A FAST AND ROBUST HYBRID WATERMARKING SCHEME BASED ON SCHUR AND SVD TRANSFORM

K.Meenakshi[1], Ch. Srinivasa Rao[2], K. Satya Prasad[3]

[1]Research scholar, ECE Dept., JNTUCE, Kakinada, A.P, India
[2]Professor of ECE, JNTUCE, Vizayanagaram, A.P, India
[3]Professor, ECE Dept, JNTUCE, Kakinada, A.P, India

Abstract

This paper presents a robust watermarking for still digital images based on schur factorization and Singular Value Decomposition (SVD). In this paper, image is decomposed into 8×8 blocks and after applying schur factorization, the stable largest eigen values of the upper triangle is used as robust locations for embedding watermark. The matrix array formed by largest eigen values further factorized by Singular Value Decomposition and singular values of these coefficients are modified with the singular values of watermark. Later inverse SVD and inverse schur is applied to get watermarked image. The watermark is subjected to checkmark watermarking evaluation software and it is found that the method is robust against number of attacks and highly imperceptible.

Keywords – *Schur factorization, Singular Value Decomposition, Peak signal to noise ratio, CC.*

--***--

1. INTRODUCTION

With the rapid development of internet and multimedia, digital data has become vulnerable to piracy at an alarming proportion, which is a major concern to the multimedia industry in general and the audio and video industry in particular. In order to prevent the illegal copying and distribution of multimedia documents such as audio, image and video, several methods were proposed. An attractive method is the process of embedding hidden information or logo into the multimedia document known as Digital watermarking. This logo is extracted from or detected for security purposes and for claiming the ownership. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity Invisibility refers to the distortion, introduced by the watermark should be negligible and there must be no distinction between watermarked and host image when viewed by third person. Robustness is the resistance of an embedded watermark against intentional and unintentional attacks such as noise, filtering, blurring, sharpening, resampling, scaling, rotation, cropping, and JPEG lossy compression. Watermarking techniques are broadly classified into two domains-Spatial domain and transform domain. In spatial domain watermark is directly embedded by modifying pixels in the image. Example is concealing logo in least significant bit position. But these techniques suffer from vulnerability due to intentional and unintentional attacks. An alternative is transform domain technique; it uses transforms like Discrete Wavelet Transform (DWT) [3], Singular Value Decomposition (SVD) [7] and (Discrete Fourier Transform (DFT)[2] and Contourlet transform (CT) (10) to convert image from spatial domain to frequency domain. The watermark is embedded in transform coefficients and later inverse transform is used to get watermarked image. These techniques are found to be superior compared to spatial domain. In this domain, one can insert watermark in least perpetually significant transform coefficients. Watermark can be redistributed over different bands of transform coefficients. This will improve the imperceptibility of the watermark and lead to less visual degradation of watermarked image. Beside, the watermark is distributed unevenly, so it is highly difficult for the hacker to remove watermark. Recently in Ref. [9] schur transform is used along with CT and SVD. The LL band of original image after CT is factorized using SVD and that of watermark after CT are decomposed by Schur Factorization. The schur form of watermark is further factorized using SVD. The modified coefficients of singular values of watermark are embedded in the singular values of original image followed by inverse SVD and inverse CT are used to obtain watermarked image. The experimental results show that the scheme is resistant against signal processing attacks such as median filtering, salt and pepper noise, Gaussian noise, compression and geometric attacks.

In ref [8] watermarked image is obtained by adding the triangular matrix of the mark obtained after the Schur decomposition to the DCT transform of the host image. They proved the watermarking technique achieves high capacity. The unitary matrix acts as secret key for the extraction of the watermark. The results show that this scheme is robust against attacks such as JPEG compression, colors reducing, adding noise, filtering, cropping, low rotations, and histogram spreading. In ref [5, 6] the authors point schur is a fast transform and robust to many attacks. They embedded watermark in host image using quantization index modulation and quantization index modulus modulation. They proved their method robust against rotation, low pass filtering, median filtering, resizing, salt & pepper noise. In SVD [7] singular values of original image is modified with singular values of watermark to obtain watermarked image . Later inverse SVD is used for extracting original watermark. In Ref. [11] two new properties of SVD on images are derived. The first property utilizes the quantitative relationship between singular values and power spectrum. The second property proves that under the condition of losing equal power spectrum, the square-error of the reconstructed image is much smaller when we reduce all singular values proportionally instead of neglect the smaller ones. Based on the two properties, a new data-hiding scheme is proposed. It performs well as for robustness, for it satisfies power-spectrum condition (PSC), and PSC-compliant watermarks are proven to be most robust. Besides, the proposed scheme has a good performance as for capacity and adaptability.

The paper is organized as follows: The properties of SVD and Schur transform are described in section ii. The watermark embedding and extraction using proposed method is described in Section iii. Simulation results and observations are presented in section iv. Conclusion is given in section v.

2. METHODOLOGY

The proposed watermarking technique employs the hybrid transforms of schur and SVD. A brief introduction of two transforms is given below.

Singular Value Decomposition is a mathematical tool widely used in image compression, retrieval and watermarking. According to it, every real matrix *A* can be decomposed into a product of three matrices,

$$A=U\Sigma V^T \qquad (1)$$

If A is represented in matrix format:

$$\begin{bmatrix} u_{1,} & u_{2,} & u_N \end{bmatrix} \times \begin{bmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & . & 0 \\ 0 & 0 & 0 & \lambda r \end{bmatrix} \times \begin{bmatrix} v_1 & v_2 & . & v_N \end{bmatrix}^T \qquad (2)$$

The Singular Value Decomposition (SVD) of A can be written as

$$A=\lambda_1 U_1 V_1 + \lambda_2 U_2 V_2 + ...\lambda_r U_r V_r \qquad (3)$$

Where r is the rank of A (r <=N). The singular values above rank r are zero. *U* and *V* are orthogonal matrices, satisfying the condition $U^T U= I$, $V^T V = I$, and Σ = diag (λ1, λ2, ...). 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*.

In SVD, singular values represent the luminance of the image layer and singular vectors represent the geometry of the image. The main advantage of the SVD is the largest singular values preserve most of the energy and are resistant to small perturbations and there by immune to most of the signal processing and image compression operations.[7]

Properties of Singular Value Decomposition:

1. **Stability**: The SVs have a strong stability since the variation of both original and disturbed SVs cannot exceed 2-norm of the difference between the original and modified matrices.

2. **Invariance to geometric distortions**: The SVD exhibits the geometric invariance can be expressed in:

3. Translational invariance: Both the matrix A and its translated counterpart has same singular values.

4. Scaling invariance: if $A\max$ has singular values $S_{i,} 1 \le i \le p$, then its scaled counterpart A^S has singular values is equal to $S_i \sqrt{F_r F_S}$ where Fr and F_S are the scaling factors of rows and columns respectively.

5. Flip invariance: Both the matrix A and its flipped counterparts have same singular values.

6. Transposition: Both matrix A and its transpose have same singular values.

The main advantage of Singular Value Decomposition is it is more resistant to scaling, translation and rotation attacks.

Schur transform: Given a square matrix A, if it has full rank of linearly independent Eigen vectors, there exists an invertible matrix P, such that $P^{-1}AP = \Lambda$, where Λ is a diagonal matrix. But all square matrices are not diagonalizable. This deficiency can be mitigated by schur factorization or QR factorization .According to schur every invertible matrix may be expressed as a product of unitary matrix U and upper triangle matrix T, $T = U^H AU$. In matrix T, the diagonal entries of T are the Eigen values of A. This decomposition refers to the structure of the matrix.

3. PROPOSED ALGORITHM

3.1 Watermark Embedding

1 .Decompose image A into non overlapping blocks of 8×8.

2. Apply schur transform to the image. It decomposes image into unitary transform U and upper triangle matrix T. The diagonal entries are Eigen values of each block. In image eigen values preserve most of the energy.

3 .By using HEBS (High Eigen value Block selection) largest eigen value of each block is selected and a matrix array formed equal to the size of watermark and denoted as B.

4. Apply singular value Decomposition to the coefficients selected based on HEBS. It decomposes into U_C ,S_C and V_C .

5. Apply SVD to watermark. It decomposed into U_W , S_W and V_W .

6. Modify singular values of original image with singular values of watermark. The singular values of S_C and S_W are λ_C and λ_w . Obtain.

$$\lambda_{watermark} = \lambda_C + \frac{alpha \times \lambda_W}{L\max} \quad (4)$$

Where $L_{\max}$ is the largest singular value of watermark.

7. Apply singular values of watermark by taking diagonal of $\lambda_{watermark}$.

8. Apply inverse SVD to obtain B'.

$$B' = U_C \times S_{watermark} \times V_C^T \quad (5)$$

9. Remap B' into largest Eigen values of the triangular matrix of SCHUR matrix denoted by T'.

10. Apply inverse schur transform.

$$A' = U \times T' \times U^T \quad (6)$$

11. Merge all 8×8 blocks to form watermarked image.

Fig.1.a)Original Lena b)Watermarked Lena with P.S.N.R=65.88

3.2. Watermark Extraction

1. Segment watermarked image into non overlapping blocks of 8×8.

2. For each 8×8 .block apply schur transform. Extract the matrix containing largest Eigen value from the blocks where watermark is embedded B''.

3. Apply SVD to B''.

It decomposes into U_{WA} , S_{WA} and V_{WA}.

4. The diagonal entries of S_{WA} are singular values λ_{WA}.

5. Repeat the above steps 1-4 to original image. The singular values of original image are λ_C .

6. Extract singular values of Watermark

$$\lambda_{ext} = \frac{(\lambda_{WA} - \lambda_C)}{alpha} \times L\max \quad (7)$$

7. Obtain S_{ext} from λ_{ext}

8. Obtain inverse Singular value Decomposition to obtain extracted watermark.

$$B' = U_W \times S_{ext} \times V_W^T \quad (8)$$

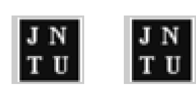


Fig.2. Original Logo and extracted Logo.

4. EXPERIMENTAL RESULTS

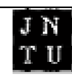
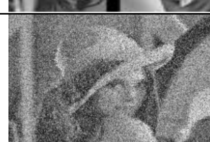
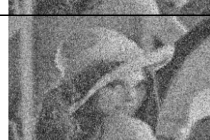
Imperceptibility is an important factor used in watermarking. PSNR is a measure of transparency.

$$PSNR = 20\log_{10}\left(\frac{Max_i}{\sqrt{MSE}}\right) \quad (9)$$

Table1: Peak signal to noise ratio

Transform	SVD	SCHUR	Proposed Method
Size of cover image	512×512	512×512	512×512
Size of watermark	32×32	32×32	32×32
Peak signal to noise ratio	39.12	55.23	65.123

Table 2: Attack, Attacked watermarked image, Extracted watermark and its corresponding cross correlation coefficient.

Attack	Attacked watermarked image	Extracted Watermark	Correlation Coefficient
Contrast Enhancement			0.9100
imresize			0.9040
Sharpening			0.8588
Histogram Equilization			0.8280
Rows and columns removal			-0.8970
DPR attack			.714
DPR_Corr attack			0.712
Frequency mode Laplacian removal			0.785

Where MSE is mean squared error between the cover frame F and the watermarked frame $\overline{F}$.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{J=1}^{N}\left|F_{ij} - \overline{F}_{ij}\right|^{2} \quad (10)$$

The watermark similarity measure is necessary to provide the judgment of robustness of watermark. Therefore, a qualitative measure used is cross correlation (CC) .

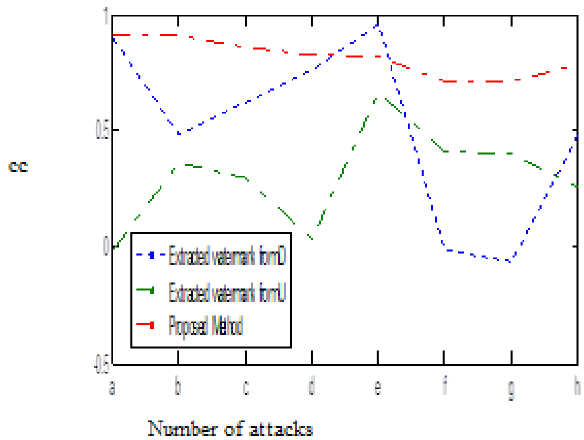


Fig 3 Robustness of proposed method compared with method in Ref. [6], extracted watermark from D and U matrix of schur Decomposition. (a) Contrast Enhancement (b) imresizing (c) sharpening (d) Histogram Equilization(e) Row column removal (f)DPR attack (g) DPR corr Attack . (h) Frequency mode Laplacian removal.

The experimental results show that the proposed method is providing high level of imperceptibility and robust to number of attacks.

REFERENCES

[1]. Hsu, C. T., & Wu, J. L. (1999). Hidden digital watermarks in images. *IEEE Transactions on Image Processing*, *8*(1), 58–68.

[2]. .Hernandez, M. Amado, F. Perez-Gonzalez, DCT-domain watermarking techniques for still images- Detector performance analysis and a new structure, IEEE Trans. Image Process, Vol. 9 (1), pp. 55–68, Jan, 2000.

[3]. M. Barni, F. Bartolini, and A. Piva, "Improved wavelet-based watermarking through pixel-wise masking," IEEE Transactions on Image Processing, vol. 10, no. 5, pp. 783–791, 2001.

[4]. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Phase watermarking of images", IEEE International Conference on Image Processing, Lausanne, Switzerland, September 1996.

[5]. B.Chandra Mohan and K.Veera Swamy" On the use of Schur Decomposition for Copyright Protection of Digital Images, International Journal of Computer and Electrical Engineering, Vol. 2, No. 4, August, 2010
1793-8163.[

[6]. B.Chandra Mohan and K.Veera Swamy, **,S.**Srinivasa **Kumar"** A Comparative performance evaluation of SVD and Schur Decompositions for Image Watermarking "International Conference on VLSI, Communication & Instrumentation (ICVCI) 2011 Proceedings published by International Journal of Computer Applications® (IJCA)

[7].Yongdong, Wu, 2005. On the Security of an SVD based ownership watermarking. IEEE transactions on Multimedia, vol 7. no.4.

[8]. Henri Bruno Razafindradina, Nicolas Raft Razafindrakoto, Paul Auguste Randriamitantsoa "Improved Watermarking Scheme Using Discrete Cosine Transform and Schur Decomposition ",IJCSN International Journal of Computer Science and Network, Volume 2, Issue 4, August 2013 .

[9]. Liu, P., Yang, J., Wei, J., Chen, F.: A Novel Watermarking Scheme in Contourlet Domain Based on Schur Factorization. In: International Conference on Information Engineering and Computer Sciences, pp. 1–4 (2010).

[10]. Yun-xia, Hong-bin zhang "Two properties of SVD and its applications in data hiding,"Advanced Intelligent Computing Theories and Applications. With Aspects of Theoretical and Methodological Issues