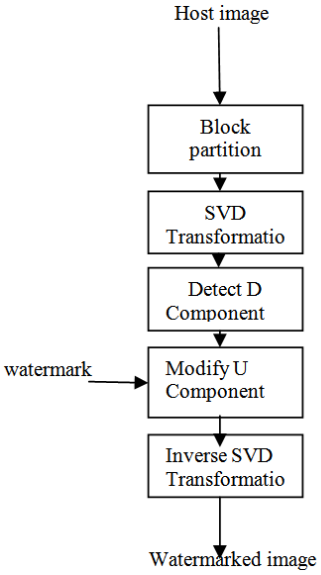


Fig. 1: The watermark embedding procedure

A grayscale digital image is specified by an m x n matrix I= $\{I_{ij}\}_{mxn}$. If a color image is represented in RGB then it can be converted to the corresponding luminance matrix Y= $\{Y_{ij}\}_{mxn}$. An arbitrary matrix, A= $\{A_{ij}\}_{mxn}$ can be represented by its SVD In the following form:

$$A = USV^{T} = \sum_{i=1}^{r} \lambda_i U_i V_i^{T} \quad (1)$$

Where, U and V are orthogonal m×n and n ×n matrices, respectively, and s is a diagonal matrix with non negative elements. Diagonal terms $\lambda_1, \lambda_{2,\ldots,} \lambda_r$ of matrix , S are SVs of matrix $A$and r is the rank of matrix.

SVD possesses several attractive mathematical properties, one of which is that each SV specifies the luminance of the SVD image layer, whereas the respective pair of singular vectors specifies intrinsic *geometry* properties of images. It was discovered that slight variations of SVs do not affect the visual perception of the cover image, which motivates the watermarking embedding through slight modifications of SVs in the segmented images.

The proposed scheme is briefly described as follows. An image represented in matrix format is segmented into blocks of size w × w (in our experiment, w is generally set to 4) and the SVD for each of the blocks is performed. Then, one bit of data is embedded through a slight modification of the SV of the block. Let *b* be the current bit of the watermark image to be embedded into this block B_k. The embedding algorithm is described as follows.

1) Segment the image into blocks B_k of size w × w, k=1,2,…,N, where N is the number of the blocks.

2) Compute $n_v = \|v+1\|$, where $v = (\lambda_1^k, \lambda_2^k, \ldots, \lambda_w^k)$, v is a vector formed by the SVs of each block B_K.

3) Compute integer number $s = [n_v / d_k]$, where d_k is the quantization step for n_v corresponding to the block, $B_{K.}$

4) Embed one bit *b* of watermark image as follows.
If *b*=1, then
If S is odd number, then $S = S + 1$
ELSE S remains unchanged
If *b*=0, then
If S is even number, then $S = S + 1$
ELSE S remains unchanged.

5) Compute the value $n_v^{'} = d_k \times s + d_k / 2$ and the modified SV

$$(\gamma_1^k, \gamma_2^k, \ldots, \gamma_w^k) = (\lambda_1^k, \lambda_2^k, \ldots \lambda_w^k) \times \frac{n_v^{'}}{n_v}$$

6) Compute the matrix of the block using the modified SV

$$\tilde{B}_K = \sum \lambda_i^k U_i(k) V_i^T(k)$$

7) Reconstruct the watermarked image from all the blocks $\tilde{B}_K$

It should be noticed that quantization step d_k would be served as a secret key to ensure the authorized access to the watermark.

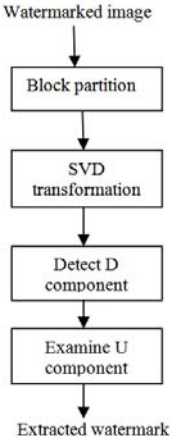


Fig. 2: The watermark extracted procedure

The extraction of the watermark is straightforward. Let $\tilde{B}_K$ be a block with an embedded watermark bit.

1) Segment watermarked image into blocks $\tilde{B}_K$ of size $w \times w$, $k = 1,2,\ldots, N$, where N is the number of the blocks.

2) Compute the value $\tilde{n}_v = \|u\| + 1, u = (\gamma_1^k, \gamma_2^k, ..., \gamma_w^k)$,

Where u is a vector formed by the SV $\gamma_1^k, \gamma_2^k, ..., \gamma_w^k$ of each block $\tilde{B}_K$.

3) Compute $s = [\tilde{n}_v / d_k]$

4) If s is even number, then the embedded bit is 1. Otherwise, it is 0.

6. RESULTS

The experimental results are simulated with the software MATLAB. It provides a single platform for computation, visualization, programming and software development. All problems and solutions in Matlab are expressed in notation used in linear algebra and essentially involve operations using matrices and vectors. We are using a 200 × 200 "image1", as the gray scale original host image, and a 50 × 50 grey- scale image of the watermark image. The image is shown in Figure 3 and 4. In the proposed method, we select the largest complexity of blocks; the original images can be separated into blocks of 4 × 4 pixels. Each block can be transformed into V, D, and U components by singular value decomposition. And then, a set of blocks with the same size as the watermark was selected, according to the feature of the D component. For an embedding watermark block, the relationship between the V component coefficients can be examined and the coefficients were modified, according to the watermark to be embedded. In our experiment, the original image and watermarked image quality is shown.

To evaluate and compare the performance of the two techniques i.e., SVD and DWT two parameters are taken into consideration. These parameters are

$$MSE = \frac{1}{MN} \sum_{I=1}^{M} \sum_{J=1}^{N} [I(i, j) - I'(i, j)]^2$$

Where, MSE is mean square error

$M \times N$ is the dimensions of the images,

$I(i, j)$ is the original image ,

$I'(i, j)$ is the watermarked image

Using the value of mean square error, PSNR (Peak Signal to Noise Ratio) for the image is calculated which give the ratio of required signal to the noise contents in the watermarked image. PSNR is calculated by the formula:

$$PSNR = 10 \log_{10} \left[\frac{255^2}{MSE} \right]$$

To carry out the experiments MATLAB R2011a software is used. Results obtained are

(a) (b)

Fig. 3: (a) Original image1 and (b) embedded watermark image

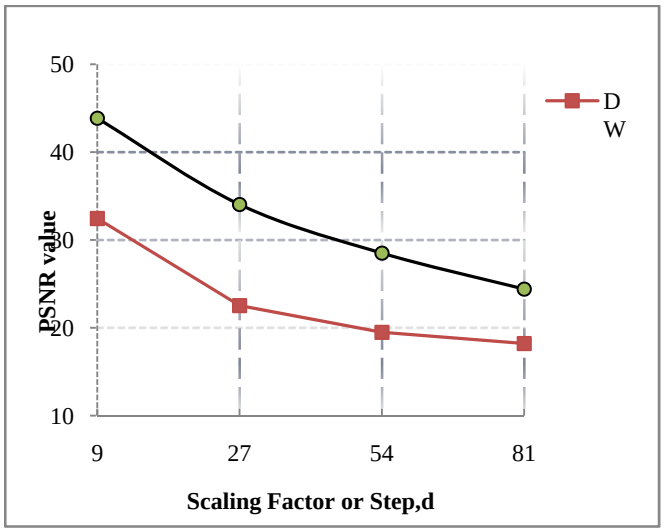
(a) (b)

Fig. 4: (a) watermarked image1 and (b) extracted watermark image

Table I: PSNR calculation of image using different techniques

Image	Constant Step, d			DWT
	9	27	54	
Image1	43.8794	34.3358	28.5298	25.5298
Baboon	44.8076	35.0587	29.1219	26.5298
Lena	43.9947	34.1596	28.3588	27.9065
Dark clouds	44.0488	35.5346	28.5663	29.0742
Shore	48.8313	34.2078	28.0401	27.6719

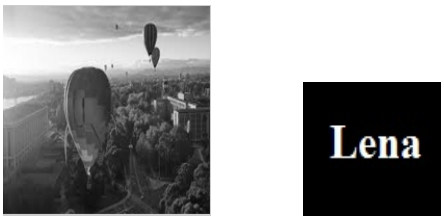
7. PLOT FOR COMPARISON BETWEEN SVD AND DWT



On comparing the value of PSNR at different value of quantization step, d it is concluded that the SVD technique is much better than DWT technique. As at every value of d or scaling factor, value of peak signal to noise ratio is more in case of the DWT technique. Less the value of PSNR more will be degradation in the quality of the original image. This shows that after watermarking, the quality of original image degrades more when DWT technique is used for embedding the watermark in comparison with SVD technique embedding.

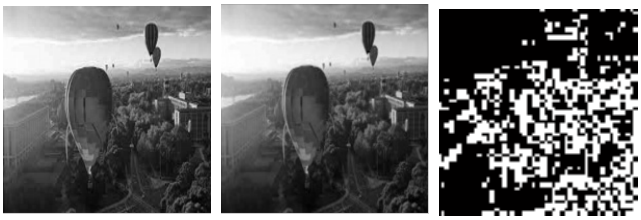
ATTACK

If anyone to attack the watermarked image on the channel, or try to extract the information using filters then the information will be fully corrupted. This means that the no anyone can see the information.



(a) **(b)**

Fig. 5: (a) Original image1 and (b) embedded watermark image



(a) **(b)** **(c)**

Fig. 6: (a) watermarked image1, (b) filtered image and (c) extracted watermark image

8. CONCLUTION

SVD based watermarking method for image authentications presented, where the watermark bits are embedded on the SV (luminance) of the blocks within each wavelet sub band of the original image. The quantization parameters of the watermarking are modeled based on the statistics of block images within different sub bands in wavelet domain thus adaptive to the individual image. The proposed method preserves high perceptual quality of the watermarked image (high PSNR). It also possesses an excellent fragility to various malicious attacks, thus enabling a variety of the authenticated networked multimedia applications. The watermark detection is also efficient and blind, i.e., only the compressed quantization parameters but not the original image are needed. Since the watermark embedding is solely determined by the quantization parameters, the malicious detection of the watermark would not be possible without knowing the quantization parameters. This scheme also achieves higher embedding rates than other methods.

REFERENCES

[1] L. Rajab, T. Khatib and A. Haj, "Combined DWT-DCT Digital Image Watermarking," *Journal of Computer Sci*ence, Vol. 3, 2002, pp. 740-749.

[2] Paul Bao and Xiaohu Ma, "*Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition"*, IEEE transactions on circuits and systems for video technology, vol. 15, no. 1, january 2005

[3] Y. Hu and S. Kwong, "Wavelet domain adaptive visible watermarking,"*Electron. Lett.*, vol. 37, no. 20, pp. 1219–1220, Sep. 2001.

[4] C. C. Chang and P. Tsai, "SVD-based Digital Image Watermarking Scheme," *Pattern Recognition Letters*, Vol. 26, No. 10, 2005, pp. 1577-1586. doi:10.1016/j.patrec.2005.01.004.

[5] T. V. Nguyen and J. C. Patra, "A Simple ICA Based Di- gital Image Watermarking Schem ces*sing*, Vol. 18, No. 5, 2007, pp. 762-776. doi:10.1016/j.dsp.2007.10.004.

[6] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[7] Sumit Kumar Prajapati, AmitNaik, AnjulataYadav/ International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-Jun 2012, pp.991-997

[8] Deepa Mathew K, "SVD based Image Watermarking Scheme", *IJCA Special Issue on "Evolutionary Computation for Optimization Techniques" ECOT, 2010.*

[9] Bhupendra Ram, *Member*, *IEEE* "Digital Image Watermarking Technique Using Discrete Wavelet Transform And Discrete Cosine Transform", International Journal of Advancements in Research & Technology, Volume 2, Issue4, April-2013 19 ISSN 2278-7763.

[10] L. Robert, T. Shanmugapriya, A Study on Digital Watermarking Techniques, International Journal of Recent Trends in Engineering, 2009.