A Region Adaptive Robust Watermarking Scheme Based on Homogeneity Analysis

Priyanka Singh and Suneeta Agarwal
Motilal Nehru National Institute of Technology, India

Abstract: *To counter the security breaches, came the need of watermarking which is one of the efficient methods to maintain the integrity of the digital content and prove the rightful ownership. Region adaptive watermarking is the technique which is based on the content of the image which is required to be protected against the various possible attacks. Homogeneity analysis of the image has been made using the quad tree based image segmentation method to chalk out the appropriate sites for embedding the secret information. The information is itself extracted from the image in terms of a feature which is hidden using the Singular Value Decomposition (SVD) properties in the cover image. The robustness of the proposed algorithm against the various attacks has been validated by attaining high Peak to Signal Noise Ratio (PSNR) and Normalized Cross Correlation (NCC) values in the experiments carried out.*

Keywords: *Homogeneity analysis, NCC, PSNR, quad tree, region adaptive watermarking, SVD.*

Received January 16, 2013; accepted August 29, 2013; published online October 29, 2015

1. Introduction

The accessibility to the Internet and the progress in information technologies led vast amounts of data such as images, text, video and audio to be digitized for easy storage, processing and transmission over the Internet. The advantage of accessibility came along with the disadvantage of tampering of data by the illegal means. To prevent the data from being grabbed from the Internet or tampered from unauthorized means, various approaches such as watermarking, digital signatures, copy detection etc., have been used. The original owners of digital media can embed the secret information into their works such as: Portraits, logos or trademarks by applying the watermarking approach and later on extracted these embedded logos for authorization by the real owners possessing the keys which contain the necessary confidential data to prove the ownership [21, 26, 27].

The basic classification of watermarking schemes can be done broadly into two categories: The spatial domain [2, 11, 18, 19, 25] and the frequency domain [1, 4, 5, 7, 12, 15, 16, 23]. In the spatial domain watermarking techniques, the direct modification of digital data (pixels) is done to hide the watermarks and provide the advantage of low computational complexity. However, the ability to resist the various types of signal processing attacks is usually low. The frequency domain approach requires transforming the digital data using various transform techniques like the Fast Fourier Transformation (FFT) or Discrete Wavelet Transformation (DWT) or Discrete Cosine Transformation (DCT). The properties of these transforms are thereby utilized to maintain the robustness and imperceptibility of the hidden watermarks into the appropriate chosen coefficients. Thereafter, the modified coefficients are inversely transformed to produce the watermarked images. The high robustness of frequency-domain watermarking techniques comes at the high computational cost.

2. Related Works

The Singular Value Decomposition (SVD) transform has been used as one of the frequency domain methods in the past few years. The basic idea behind embedding the watermark using SVs comes from the fact that changing the SVs slightly does not deteriorate the image quality significantly. Some methods embedded the watermark using the SVs of transform coefficients [9, 15, 20] while others directly used the SVs of the cover image [3, 13, 22, 24]. Some proposed non-blind schemes [9, 13, 22, 24], some semi-blind [20] while others the blind schemes [3, 15] with a specific quantization method.

A double watermarking scheme based on SVD that embedded the watermark twice was presented in [14]. The division of the cover image into smaller blocks was done in the first layer, thereby embedding a piece of the watermark into each block. The second layer treated the cover image as a single block to embed the whole watermark. The idea of considering two layers for embedding the watermark furnished the advantages of flexibility in the data capacity provided by the first layer, and additional robustness against the attacks provided by the second layer. A hybrid approach based on SVD-DCT watermarking method was presented in [17]. The DCT of the original image was taken and SVD transformation was performed on the watermark. The alteration of the DCT coefficients of original image was done to embed the singular values of the watermark. The highest possible robustness without

degrading the visual quality of the image was achieved by using the LPSNR criterion. However, the data capacity for embedding was quite low. This was eradicated in image compression watermarking scheme introduced in [8]. The cover image was divided into blocks and SVD applied to each one of them. All non-zero singular values were thereby used for embedding the watermark based on the local features of the cover image. It fetched the advantage of balancing the embedding capacity with distortion.

A SVD based splitting the original image into non-overlapping blocks and inserting the watermark into the singular vector angles of each block [6]. Each watermark bit was thereby embedded by modifying a set of singular vector angles, i.e., angles formed by the right singular vectors of each block. This approach enhanced the robustness level of the algorithm however, the imperceptibility was compromised. In this paper, a quad tree based homogeneity analysis has been proposed to embed the secret information into the singular values of the appropriate homogenous blocks that is selected using a threshold criterion. The difference between the maximum and the minimum pixel values has been defined as the test criterion. This provided the invisibility and robustness requirements simultaneously towards the appropriateness of the methodology for rightful ownership verification.

The paper is organized as follows: Basic concepts and key features of quad tree image segmentation and SVD are outlined in section 3. Section 4 gives an insight into the proposed watermarking methodology and experimental results along with analysis are given in section 5. Conclusions along with the scope of future work are drawn in section 6.

3. Brief Overview of the Concepts Used

3.1. Quad Tree Segmentation

Quad tree is a tree based structure where each node has exactly four descendants. The entire image being represented by the parent node and its four descendants representing the disjoint sub regions within the larger region. The segmentation process involves iteratively dividing the given square image into four equal sized sub square blocks, until the blocks meet the criterion. Each block is being checked for the homogeneity criteria. If it meets the criteria, it is not divided further and if it does not, it is again subdivided into four blocks, applying the test criterion to the resulting blocks generating blocks of several different sizes.

Quad tree based image segmentation splits the image into regions based on intensities of the pixels present in an image. When the intensities are uniform, large regions are formed and in the comparatively non-uniform areas of the image small regions of variable sizes are formed. Large regions signify less valuable information present in an image, the absence of edges and mainly the background area. Small regions imply the presence of the critical information present in the image and are probably good sites for embedding the watermark. The proposed homogeneity analysis based watermarking technique applies quad tree for selecting those 4×4 blocks, which pass the homogeneity test i.e., whose difference between the maximum gray values of the block elements and minimum gray value of the block elements is less than the threshold value. These 4×4 blocks are considered as the Region Of Interest (ROI) and feature extracted from these blocks has been considered as the watermark to be embedded in them, thereby providing more robustness and better copyright protection.

3.2. Singular Value Decomposition

The SVD has been applied successfully to a variety of applications, such as: pattern analysis, data compression and signal processing [13, 22]. The property of SVD that is being exploited in watermarking is that slightly changing the SVs does not perceptually affect the visual quality of the image. Even the application of the various image processing attacks doesn't change the SV values much. The SVD decomposition of any discrete image matrix A of size m×n, from the viewpoint of linear algebra can be represented as:

$$A=USV^T \quad (1)$$

Where U and V are orthogonal matrices (UU^T=I, V^TV= I) of size m×m and n×n respectively.

The columns of V and U matrices are called right and left singular vectors respectively and represent vertical and horizontal details of an image. The non-zero diagonal elements of S matrix with size mxn are called as singular values of A matrix. They represent the luminance values of the image layers produced by right and left singular vectors. The singular values are arranged in decreasing order from the first SV to the last one and so, their importance decreases in SVD based compression methods.

4. The Proposed Methodology

The proposed watermarking scheme consists mainly of two parts, watermark embedding and extraction. The homogeneity analysis of the cover image is done in the embedding process to select the appropriate regions called as ROI for embedding of watermark. The feature extracted from the image itself is being used as the watermark to be inserted, thus minimizing the storage requirements of the algorithm. The detail block diagram representation of the proposed embedding scheme is shown in Figure 1.

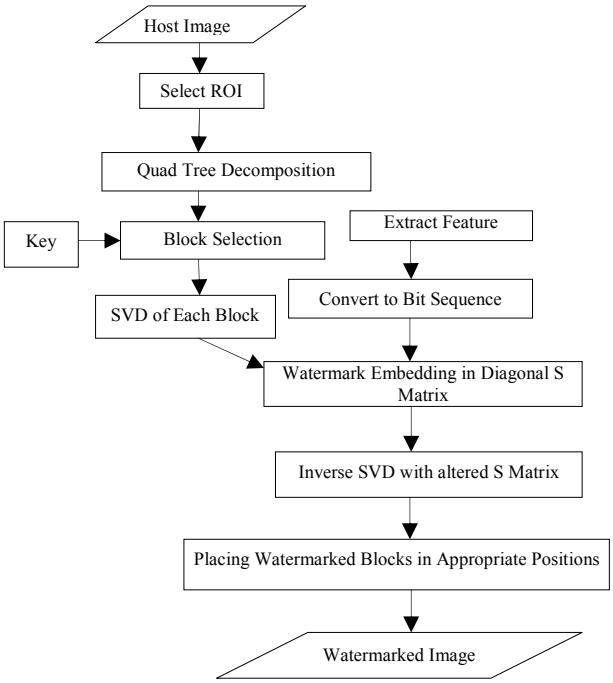

Figure 1. Watermark embedding process.

4.1. Watermark Embedding

In the embedding process, the homogeneity analysis is done on the cover image to find appropriate regions for inserting the secret information which is extracted in the form of a feature from the cover image itself. The stepwise procedure is listed in Figure 1 as follows:

- *Step* 1: Select the ROI from the cover image. The ROI is taken to be that part of the image that is most important from an application point of view and its minimum tampering is permissible like for some water related problem, the water bodies would be chosen as the ROI. The other regions like the forest, sandy regions etc., would not be of much importance and hence, not appropriate to serve as the embedding sites or the ROI. Regions important in one application may not of much significance in others. As for the vegetation study of the same area in the above example, the forest cover would serve the purpose of being the ROI not the water bodies. The ROI region is chosen as the appropriate embedding sites so that it has enhanced robustness against the various attacks and retains the commercial value of the image.
- *Step* 2: Now, the homogeneity analysis is done using the quad tree based image segmentation of the cover image setting some test criteria like the difference between the maximum and minimum gray level values in a block must be less than a threshold value. The size of the blocks may be fixed depending on the level of segmentation needed for the application. Here, we have considered blocks of 4×4 pixels from the quad tree segmentation of the cover image.
- *Step* 3: The feature is selected from these 4×4 pixels blocks in the form of a bit sequence which is formed by calculating the average value of the block and comparing it with a user defined optimum value. If the average value is more, bit is taken as 1 otherwise 0. Same process is repeated for every 4×4 pixels block to build the feature to be inserted.
- *Step* 4: Homogeneous blocks of 4×4 pixels are selected in a random fashion depending upon the secret key generated which is a random permutation of numbers from 1 to n, where n is the count of the homogenous blocks. The order of selection of the homogenous blocks will be the same as the sequence of elements in the secret key. The feature is embedded in the singular values of the blocks as these are very stable and produce minimum perceptual distortion in the visual quality of the cover image. The strategy used is quite similar to the one proposed in [10] but vary in exactly what singular values are being altered to embed the secret information. These values are arranged in decreasing order and hence, in the proposed algorithm only the third and the forth values are altered for hiding the secret bit as compared to second and third values as in [10], as it would deteriorate less the perceptual quality of the cover image. The following process is repeated until the entire feature is embedded:

  - *Step* 4.1: Compute the SVD decomposition of each block say k. It results in two orthogonal matrices U_k and V_k. They represent the left and right singular vectors and a diagonal matrix S_k whose values are arranged in decreasing order as shown below:

$$S_k = \begin{bmatrix} a_1 000 \\ 0 a_2 00 \\ 00 a_3 0 \\ 000 a_4 \end{bmatrix} \tag{2}$$

  - *Step* 4.2: The S_k matrix is a 4×4 diagonal matrix. The forth diagonal element of the matrix S_k is put equal to the third diagonal element and obtain S'_k given by:

$$S'_k = \begin{bmatrix} a_1 000 \\ 0 a_2 00 \\ 00 a_3 0 \\ 000 a'_4 \end{bmatrix} \tag{3}$$

  Where $a'_4 = a_3$

  - *Step* 4.3: Now, the third diagonal element is allotted a value equal to its previous value incremented by constant times the watermark bit and a new S''_k is obtained given by:

$$S''_k = \begin{bmatrix} a_1 000 \\ 0 a_2 00 \\ 00 a'_3 0 \\ 000 a'_4 \end{bmatrix} \tag{4}$$

Where $a'_3 = a_3 + \delta * W_k$, where δ is a constant.

- *Step* 4.4: The watermarked block BW_k is obtained by inverse transforming this new obtained S''_k value with the initially obtained U_k and V_k values of the block, as follows:

$$BW_k = U_k S''_k \quad (5)$$

- *Step* 4.5: This watermarked block is then placed in its original location with respect to the cover image.

- *Step* 5: Watermarked image is then formed after inserting the entire feature vector and placing the blocks in their corresponding positions.

4.2. Watermark Extraction

The detailed steps for the watermark extraction are described in Figure 2 as follows:

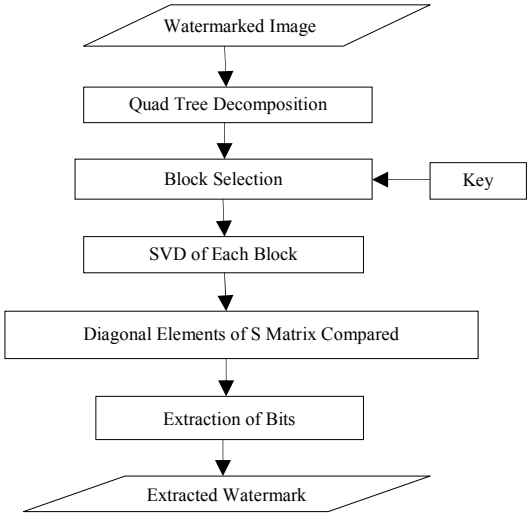

Figure 2. Watermark extraction process.

- *Step* 1: Quad tree based image segmentation is done of the watermarked image and blocks of size 4×4 are selected using the same homogeneity criteria, used at the time of embedding.
- *Step* 2: Now, select the corresponding 4×4 blocks of the segmented watermarked image (possibly distorted version of the watermarked) using the secret key generated at the time of embedding. Compute SVD of each block and obtain three matrices BU_k, BS_k and BV_k as follows:

$$BS_k = \begin{bmatrix} aw_1 000 \\ 0aw_2 00 \\ 00aw_3 0 \\ 000aw_4 \end{bmatrix} \quad (6)$$

- *Step* 3: If the difference between the third and the forth diagonal element is greater than the strength factor δ, then extracted watermark bit W_k=1 otherwise W_k=0.
- *Step* 4: Same process is repeated for each of the block to extract the bits and build up the feature hidden which is then compared with the actual feature vector to prove the ownership.

5. Experimental Results and Analysis

The performance of the proposed technique is authenticated by simulating on a wide set of color 512×512 cover images using MATLAB10 as shown in Figure 3.

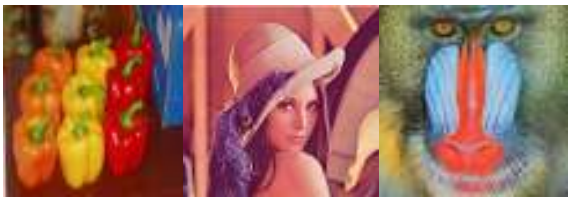

Figure 3. Set of cover images tested for watermarking.

The optimum values for the constants used in the algorithm based on a large number of experiments is as follows: the homogeneity criteria threshold value for the quad tree based image segmentation taken as 10 and the constant value being compared with the average values of the blocks to decide the bit in the extracted feature formed from the cover image taken as 61. The constant delta determining the strength of the proposed algorithm is taken as 2. The Peak Signal to Noise Ratio (PSNR) has been used as a measure to determine the imperceptibility of the watermarked image from the original image. High values indicate good indistinguishability of the watermarked image from the original cover image. The PSNR value varies with respect to two factors considered in the algorithm that is, the threshold value considered for the quad tree based segmentation of ROI of the cover image and the strength factor δ used while embedding the feature vector bits in the singular values. The variation plots are depicted in Figures 4 and 5 respectively.

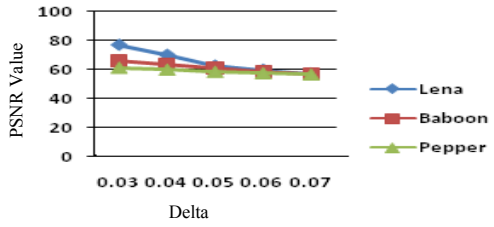

Figure 4. Variation of PSNR with threshold value.

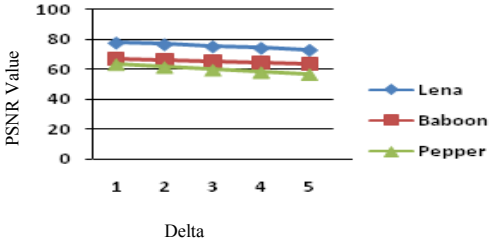

Figure 5. Variation of PSNR with delta value.

The similarity between the extracted feature vector from the watermarked image and the original calculated from the original cover image has been quantitatively measured by the Normalized Cross Correlation (NCC) value defined as follows:

$$NCC = [W_{ij} \times W'_{ij}] / [W_{ij} \times W_{ij}] \quad (7)$$

Where W_{ij} and W'_{ij} are the pixel values at the $(i, j)^{th}$ position in the original and extracted watermark.

The value of NCC ranges from 0 to 1. High values indicate good robustness against the various image processing attacks. Imperceptibility and robustness are two inverse proportionate measures and a trade-off has to be maintained between the two for the efficiency of the algorithm. The robustness of the proposed scheme has been validated by applying the various image processing attacks on the watermarked image. The Tables 1, 2 and 3 enlist the calculated normalized correlation values after the applied attacks in the experiment.

Table 1. Attacks applied on watermarked pepper image.

Attacks	NCC Value	PSNR Value
No Attack	1	61.37
Salt and Pepper Noise	0.98	38.84
Gaussian Filter	0.89	54.98
Cropping	1	61.37
Speckle Noise	0.92	42.88
Laplacian Filter	0.81	23.08
Rotation	0.79	39.28
Histogram Equalization	0.99	11.30
Resize	0.84	43.02
Median Filter	0.65	48.52
Average Filter	0.54	45.93
Wiener Filter	0.54	50.93
JPEG	0.77	53.77
Gaussian Noise	0.99	26.44

Table 2. Attacks applied on watermarked lena image.

Attacks	NCC Value	PSNR Value
No Attack	1	76.78
Salt and Pepper Noise	1	40.32
Gaussian Filter	0.70	41.38
Cropping	1	76.78
Speckle Noise	1	41.48
Laplacian Filter	0.88	12.03
Rotation	1	29.30
Histogram Equalization	1	20.91
Resize	0.88	35.07
Median Filter	0. 53	35.01
Average Filter	0.53	32.93
Wiener Filter	0.64	37.26
JPEG	1	18.81
Gaussian Noise	1	24.80

Table 3. Attacks applied on watermarked baboon image.

Attacks	NCC Value	PSNR Value
No Attack	1	66.32
Salt and Pepper Noise	0.99	39.74
Gaussian Filter	0.94	46.58
Cropping	1	66.31
Speckle Noise	0.97	38.24
Laplacian Filter	0.87	8.34
Rotation	0.83	30.43
Histogram Equalization	0.98	22.55
Resize	0.84	38.29
Median Filter	0.73	36.95
Average Filter	0.74	42.72
Wiener Filter	0.73	44.26
JPEG	0.85	50.29
Gaussian Noise	0.99	25.32

6. Conclusions

The present paper proposed a region adaptive watermarking scheme which was based on homogeneity analysis of the image to be protected against the various tampering attacks possible. The properties of quad tree based image segmentation method was utilized for finding appropriate sites for the embedding of the secret information which was extracted from the image itself in the form of a feature. The indistinguishability of the watermarked image from the original was reflected by high attainable PSNR values (upto76) for the various colored images considered in the experiments. Also, the robustness of the scheme was validated by the high NCC values against the various attacks like noises, filtering, rotating, cropping etc. The future study can be focused on making the scheme applicable to the video watermarking too and enhancing its robustness against more variety of attacks.

References

[1] Amirgholipour S. and Aboosaleh S., "A Pre-Filtering Method to Improve Watermark Detection Rate in DCT Based Watermarking," *The International Arab Journal of Information Technology*, vol. 11, no. 2, pp. 178-185, 2014.

[2] Bangaleea R. and Rughooputh H., "Effect of Channel Coding on the Performance of Spatial Watermarking for Copyright Protection," *in Proceedings of the 6th IEEE Africon Conference in Africa*, pp. 149-153, 2002.

[3] Bao P. and Ma X., "Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 15, no. 1, pp. 96-102,2005.

[4] Barni M., Bartolini F., Rosa A., and Pivaa A., "Optimum Decoding and Detection of Multiplicative Watermarks," *IEEE Transaction Signal Processing*, vol. 51, no. 4, pp. 1118-1123, 2003.

[5] Bas P., Chassery J., and Macq B., "Geometrically Invariant Watermarking using Feature Points," *IEEE Transactions on Image Processing,* vol. 11, no. 9, pp. 1014-1028, 2002.

[6] Basso A., Bergadano F., Cavagnino D., Pomponiu V., and Vernone A., "A Novel Block-Based Watermarking Scheme Using the SVD Transform," available at: mdpi.com/journal/algorithms, last visited 2009.

[7] Bovik A., Huang T., and Munson D., "Robust Wavelet-based Video Watermarking using Edge Detection," *Adv. Elect. Eng. Comp. Sci.*, 399, pp. 173-182, 2009.

[8] Calagna M., Guo H., Mancini, L., and Jajodia, S., "A Robust Watermarking System based on SVD Compression" *in Proceedings of ACM Symposium on Applied Computing,* Dijon, France, pp. 1341-1347, 2006.

[9] Chandra D., "Digital Image Watermarking using Singular Value Decomposition," *in Proceedings of the 45th Midwest Symposium on Circuits and Systems*, pp. 264-272, 2002.

[10] Chang C., Hu Y., and Lin C., "A Digital Watermarking Scheme Based on Singular Value Decomposition," *in Proceedings of the 1st International Symposium, ESCAPE 2007*, Hangzhou, China, pp. 82-93, 2007.

[11] Cox I., Killian J., Leighton F., and Shamoon T., "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transaction Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.

[12] Djurovic I., Stankovic S., and Pitas I., "Digital Watermarking in the Fractional Fourier Transformation Domain," *Journal of Network and Computer Applications*, vol. 24, no. 2, pp. 167-173, 2001.

[13] Ganic E. and Eskicioglu A., "Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," *in Proceedings of ACM Multimedia and Security Workshop* (*MM and SEC04*), pp. 166-174, 2004.

[14] Ganic E., Zubair N., and Eskicioglu A., " An Optimal Watermarking Scheme based on Singular Value Decomposition," *in Proceedings of IASTED International Conference on Communication, Network and Information Security,* New York, USA, pp. 1-6, 2003.

[15] Gorodetski V., Popyack L., and Samoilov V., "SVD Based Approach to Transparent Embedding Data into Digital Images," *in Proceedings of the International Workshop on Mathematical Methods*, *Models and Architectures for Computer Network Security*, pp. 263-274, 2001.

[16] Hsieh M., Tseng D., and Huang Y., "Hiding Digital Watermarks Using Multiresolution Wavelet Transform," *IEEE Transactions on Industrial Electronics,* vol. 48, no. 5, pp. 875-882, 2001.

[17] Huang F. and Guan Z., "A Hybrid SVD-DCT Watermarking Method based on LPSNR," *Pattern Recognition Letters*, vol. 25, no. 15, pp. 1769-1775,2004.

[18] Kim Y., and Oh I., "Watermarking Text Document Images using Edge Direction Histograms," *Pattern Recognition Letter*, vol. 25, no. 11, pp. 1243-1251, 2004.

[19] Lee C. and Lee Y., "An Adaptive Digital Image Watermarking Technique for Copyright Protection," *IEEE Transactions on Consumer Electronic*, vol. 45, no. 4, pp. 363-370, 1999.

[20] Liu R. and Tan T., "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121-128, 2002.

[21] Meerwald P. and Uhl A., "A Survey of Wavelet-Domain Watermarking Algorithms," *in Proceedings of Symposium, Electronic Imaging, Conference on Security and Watermarking of Multimedia Contents*, San Jose, USA, 2001.

[22] Quan L. and Qmgsong A., " A Combination of DCT-Based and SVD-Based Watermarking Scheme," *in Proceedings of 7th International Conference on Signal Processing*, pp. 873-876,2004.

[23] Senthi V., Bhaskar I., and Bhaskar R., "Digital Image Watermarking using Edge Detection and Wavelets with Robustness Analysis against JPEG Compression Attacks," *in Proceedings of International Conference on Innovations in Information Technology*, Al Ain, pp. 583-587, 2008.

[24] Sverdlov A., Dexter S., and Eskicioglu A., "Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in All Frequencies," available at: http://kilyos.ee.bilkent.edu.tr/~signal/defevent/papers/cr1023.pdf, last visited 2005.

[25] Tsekeridou S., Nikolaidis N., Sidiropoulos N., and Pitas I., "Copyright Protection of Still Images using Self-Similar Chaotic Watermarks," *in Proceedings of IEEE International Conference on Image Processing*, Vancouver, pp. 411-414, 2000.

[26] Wong P. and Memon N., "Secret and Public Key Image Watermarking Schemes for image Authentication and Ownership Verification," *IEEE Transactions on Image Processing*, vol. 10, no. 10, pp. 1593-1600, 2001.

[27] Wu M. and Liu B., "Data hiding in image and Video. I. Fundamental Issues and Solutions," *IEEE Transaction Image Process*, vol. 12, no. 6, pp. 685-695, 2003.

Priyanka Singh received BTech degree from HBTI, Kanpur, MTech degree from MNNIT, Allahabad and presently pursuing PhD from MNNIT, Allahabad. Her areas of interests include digital watermarking, visual cryptography, and security related concepts.

Suneeta Agarwal received PhD degree from IIT, Kanpur is Head of Department of Computer Science and Engineering Department in MNNIT, Allahabad and professor at the same. She has numerous contributions in various International and National Journals. Her areas of interests include image processing, automata theory, compression, pattern matching and fingerprint recognitions.