Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Oblivious and Robust Image Watermarking Algorithm Using SVD Transformation

K.S.S. Manasa[1], G. Upendra[2], G. Aishwarya[3], A. Prudhvi Raj[4], Dr. K. Ramanjaneyulu[5]
[1,2,3,4]Dept. of ECE, [5]Professor, ECE, PVP Siddhartha Institute of Technology, AP, India

Abstract--Digital multimedia content protection has increasingly become an important issue. As image watermarking is identified as a major technology used in Copyright and Content Protection, a key necessity for image watermarking is the improvement of its impalpability and robustness. To meet this requirement, in this paper, an algorithm for watermarking of digital images based on singular value decomposition (SVD) is considered. At the transmitter, the host image is split into blocks and by performing SVD transformation the D components are detected. All the D components of the host image are now modified in accordance with the embedding criteria and the type of watermark bit. During extraction, the diagonal matrix of each block of the watermarked image has been observed and the reconstruction of watermark is performed.

Index Terms: Digital Image watermarking,SVD Transform, Copyright Protection, Normalized Cross Correlation(NCC),and Peak Signal to Noise Ratio(PSNR).

I. INTRODUCTION

Digital Watermarking is the way to protect multimedia files.We are aware of various multimedia files like audio, video, image, text, speech etc., which carries some sort of information within them. The information may be either analog or digital. Now-a-days, with the present technology, it is very easy to copy the data whatever may be the format it is. So, the protection and illegal redistribution of data is an important issue to be considered in the digital scenario. This is due to the popularity and accessibility of internet by the people. This results in recording, editing and replication of multimedia contents. So the main theme is to have Copyright Protection and Content Protection.If we want to protect the content that we own from malicious use i.e., to protect Intellectual Property Rights (IPR) and to have Security through obscurity, it is necessary to hide the information. There are two ways to hide the information. One way is to embed the information which can't be visually perceived which is treated to be the classical approach and the other way is embedding information in digital data so that it can't be visually or audibly perceived which is treated to be the Modern approach.

Various information hiding techniques are Cryptography, Steganography and Watermarking. Cryptography is a common method to protect digital content. However,an unauthorized party can easilydecrypt the message. Steganography hides a message in a cover to obtain new data which is practically indistinguishable from cover data, by people, in such a way that a third party cannotdetect the presence of message in the new data but it is used in one to one communication only.Similarly, Watermarking hides a message in a cover to obtain new data which is practically indistinguishable from cover data, by people, in such a way that a third party cannot remove or replace message in the new data. Digital Watermarking can protect the content even ifit is decrypted.

Digital watermarking is the function of hiding a message related to a digital signal which allows embeddingspecial pattern or some data. Features of watermarking are Invisible/Inaudible;Inseparable and Unchanging data file size.Hence, the proposed scheme is said to be oblivious i.e., unaware and is having robustness. Classification of watermark can be done according to human perception, robustness and types of document. Watermarking can be done in two major steps depending on location selection-where to embed watermark and depending on the processing-how to modify original data to embed watermark. Watermarking mainly involves three major steps 1)Watermark embedding 2)Attacks 3) Watermark extraction.

In this paper, an oblivious and robust image watermarking algorithm using SVD transformation is proposed.Rest of the paper is categorized as: Section 2 handles review of the related works. Section 3 handles the proposed method, section4 handles experimental results showing the improved performance of the proposed method in relation with the existing techniques. Robustness against the most common attacks is also presented. Finally, the section 5 discusses conclusion part.

II. REVIEW OF THE RELATED WORKS

Singular Value Decomposition (SVD) is a persuasive mathematical dissection that is extensively used for image processing. Matrix analysis can be done using SVD. In SVD transformation, each matrix is divided in to three other matrices having similar size of a host matrix.Those are upper triangular matrix (V), lower triangular matrix (U)and diagonal matrix (S).In diagonal matrix, the

Volume 4 Issue IV, April 2016
ISSN: 2321-9653

diagonal elements are non-negative and they are called as singular values.The diagonal matrix considered here is a square matrix and is less affected when general image processing is done. The largest S coefficients are modified to embed a watermark. The modification is done using a quantization mechanism. Depending on the watermark bit there is a possibility to have a clear idea whether the embedding and extracting procedures are performed well or not. Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin [1]proposed SVD-based digital image watermarking scheme which is focused on exploring both S and U components for embedding a watermark. However, modifications in the U component coefficients leads to the alteration of the original pixel values as well as degrade the quality of the watermarked image having less performance criteria ofPSNR and NCC which is a drawback of their method. So, by considering only S component which can resist to any modifications that are impressed on it the effective robustness can be obtained with an improved performance evaluation parameters PSNR and NCCwhich are discussed in the section 4.

III. PROPOSED WATERMARKING SCHEME

In this section, the scheme proposed is characterized in to three sub sections. Section 3.1 handles Embedding of watermark, Section 3.2 handles attacks and in Section 3.3.Extraction of watermark is explained. The performance evaluation is studied based on the resultant PSNR and NCC values.

A. Watermark Embedding

Embedding of watermark using SVD transformation involves the following steps. 1) Block partition 2) SVD transformation 3) Identifying the diagonal component 4) Modifying thediagonal component as per the embedding criteria 5) Inverse SVD transformation.

Let the host image be H and watermark image be W. Host image Hwill be partitioned into blocks of size 8x8. The size of host image is takenas 512x512.Let P_i represents i^{th}block of the host image H.SVD transformation is performedon $P_i$for all i.Then, largest component of diagonal matrix is identified. All those components are now modified by embedding a watermark of size 64x64 which is a binary image which results in a watermarked image and let it be H'. Depending upon the quantization mechanism the quality of watermarked image can be maintained. Now, inverse of SVD transformation is performed to reconstruct the watermarked image i.e., the selected S components from each block which have undergone watermark are now re-arranged in to their previous positions.

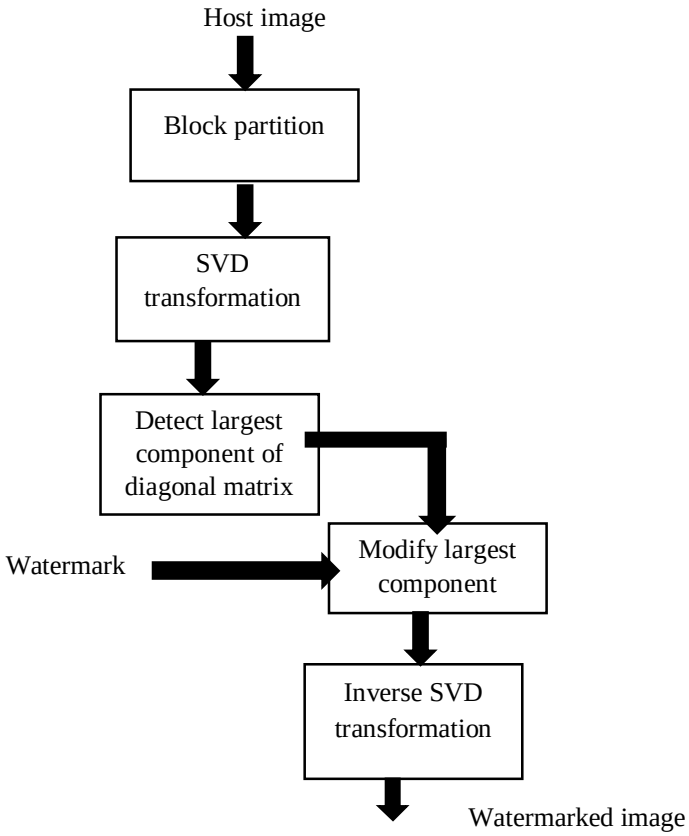


Figure 1. Embedding procedure

Volume 4 Issue IV, April 2016
ISSN: 2321-9653

B. Attacks

In any application, the watermarked digital image is transmitted through a network, usually internet, to other party or stored in some storage media for future purpose.In any case, watermarked image will be undergoone or more image processing operations which may modify the content of the watermarked image.Any image processing operation performed on watermarked image is called an attack. The watermarked image is now tested for various attacks to find the robustness of the watermark. JPEG compression with various values for quality factors,median filter, Gaussian filter, Average filter, High pass filterhistogram equalization, Resize or scaling, Cropping s(1/4), Gaussian noise, Salt and Pepper noise etc., are the attacks used on watermarked image. Now the distorted watermark image obtained after undergoing various attacks is treated to be H''.

Different quality factors ranging from 10 to 100 are applied on to the watermarked image and the corresponding Normalized Correlation Coefficients are noted down for both Lena and Camera man watermarked images.

Table 1.NCC of the watermark images extracted from JPEG attacked Lena and Camera man watermarked images with different values for quality factors

JPEG Quality Factor (QF)	NCC for Lena	NCC for Camera man
10	0.1298	0.3247
20	0.9159	0.8587
30	0.9948	0.9889
40	1.0000	1.0000
50	1.0000	1.0000
60	1.0000	1.0000
70	1.0000	1.0000
80	1.0000	1.0000
90	1.0000	1.0000
100	1.0000	1.0000

PSNR obtained for Lena and Camera man watermarked images are 40.0587 and 40.7036 respectively.

Table 2.NCC of the watermark images extracted from Lena and Camera man watermarked images with various other attacks

Type of Attack	NCC for Lena	NCC for Camera man
Median Filter (3 x 3)	0.7874	0.8589
Gaussian Filter (3 x 3) Variance = 0.5	0.9149	0.9009
Average Filter (3×3)	0.6196	0.6345
Sharpening Filter	0.2265	0.3849
Histogram Equalization	0.0532	-0.0574
Scaling 50%	0.5410	0.6176
Cropping 25%	0.4192	0.8440
Gaussian noise (0.001)	0.7598	0.8257
Salt & pepper noise (0.001)	0.8303	0.9217

Volume 4 Issue IV, April 2016
ISSN: 2321-9653

C. Watermark Extraction

Extraction of watermark is similar to that of embedding procedure except the host image is replaced with the watermarked image. Steps involved in extraction procedure are 1) Block partition the watermarked image 2) Apply SVD transformation 3) Detect largest component of the diagonal matrix4) Watermark Extraction.During extraction, as per the extraction criteria, decision will be taken either in favor of 1 or 0. Now, the extracted/recovered watermark is identified with a symbol w'.

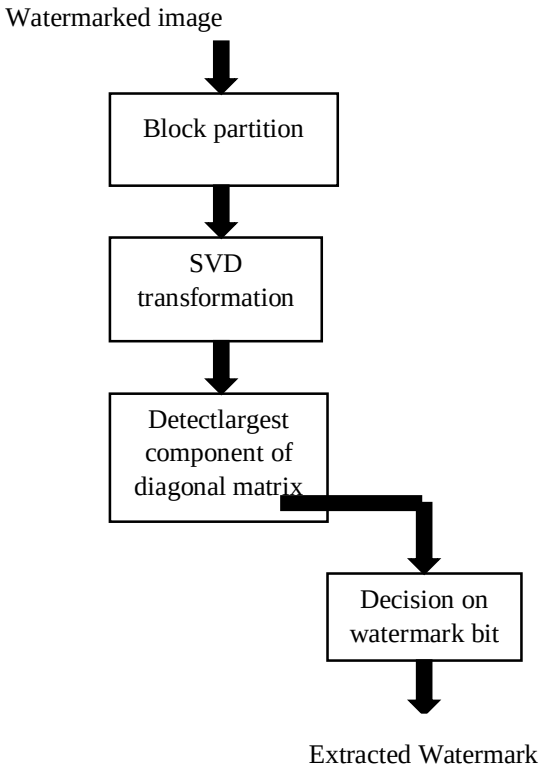
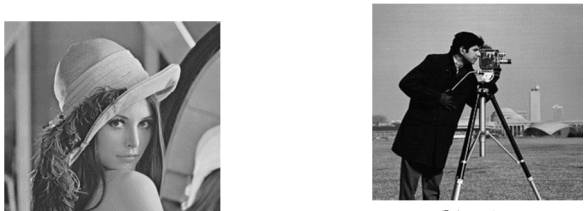


Figure 2. Extracting proc

IV. EXPERIMENTAL RESULTS

The host images used for experimentation are Lena and Camera man,each of size 512×512 pixels, 8 bits/pixel and the watermarks used are binary images ECE and star, each of size 64x64.



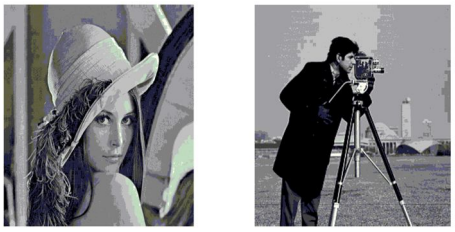
(a) Lena (b) Camera man

Figure 3. Host Images of size 512 × 512

(a) Binary image ECE (b) Star

Figure 4. Watermark Images of size 64x64

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



(a)Watermarked Lena (b) Watermarked Camera man
Figure 5. Watermarked Images

Figure 6. Extracted Watermark Images

To demonstrate the robustness ofthe proposed scheme the peak signal to noise ratio (PSNR) is used to estimate the quality of the watermarked image.

$$PSNR = 10\log_{10}\frac{255\times 255}{\frac{1}{M\times N}\sum_{x=1}^{M}\sum_{y=1}^{N}\left[f(i,j)-g(i,j)\right]^2}\,dB$$

Where, M and N are the height and width of the image, respectively. f(i, j) and g(i, j) are the pixel values located at coordinates (i, j) of the original image, and the attacked image, respectively.

Normalized Correlation Coefficient(NCC) is used to estimate the correctness of the extracted watermark.

$$NCC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}[w(i,j)-w_{mean}][w^{\circ}(i,j)-w^{\circ}_{mean}]}{\sqrt{\left(\sum_{i=1}^{m}\sum_{j=1}^{n}[w(i,j)-w_{mean}]^2\right)\left(\sum_{i=1}^{m}\sum_{j=1}^{n}[w^{\circ}(i,j)-w^{\circ}_{mean}]^2\right)}}$$

Where, m and n are the height and width of the watermark, respectively. The symbols $w(i,j)$ *and* $w^{\circ}(i,j)$ are the bits located at the coordinates (i,j) of the original watermark and the extracted watermark respectively. The symbols w_{mean} and w°_{mean} are the mean values of the original watermark and the extracted watermark respectively.

V. CONCLUSIONS

In this paper, an oblivious and robust image watermarking algorithm using SVD transformation is proposed. A binary watermark is embedded on to the host image which is of gray scale. The observable quality of the watermarked image obtained after embedding is up to snuff and the watermark can withstand for JPEG attacks and for various other attacks. Advantage of the proposed scheme over previous methods is having optimum values of PSNR and NCC.Experimental results shows that the performance of the scheme is better in terms of the embedding capacity, PSNR and NCC which shows that this scheme is said to have effective protection towards the copyright and content.

REFERENCES

[1] Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin, “SVD-based digital image watermarking scheme”, Science direct-Pattern Recognition Letters 26 (2005), 1577-1586.
[2] H. C. Andrews and C. L. Patterson, “Singular value decompositions and digital image processing” ,IEEE Trans. on Acoustics, Speech, and Signal Processing, vol. ASSP-24, pp. 26–53, 1976.
[3] K. Konstantinides, B. Natarajan, and G.S. Yovanof, “Noise Estimation and Filtering Using Block-Based Singular Value Decomposition,” IEEE Trans. Image

Processing, vol. 6, pp. 479- 483, March 1997.

[4] V.I. Gorodetski, L.J. Popyack, V. Samoilov, and V.A. Skormin, "SVDBased Approach to Transparent Embedding Data into Digital Images," Proc. Int. Workshop on Mathematical Methods, models and Architecture for Computer Network Security, Lecture Notes in Computer Science, vol. 2052, Springer Verlag, 2001.

[5] Dobrovolny M. Šilar Z., Černy M.,"Asymmetric Image Compression for Embedded Devices based on Singular Value Decomposition", IEEE Applied Electronics Pilsen, 2011.

[6] Singh, S.K., Kumar, S. " A Framework to Design Novel SVD Based Color Image Compression, Computer Modeling and Simulation", 2009. EMS '09, Third European Symposium, Athens 2010

[7] A. Shnayderman, A. Gusev and A. M. Eskicioglu, " A Multidimensional Image Quality Measure Using Singular Value Decomposition," IS&T/SPIE Symposium on Electronic Imaging 2004, Image Quality and System Performance, San Jose, CA, January 18-22, 2004.

[8] Ganic, N. Zubair, and A.M. Eskicioglu, "An Optimal Watermarking Scheme based on Singular Value Decomposition", Proceedings of the IASTED International Conference on Communication, Network, and Information Security (CNIS 2003), pp. 85-90, Uniondale, NY, December 10-12, 2003

[9] Rowayda A. Sadek, "Blind Synthesis Attack on SVD Based watermarking Techniques", International Conference on Computational Intelligence for Modeling, Control and Automation - CIMCA'2008.

[10] J. Bigun, G. H. Granlund, and J. Wiklund, "Multidimensional orientation estimation with applications to texture analysis and optical flow", IEEE Transactions on Pattern Analysis and Machine Intelligence 13(8) (1991), 775–790.

[11] H. Demirel, G. Anbarjafari, and C. Ozcinar, "Satellite Image Contrast Enhancement using Discrete Wavelet Transform and Singular Value Decomposition", IEEE Geoscience and Remote Sensing Letters, vol. 7, no. 2, pp. 334-338, Apr. 2010.

[12] R. Liu and T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE Transaction on Multimedia, 4(1), pp.121-128, March 2002

[13] D. V. S. Chandra, "Digital Image Watermarking Using Singular Value Decomposition", Proceeding of 45th IEEE Midwest Symposium on Circuits And Systems, pp. 264-267, Tulsa, OK, August 2002.

[14] Kuo-Liang Chung, C. Shen, L. Chang, "A novel SVD- and VQ-based image hiding scheme", Pattern Recognition Letters, 2002,1051-1058

[15] Andrews, H.C., Patterson, C.L., 1976. "Singular value decomposition (SVD) image coding",IEEE Trans. Comm. COM-24, 425–432.