A Semi-Blind Self Reference Color Image Watermarking using Singular Value Decomposition

R. V. Phani Sirisha
M.Tech (DECS)
Department of ECE
Vishnu Institute of Technology

G. Prasanna Kumar
Assistant Professor
Department of ECE
Vishnu institute of technology

P. Satyanarayana Murty
Professor
Department of ECE
Vishnu institute of technology

ABSTRACT
Digital multi-media data can easily be replicated and distributed. The rapid proliferation of internet raised concerns from content owners in terms of providing protection to their digital data. Image watermarking techniques are deployed to achieve these goals. In this paper, a more secured and novel color image watermarking scheme is proposed based on Singular value Decomposition (SVD). At first host image is partitioned into blocks of size p×p then found edges in each block by using various edge detection algorithms. A reference image is formed from the essential blocks whose values are less than or equal to the threshold. Embedding is done by modifying the U and V components of the reference image using U and V components of the watermark image. Segmentation of modified reference image is done and these segmented blocks are placed in their original positions to form a watermarked image. The watermarked reference image is formed from the positions of the selected blocks of watermarked image for extraction. The reverse process is executed to extract the singular values of the watermark from the watermarked reference image at hand. Analysis and experimental results are showing that the proposed algorithm is performed well and is examined against various attacks to verify robustness.

Keywords
Digital image watermarking, Singular Value Decomposition, PSNR, Robustness.

1. INTRODUCTION
Rapid developments in the field of digital multi-media technology have increased the popularity of image-based applications. Simultaneously this technical advancement also resulted in unauthorized copying, distribution or modification of digital images. So the protection of digital multimedia content has become an increasingly important issue for content owners and service providers. As watermarking is identified as a major technology to achieve copyright protection, the relevant literature [1-2] includes several distinct approaches for embedding data into a multimedia element. Watermarking, is the process of embedding data into a multimedia cover, and can be used primarily for copyright protection and other purposes. Watermarking schemes are classified into two type's namely spatial domain watermarking schemes and transform domain watermarking schemes. Spatial watermarking schemes are easy to implement, but not robust against various attacks [3-9]. With the aim of obtaining better imperceptibility as well as robustness, embedding of watermark is done in the transform domain. Many digital watermarking schemes have been proposed for copyright protection. Most existing watermarking algorithms focus mainly on embedding watermarks into gray scale images in spatial or frequency domain. The extension to color images is usually accomplished by marking the image luminance component or by processing each color channel separately [10-14].

The rest of the paper is organized as follows. SVD transformation is discussed in section 2. Proposed algorithm is elaborated in section 3. Experimental results are given in section 4. Concluding remarks are given in section 5.

2. SINGULAR VALUE DECOMPOSITION (SVD)
SVD is an important factorization of a rectangular real or complex matrix, with many applications in signal processing and statistics. It is a numerical technique for diagonalizing matrices in which the transformed domain consists of basis states that is optimal in some sense [15-17]. Applications which employ the SVD include computing the pseudo inverse, least squares fitting of data, matrix approximation, and determining the rank, range and null space of a matrix. SVD has also been used in several watermarking algorithms. The SVD of an N x N matrix M is defined by the operation: $M=USV^*$ where U and V are unitary matrices, * denotes the transpose and S is a diagonal matrix. The diagonal entries of S are called the singular values of M and are assumed to be arranged in decreasing order $\sigma_i > \sigma_{i+1}$. The columns of the U matrix are called the left singular vectors while the columns of the V matrix are called the right singular vectors of M. Each singular value σ_i specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer [18-21].

Let us assume that P is an N × N square matrix with rank r, r ≤ N. The SVD of P is represented as

$$P = USV^T = \begin{bmatrix} U_{1,1} & \cdots & U_{1,N} \\ U_{2,1} & \cdots & U_{2,N} \\ \vdots & \ddots & \vdots \\ U_{N,1} & \cdots & U_{N,N} \end{bmatrix} \begin{bmatrix} S_1 & 0 & \cdots & 0 \\ 0 & S_2 & \cdots & 0 \\ \vdots & 0 & \cdots & \vdots \\ 0 & 0 & \cdots & S_N \end{bmatrix} \begin{bmatrix} V_{1,1} & \cdots & V_{1,N} \\ V_{2,1} & \cdots & V_{2,N} \\ \vdots & \ddots & \vdots \\ V_{N,1} & \cdots & V_{N,N} \end{bmatrix}$$

Where U and V are N×N orthogonal matrices and S is an N×N singular, Diagonal matrix with diagonal entries Si's(singular values) satisfying $S1 \geq S2 \geq S3 \geq \ldots\ldots Sr > Sr+1 = \ldots\ldots SN = 0$.

3. PROPOSED ALGORITHM
3.1. Watermark Embedding Procedure
Consider an original rgb image of size N×N, is denoted by **F**. convert the RGB values to the YCbCr color space. Each row in YCbCr represents the equivalent color to the corresponding row in the RGB color map. Then Y space is divided into a number of blocks of size p×p. Edges in each block are found by using a canny edge detection algorithm. Arrange the number of edges containing in each block into ascending or descending order and select a threshold. By using this threshold form a reference image of size n×n, where

the selection of the block is done by selecting the blocks which are less than or equal to the threshold. These blocks are called significant blocks and are used to form a reference image.

Step1: The reference image is denoted by F_{ref}.

Step2: Apply SVD to F_{ref} and is denoted by F_{ref}^{U} , F_{ref}^{S} and F_{ref}^{V} respectively.

Step3: The watermark F_W is exposed to the SVD. The resultant matrices are denoted by F_W^U, F_W^S and F_W^V respectively.

Step4: Modify the U and V values of the reference image with the U and V values of watermark image to embed the watermark.

$$S_W^U = F_{ref}^U + \beta * F_W^U \quad (1)$$

$$S_W^V = F_{ref}^V + \beta * F_W^V \quad (2)$$

Step5: Find the inverse SVD and denoted by

$$F_{ref}^{ISVD} = S_W^U * F_W^S * S_W^{V^T} \quad (3)$$

Step6: Divide F_{ref}^{ISVD} into blocks of size p×p and rearrange these blocks into their original positions to form the watermarked image and is represented by F^*.

3.2. Watermark Extraction Procedure

Step 1: Divide the Y space of watermarked image F^* into blocks of size p×p.

Step 2: Find the significant blocks and form a reference image which is denoted by F_{ref}^*.

Step 3: Apply SVD transformation to F_{ref}^*. The resulting matrices are denoted by F_{ref}^{*U}, F_{ref}^{*S} and F_{ref}^{*V} respectively.

Step 4: Extract the watermark by using the following equations

$$S_W^{*U} = \left(F_{ref}^{*U} - F_{ref}^U\right)/\beta \quad (4)$$

$$S_W^{*V} = \left(F_{ref}^{*V} - F_{ref}^V\right)/\beta \quad (5)$$

Step 5: Find the inverse SVD and is denoted by

$$F_W^{*U} = S_W^{*U} * F_W^S * S_W^{V^T} \quad (6)$$

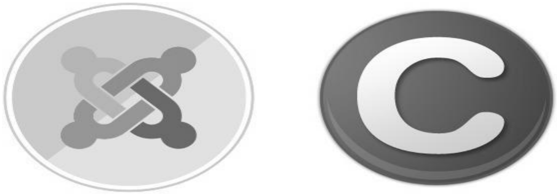
4. EXPERIMENTAL RESULTS

In order to explore the performance of the proposed watermarking algorithm, MATLAB platform is used. The watermark embedding and extraction is done for Peppers and Mandrill images. RGB images of size 512×512 are used as the cover images. Logo and Copyright gray scale images are used as two watermark images of size 256×256. Fig 1(a) and 1(b) show cover images of size 512×512. Fig 2(a) and 2(b) show watermark images of size 256×256.

The standard of the watermarked image is assessed by the parameter called Peak Signal to Noise Ratio (PSNR) and the robustness of the extracted watermark is evaluated by the quantitative indices such as Normalized Cross Correlation Coefficient (NCC) and Bit Error Rate (BER). In order to judge the difference between cover image and watermarked image, Mean square error (MSE) is used. Peak Signal to Noise Ratio (PSNR) is used to estimate the watermark imperceptibility and is given in equation (7).

(a) Peppers image **(b) Mandrill image**

Fig 1. Cover Images



(c) Logo image **(d) Copyright image**

Fig 2. Watermark Images

Fig 3. Watermarked Images

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (7)$$

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[x(i,j) - y(i,j)]^2 \quad (8)$$

Where x (i, j) and y (i, j) represent the pixel value of the original and the watermarked image respectively. Higher the value of PSNR more will be the quality of watermarked image which resembles the original image. The similarity between the original watermark and the extracted watermark is verified by using NCC and is given in equation (9). The value of NCC lies in between [-1 1].

$$\mathbf{NCC} = \left[\frac{\sum_{i=0}^{M-1}\sum_{j=0}^{-1N}[W(i,j) \quad W^1 \quad (i,j)]}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[W(i,j)]^2}\right] \quad (9)$$

The detection performance of watermarking is measured by the bit error rate (BER). It is a dimensionless measure and is defined as the number of received bits that are altered during transmission through the channel divided by the total number of transferred bits during a given time interval.

With the aim of improving capacity and invisibility, K.L Chung et.al [23] proposed two important notes based on the properties of the various components of SVD. Instead of embedding watermark in only U-component proposed by Chang et.al [22], Chung proposed an algorithm to embed watermark in both U and V components of SVD. Comparison of PSNR performance between Chung et.al [23] and proposed methods is clearly elaborated in Table.1. The subscripts U and UV in the first column of Table.2 represent that the watermark is embedded into U component only and into both U and V components of the original image, respectively.

According to the proposed algorithm PSNR is improved on comparison with Chung et al. [23] method.

Table 1.Comparison of PSNR performance

Images	Chung et.al [23] method for T=0.012	Proposed method(256 column of U component and 256 row of V^T components)
Lena $_U$	45.38	**52.03**
Lena $_{UV}$	43.59	**50.43**
Peppers $_U$	44.65	**52.21**
Peppers $_{UV}$	43.05	**52.03**

The watermarked image quality is measured by using PSNR. Watermarked images of both Peppers and Mandrill images are shown in Fig.3. No perceptual degradation is observed between the original image and the watermarked image. PSNR, NCC and BER values of watermarked Peppers image are tabulated in Table.2.

According to the proposed algorithm, modification in first column of U-component and first row of V^T components, results in more distortion of image quality so low PSNR of value 24.36dB is observed for Peppers image. Due to this fact, BER of value 1 is achieved. On moving from the first column to the remaining columns of U-component from left to right and first row to the remaining rows of V^T component from top to bottom, less distortion of image quality is observed so that PSNR increases to 52.20dB and BER of value 0 is achieved. This is observed for column 256 of U-component and row 256 of V^T components in Table.2.

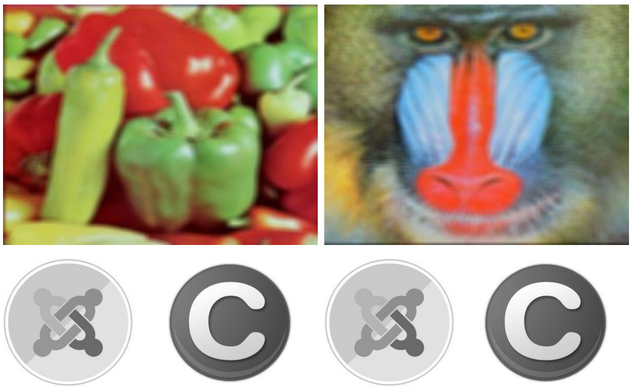
Table 2. PSNR, NCC and BER values of Peppers image by modifying different columns and rows of U and V^T components respectively

Embedding Column in U and Row in V^T components	Performance Measures				
	PSNR (dB)	NCC		BER	
		U	V	U	V
1,1	24.36	0.3643	0.9213	1.0000	0.0039
32,32	52.04	0.9996	0.9381	0.4050	0.0039
64,64	52.19	0.9999	0.9465	0.0910	0.0038
128,128	52.20	1.0000	0.9502	0.0201	0.0038
256,256	52.20	1.0000	1.0000	0	0

To examine the robustness of the proposed watermarking algorithm, the watermarked image is attacked by a variety of attacks, namely Average and Median filtering, Gaussian Noise addition, JPEG compression, Rotation, Cropping, Resizing, Histogram Equalization, Sharpening, Contrast adjustment and Pixilation. The extracted watermark images are compared with the original watermark images after these attacks are performed on watermarked images and the results are tabulated in Table.3.

4.1. Filtering

The most common manipulation on digital image is filtering. In image processing to combat high frequency noise in an image, median filtering operation is frequently used. For median filtering, 13×13 mask is used. It conserves edges edges while removing noise. The extracted watermarks, after applying 13×13 averaging and median filtering are shown in Figures.4 & 5. It is observed that after applying filtering attack, images are not degraded and the extracted watermarks from U and V-components are recognizable.



U-1.0000 V-1.0000 U-1.0000 V-1.0000

Fig 4 : Average Filtering attack on Watermarked Images (Top) and Extracted Watermarks from U and V

4.2. Addition of noise

Addition of Gaussian noise to the watermarked image is used for the distortion and degradation of the image and results in complexity of watermark extraction. Fig.6 shows the watermarked image and extracted watermarks.

4.3 JPEG compression

To verify the robustness against image compression, the watermarked image is tested with 80:1 JPEG compression attacks and the extracted watermarks are shown in Fig.7.

4.4. Rotation

Rotation attack is among the most popular kinds of geometrical attack. The rotation is used to realign horizontal features of an image. Rotation is tested by rotating the image in 60 degrees direction. Fig.8 shows the watermarked image and extracted watermark images.

4.5. Cropping

Image cropping is one of the most commonly used geometrical attacks on digital multimedia images. For this to be done, 50% of the watermarked image is cropped and then a watermark is extracted. The extracted watermark images from the cropped watermarked image are as shown in Fig.9.

4.6. Resize

To fit the image into desired size, expansion or reduction is a commonly used operation in image processing. It is referred as resizing attack. Results are shown in Fig.10.

4.7. Histogram Equalization

Histogram equalization is the process in which intensity of the pixels are reassigned in such a way that all the values available for assigning a gray level are utilized. This technique is generally used to enhance the image, so it can be an attack for the image watermark. Fig 11 shows watermarked images after histogram equalization and their extracted watermarks.

4.8. Sharpening

To improve the individual quality of an image, sharpening operations are used. A sharp image includes small components, the fine detail, down to the limit of vision. Fig.12 shows the watermarked image and the extracted watermarks.

U-1.0000 V-.1.0000 U-1.0000 V-1.0000

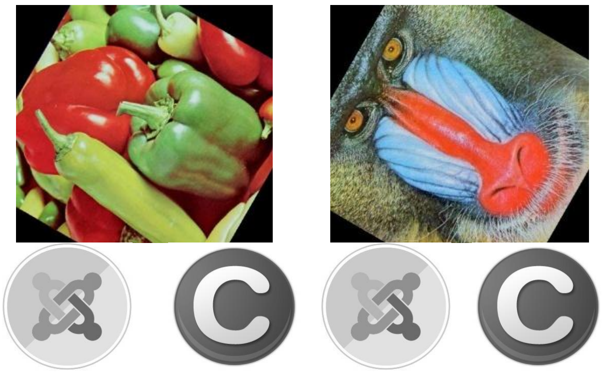
Fig 6 : Gaussian noise attack on Watermarked Images (Top) and Extracted Watermarks from U and V

4.9. Contrast adjustment

Contrast adjustment is one of the signal processing attack. Fig 13 shows watermarked images after contrast adjustment and their extracted watermarks.

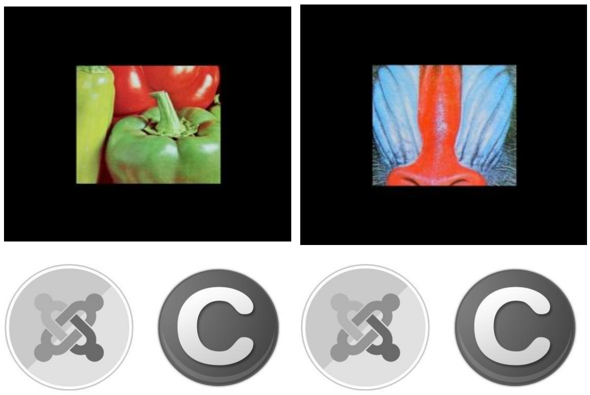
U-1.0000 V-.1.0000 U-1.0000 V-1.0000

Fig 7 : Compression attack on Watermarked Images (Top) and Extracted Watermarks from U and V



U-1.0000 V-.1.0000 U-1.0000 V-1.0000

Fig 8 : Rotation attack on Watermarked Images (Top) and Extracted Watermarks from U and V



U-1.0000 V-.1.0000 U-1.0000 V-1.0000

Fig 9 : Cropping attack on Watermarked Images (Top) and Extracted Watermarks from U and V

U-1.0000 V-.1.0000 U-1.0000 V-1.0000

Fig 10 : Resizing attack on Watermarked Images (Top) and Extracted Watermarks from U and V

4.10. Pixilation:

Pixilation is the display of a digitized image where the individual pixels are apparent to a viewer. Results are shown in Fig.14.

U-1.0000 V-1.0000 U-1.0000 V-1.0000

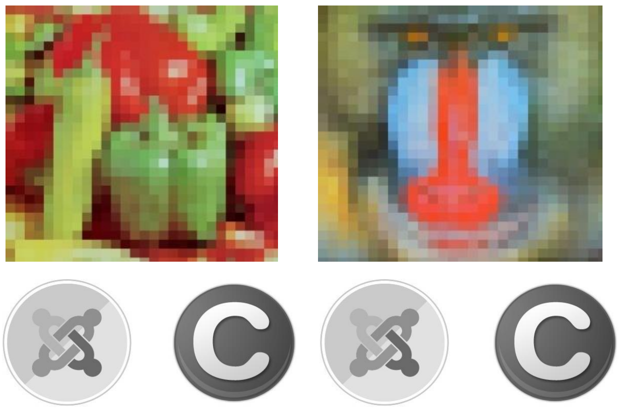
Fig 11 : Histogram Equalization attack on Watermarked Images (Top) and Extracted Watermarks from U and V

U-1.0000 V-.1.0000 U-1.0000 V-1.0000

Figure 12 : Sharpening attack on Watermarked Images (Top) and Extracted Watermarks from U and V

U-1.0000 V-.1.0000 U-1.0000 V-1.0000

Figure 13 : Contrast adjustment attack on Watermarked Images (Top) and Extracted Watermarks from U and V



U -1.0000 V-1.0000 U-1.0000 V-1.0000

Fig 14 : Pixilation attack on Watermarked Images (Top) and Extracted Watermarks from U and V

The error rate between the extracted watermark and the original watermark is used to assess the robustness of the embedded watermark. Comparison of BER between Chang et al. [22], Chung et al. [23] and the proposed method is clearly tabulated in Table.4. According to the proposed algorithm, BER of 0 is achieved.

Table 4. Comparison of Bit Error Rate (BER) after various attacks

Type of Method	**Attacked images**	**JPEG compression 70**	**Gaussian noise 3%**	**Cropping**
C C Chang et.al [22] method	Mandrill	0.0195	0.0332	0.0625
	Lena	0.0850	0.0557	0.0479
K.L Chung et.al [23] method	Lena $_{U}$	0.072	0.061	0.059
	Lena $_{V}$	0.089	0.076	0.071
	Peppers $_{U}$	0.044	0.049	0.042
	Peppers $_{V}$	0.068	0.071	0.077
Proposed method	Mandrill $_{U}$	**0**	**0**	**0**
	Mandrill $_{V}$	**0**	**0**	**0**
	Lena $_{U}$	**0**	**0**	**0**
	Lena $_{V}$	**0**	**0**	**0**
	Peppers $_{U}$	**0**	**0**	**0**
	Peppers $_{V}$	**0**	**0**	**0**

5. CONCLUSION

In this paper, a more secured and novel semi-blind self-reference digital color image watermarking scheme is presented. In this paper, the basic properties of Singular Value Decomposition (SVD) transformation are completely explored. Analysis led to the fact that the modification in rows of U-component along with the modification in columns of V^T component is given a poor imperceptibility. Excellent imperceptibility is achieved when a modification is done in columns of U-component and rows of V^T component simultaneously. Furthermore, modification in columns from left to right and rows from top to bottom is provided an excellent PSNR. In literature, there is a trade-off between PSNR and NCC. But according to the proposed algorithm, as the PSNR increases NCC is also increased. Robustness of the presented algorithm is carried out by a variety of attacks. Proposed algorithm can be hybridized with other transforms like DCT-SVD or DWT-SVD. One can use optimization techniques to improve the performance of the proposed watermarking algorithm.

6. ACKNOWLEDGEMENTS

We would like to thank the authors of [1-23] for kindly providing their essential information and would also like to thank my professors , teaching and non-teaching staff of my department for their valuable comments and suggestions which helps us to complete this work successfully.

7. REFERENCES

[1]. M. Vidyasagar, S. Han and E. Chang, "A Survey of Digital Image Watermarking Techniques," 3rd IEEE International Conference on Industrial Informatics (INDIN), Perth, Australia, pp.709-716, Aug 10 -12, 2005.

[2]. Mr.Manjunatha Prasad.R,Dr.Shivaprakash Koliwad "A Comprehensive Survey of Contemporary Researches in Watermarking for Copyright Protection of Digital Images" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.4, pp. 91–107,April 2009.

[3]. I. J. Cox, M. L. Miller, J. A. Bloom, Digital Watermarking, Academic Press,2002.

[4]. Hartung and M. Kutter, "Multimedia Watermarking Techniques," in Proceedings of the IEEE, vol. 87, no.7, pp. 1079-1107, July 1999.

[5] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd Ed. (The Morgan Kaufmann Series in Multimedia Information and Systems), 2nd ed. Morgan Kaufmann, 11 2007

[6]. M. Barni and F. Bartolini, Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. Imprint unknown, 1 2004.

[7]. Arnold M., Schmucker M., Wolthusen S.D., "Techniques and application of Digital Watermarking and Content Protection", Eds. Northwood, Artech House, 2003.

[8]. Chi-Kwong Chan , L.M. Cheng "Hiding data in images by simple LSB substitution "Pattern Recognition 37 (2004) 469– 474 , ww.elsevier.com/locate/patcog.

[9]. Dr.M.A.Dorairangaswamy "A Robust Blind Image Watermarking Scheme in Spatial Domain for Copyright Protection" International Journal of Engineering and Technology Vol. 1, No.3,August, 2009 , ISSN: 1793-8236.

[10]. M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," Journal of Electronic Imaging, vol. 7, pp. 326-332, 1998.

[11] L. Lian-Shan, L. Ren-Hou, and G. Qi, "A new watermarking method based on DWT green component of color image," in International Conference on Machine Learning and Cybernetics, vol. 6, 2004,3949-3954

[12] D. Fleet and D. Heeger, "Embedding invisible information in colorimages," in IEEE Int. Conf. on Image Processing ICIP'97, vol. 11997, pp. 532-535.

[13] M. Barni, F. Bartolini, and A. Piva, "Multichannel watermarking ofcolor images," IEEE Transactions on Circuits and Systems for Video Technology, vol. 12(3), pp. 142-156, 2002.

[14] P. Tsai, Y. C. Hu, and C. C. Chang, "A color image watermarking scheme based on color quantization," Signal Processing, pp. 95-105,2004.

[15]. Kuo_Liang Chung, Wei-Ning Yang, Young-Huai Huang, Shih_Tung Wu and Yu-Chiao Hsu " On SVD-based watermarking algorithm " Applied Mathematics and Computation 188 (2007) 54–57, Elsevier.

[16]. Digital Image Watermarking Using Singular Value Decomposition Sura Ramzi Sheriff. *Raf. J. of Comp. & Math's. , Vol. 7, No. 3, 2010* Third Scientific Conference Information Technology 2010 Nov. 29-30

[17]. AKSHYA KUMAR GUPTA, MEHUL S RAVAL " A robust and secure watermarking scheme based on singular value replacement" *Sadhan ¯ a ¯* Vol. 37, Part 4, August 2012, pp. 425–440. Indian Academy of Sciences.

[18]. V. Madhuri, K. Veera Swamy " Robust Image Watermarking using Three Domains of SVD" International Journal of Research in Computer and Communication Technology, Vol 3, Issue 11, Page 1478 -1482, November - 2014.

[19]. B.Chandra Mohan, S. Srinivas Kumar "A Robust Image Watermarking Scheme using Singular Value Decomposition "Journal of Multimedia, VOL. 3, NO. 1, pp 7-15, MAY 2008.

[20]. Alessandro Basso, Francesco Bergadano, Davide Cavagnino " A Novel Block-based Watermarking Scheme Using the SVD transform" , Algorithms 2009, 2, PP 46-75; doi:10.3390/a2010046.

[21]. Ahmad A. Mohammad, Ali Alhaj, Sameer Shaltaf " An improved SVD-based watermarking scheme for protecting rightful ownership" Signal Processing, Volume 88, Issue 9, September 2008, Pages 2158–2180- Elsevier.

[22]. C.C. Chang, P. Tsai, C.C. Lin, SVD-based digital image watermarking scheme, Pattern Recogn. Lett. 26 (2005) 1577–1586.

[23]. Chung K L,Yang W N, Y Huang, S Tung Wu and Y Chiao "On SVD-based watermarking algorithm",Applied Mathematics and Computation,2007, ELSEVIER.