An Enhanced Watermarking for Copyright Protection using DWT-SVD Approach

Vijay Kumar Patil
M. Tech Scholar
Department of Information Technology
Samrat Ashok Technological Institute
Vidisha (M.P.)

Rashmi Nigoti
Assistant Professor
Department of Information Technology
Samrat Ashok Technological Institute
Vidisha (M.P.)

ABSTRACT
With the fast improvement in information technology and multimedia, the need of digital data is enlarging every day while the speed of data over networks has passed over the crossbars. So it becomes important to protect our data from piracy and also it's very challenging today. There is crucial need to secure the copyright of individual's creation, to overcome from these types of problem. Digital Watermarking is treated as a solution to secure the multimedia data. Digital watermarking is hiding information in any form- audio, video, text, and image in original data without humiliating its perceptual quality. Watermarking is done for data authentication, security, and copyright protection of the original data. Copyright protection concerns the positive identification of content ownership as to protect the rights of the owner. In copyright protection robust watermark can be used because they are persistently combined with an image. Attempts to remove the watermark should result in serious degradation of image's visual quality. The detection of watermark in an image perhaps used to find the copyright holder. This paper discusses the latest method of watermarking for copyright protection. The performance parameters used to evaluate results are Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). High values of PSNR are considered as it shows the good imperceptibility of the techniques used.

Keywords
Watermark, Singular Value Decomposition (SVD), Discrete Wavelet Transformation (DWT).

1. INTRODUCTION
Watermarking techniques emerged on the basis of image processing, is the most generally used technique for the security of images .Thus the techniques by which the copyright information is embedded inside the original images, which is to be protected from the illegal modification/ replication and distribution is known as "Digital Watermarking" [20]. Digital Watermarking is the process of hiding or embedding an invisible signal (data) into the given signal (data). The invisible signal is called watermark and the given signal is called embedded data which may be text, image, audio or video for security purposes this embedded data can later be extracted from multimedia. The watermarking structure consists of an embedding algorithm, and an extraction or detection algorithm. Digital watermarking is a technique produced to secure a information by hiding so that the information in another object can be kept secret from everybody except the independent beneficiary [19]. In visible digital watermarking, information is visible in audio or video. Generally, the watermark is text or logo which analyzes the owner of the media. The information which is added as digital data to audio or video, text and images in invisible digital watermarking, still it can't be recognized. It may be a pattern of steganography where a party interacts with a secret message embedded in the digital signal. The major goal of digital watermarking application is to provide security to the digital content. Some of the digital watermarking applications are Digital Fingerprinting [13], Transaction Tracking [14], Broadcast Monitoring [12], and Copyright protection [15], Temper Detection [16], Data Hiding [17] and Content Authentication [18] etc.

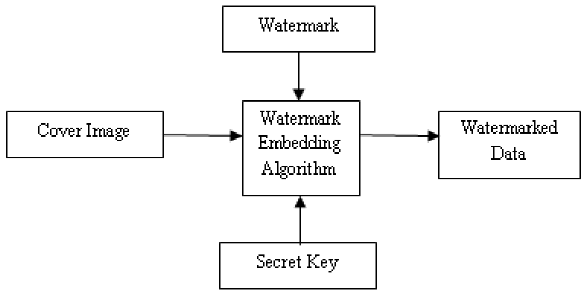

Figure1: Watermark Embedding Process

Digital watermarking technique consists of two algorithms: the first one is as the embedding algorithm and second is the extracting algorithm. These two processes are same for all the type of watermarking techniques. Figure 1 shows the watermark embedding process in which the watermark is embedded in the cover image by using the embedding algorithm. And Figure 2 shows the watermark detection process in which the embedded watermark is recovered by using the detection algorithm [1].

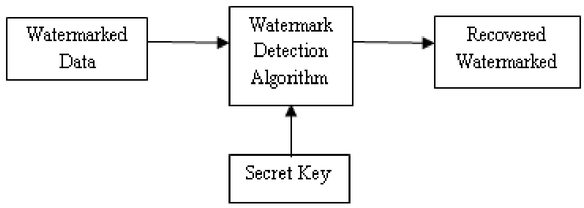

Figure 2: Watermark Detection Process

2. DIGITAL WATERMARKING TECHNOLOGY
Figure 3 shows the working of digital image watermarking. It can be classified in three stages [2]:

2.1 Embedding Stage
The embedding stage is first stage, in which the watermark is embedded in the original or cover image by applying embedding algorithm and secret key, after that watermarked image is generated. So the watermarked image is transmitted over the network.

2.2 Distortion/Attack Stage

The distortion/attack stage is the second stage, when the data is transmitted over the network. Either some noise is added with the watermarked image or some attacks are performed on the watermarked image. So, our watermarked data is either modified or destroyed.

2.3 Detection/Extracted Stage

The detection/extracted stage is the last stage, the watermark is detected or extracted by the dedicated detector/extractor from the watermarked image by applying some detection/extraction algorithm and by applying secret key. In addition to this, noise is also detected.

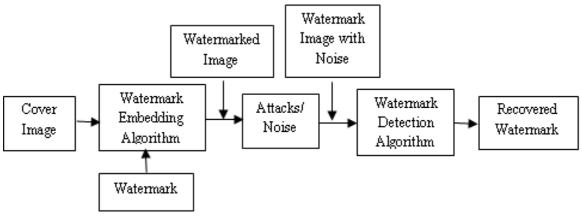

Figure 3: Stages in Digital Image Watermarking

3. WATERMARKING TECHNIQUES

According to domain, digital watermarking is classified in two domains. They are -

1. Spatial Domain method
2. Frequency Domain method

3.1 Spatial domain

In spatial domain image is represented in the form of pixels. By modifying or adjusting the intensity and the color value of some selected pixels [3] watermark embedding is done. In spatial domain, algorithm directly loads the basic data into the original image. Spatial domain watermarking can also be enforced by applying color separation. Thus, the watermark emerges in only one of the color bands. This gives the watermark visibly subtle such that it is challenging to identify it under regular viewing.

Singular Value decomposition (SVD):

The singular value decomposition (SVD) matrix is very effective in computer perception as a decomposition matrix and it is a useful tool for image transformations [4]. The SVD of a given image I in the form of a matrix is represented as

$$I = USV^T$$

Where, S is the diagonal matrix

$$S = \begin{bmatrix} S_1 & 0 \cdot & 0 & 0 \\ 0 & S_2 \cdot & 0 & 0 \\ . & . \cdot & . & . \\ 0 & 0 \cdot S_{n-1} & & 0 \\ 0 & 0 \cdot & 0 & S_n \end{bmatrix}$$

And U and V are the orthogonal matrices

$$U^T U = V^T V = 1$$

$$VV^T = 1$$

$$S_1, S_2, \ldots \ldots \ldots S_{n-1}, S_n \geq 0$$

The diagonal elements of matrix S are the singular values of matrix I and non-negative numbers.

Methods based on the singular values and watermarking using them was also developed. SVD of an image will give the dominant pixels in the image. This method uses Human Visual Characteristics of the image to find out at which portion the watermark is to be embedded.

3.2 Frequency domain

Frequency domain watermarking is achieving much success in comparisons to the spatial domain watermarking. In the transform domain watermarking techniques, firstly the original image is converted in a predefined transformation. Then the watermark is embedded to the transform image or to transformation coefficients. Finally, the inverse transform is performed to obtain the watermarked image [5].In transform domain most commonly used methods are Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT).

Discrete Wavelet Transform:

Discrete wavelet transform (DWT) of the image produces multi resolution representation of an image. The multi resolution representation provides a simple framework for interpreting the image information. The DWT analyses the signal at multiple resolution. DWT divides the image into high frequency quadrants and low frequency quadrants. The low frequency quadrant is again split into two more parts of high and low frequencies and this process is repeated until the signal has been entirely decomposed.

The single DWT transformed two dimensional image into four parts: one part is the low frequency of the original image, the top right contains horizontal details of the image, the one bottom left contains vertical details of the original image, the bottom right contains high frequency of the original image. The low frequency coefficients are more robust to embed watermark because it contains more information of the original image [6]. The reconstruct of the original image from the decomposed image is performed by IDWT [7].

LL2	HL2	HL1
LH2	HH2	
LH 1		HH1

Figure 4: Discrete Wavelet Transform Region

The DWT is applied on the host image to decompose the image into four non overlapping multi resolution coefficient sets.

$$W_{LL}^{j} = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} g(x)\, g(y) W_{LL}^{J-1}(2u - x)(2v - y)$$

$$W_{LH}^{j} = \sum_{x=0}^{N-1} \sum_{Y=0}^{N-1} g(x)h(y) W_{LL}^{J-1}\,(2u - x)(2v - y)$$

$$W_{HL}^{j} = \sum_{x=0}^{N-1} \sum_{Y=0}^{N-1} h(x)g(y) W_{LL}^{J-1}\,(2u - x)(2v - y)$$

$$W_{HH}^{j} = \sum_{x=0}^{N-1} \sum_{Y=0}^{N-1} h(x)h(y) W_{LL}^{J-1}\,(2u - x)(2v -$$

yWhere J is the level of the 2-D DWT, h (n) and g (n) are the impulse response.

4 PROPOSED METHOD

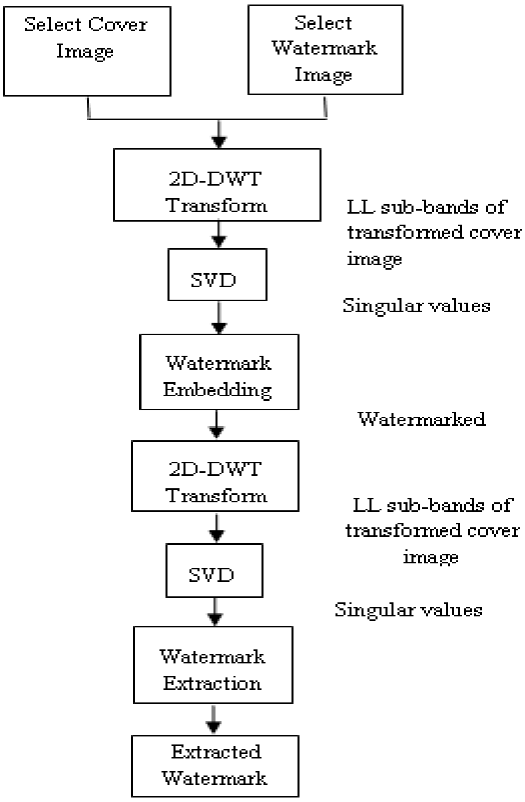

Figure 5: Flow chart of DWT-SVD

In DWT-SVD method the cover image is divided into different frequency sub-bands and the SVD of the low frequency sub-band is taken. The watermark is embedded in the low frequencies of the cover image. The embedding and extraction procedure is explained below.

A. Watermark Embedding

1. Perform DWT on the cover image and divide the image into LL, LH, HL and HH sub-bands.

2. Perform SVD on the LL sub-band to get the singular values using.

$$\mathrm{ILL_{SVD}} = U_{ILL} * S_{ILL} * V_{ILL}^{T}$$

3. Now, perform DWT on the watermark image and divide the image into LL, LH, HL and HH sub-bands.

4. Perform SVD on the LL sub-band to get the singular values.

$$\mathrm{WLL_{SVD}} = \mathrm{U_{WLL}} * \mathrm{S_{WLL}} * \mathrm{V_{WLL}^{T}}$$

5. Find out the singular values for the watermarked image using where k is the watermark strength factor.

$$\mathrm{S} = \mathrm{S_{ILL}} + \mathrm{k} * \mathrm{S_{WLL}}$$

6. Perform inverse SVD

$$\mathrm{W'LL_{SVD}} = \mathrm{U_{ILL}} * \mathrm{S} * \mathrm{V_{ILL}^{T}}$$

7. Perform inverse DWT to get the watermarked image.

B. Watermark Extraction

1. Perform DWT on the original image and divide into LL, LH, HL and HH sub-bands.

2. Perform SVD on the original image to get the singular values.

$$\mathrm{ILL_{SVD}} = \mathrm{U_{ILL}} * \mathrm{S_{ILL}} * \mathrm{V_{ILL}^{T}}$$

3. Perform DWT on the watermarked image and divide into LL, LH, HL and HH sub-bands.

4. Perform SVD on the watermarked image to get the singular values.

$$\mathrm{W'LL_{SVD}} = \mathrm{U_{W'LL}} * \mathrm{S_{W'LL}} * \mathrm{V_{W'LL}^{T}}$$

5. Find out the singular values for the resultant original image using where k is the watermark strength factor

$$\mathrm{S_{WLL}} = \frac{\mathrm{S_{WLL'}} - \mathrm{S_{ILL}}}{\mathrm{k}}$$

6. Perform inverse SVD

$$WLL_{SVD} = S_{WLL} * S_{WLL} * V_{WLL}^{T}$$

7. Perform inverse DWT to get the watermark image.

5 RESULT ANALYSIS

To evaluate the performance of the watermark images there are some quality measures such as PSNR, MSE and Computing Time.

MSE (Mean Square Error): The average squared difference between a cover image and a embedded image is known as MSE. By the formula given below MSE can be calculated.

$$MSE = \frac{1}{\mathrm{XY}} \sum_{I=1}^{X} \sum_{\mathrm{j=1}}^{\mathrm{Y}} \left(\mathrm{c(i,j)} - \mathrm{w(i,j)}\right)^{2}$$

X and Y are height and width respectively of the image. The c (i, j) is the pixel value of the cover image and w (i, j) is the pixel value of the watermarked image [10].

The PSNR (peak signal to noise ratio): Peak Signal to Noise Ratio (PSNR) is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [11]. It is expressed in decibels (dB). A larger PSNR indicates that the watermarked image closely resembles the original cover image, meaning that the watermarking method makes the watermark more imperceptible. It is calculated by the formula given below

$$PSNR = 10\log_{10}\left(\frac{\mathrm{L} * \mathrm{L}}{\mathrm{MSE}}\right)$$

L is the peak signal value of the cover image. It is equal to 255 for 8 bit images.

Figure 6: Lena image of DWT-SVD

Table 1: Analysis Result

IMAGE	PSNR IN DB		MSE IN %	
	Without Noise	With Noise	Without Noise	With Noise
LENA	40.24	32.77	24.78	138.54
BABOON	40.39	33.62	23.95	113.88
CAMERA MAN	40.14	32.93	25.40	133.53

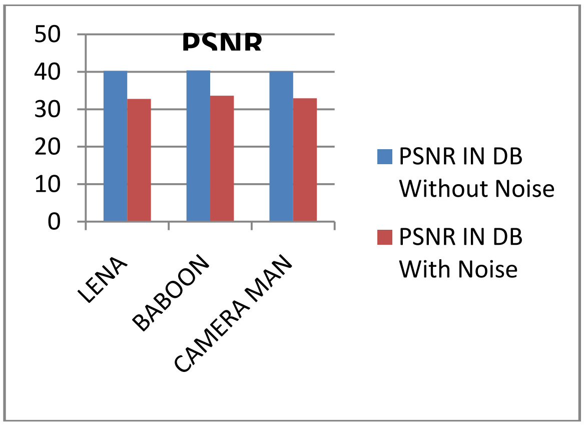

Figure 7: PSNR in DB without and with noise

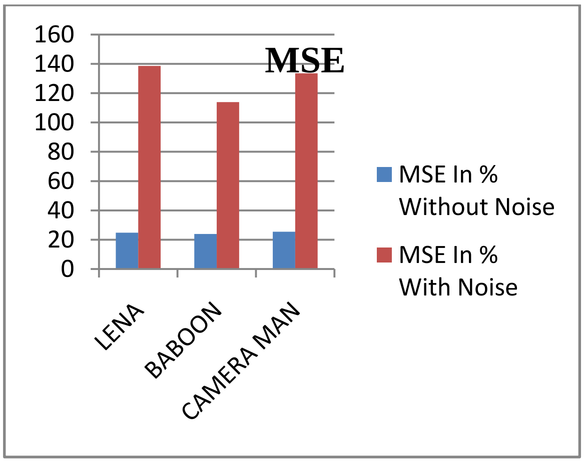

Figure 8: MSE IN % without and with noise

6 CONCLUSION

This paper is written to analyze watermarking algorithms using DWT-SVD technique. Paper analyzes DWT-SVD technique on 1-dimensional and 2-dimensional basic. Obtained results are showing that 2-dimesional application of DWT- SVD is better in terms of PSNR and MSE parameter.

Future work can be extended for the analysis of these techniques by applying certain attacks. With the same one can test for the robustness and security strength of technique.

7 REFERENCES

[1] Preeti Parashar and Rajeev Kumar Singh, “A Survey: Digital Image Watermarking Techniques”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014), pp. 111-124

[2] L. Robert, T. Shanmugapriya, ”A Study on Digital Watermarking Techniques”, International Journal of Recent Trends in Engineering, vol. 1, no. 2, May (2010).

[3] N. Chandrakar, J. Baggaa, ”Performance Comparison of Digital Image Watermarking Techniques: A Survey”, International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130.

[4] Md. Maklachur Rahman, “A DWT, DCT AND SVD based watermarking technique to protect the image piracy”, International Journal of Managing Public Sector Information and Communication Technologies (IJMPICT), Vol. 4, No. 2, June 2013.

[5] F.Daraee, S.Mozaffari, “Watermarking in binary document images using fractal codes”, Pattern Recognition Letter, (2013).

[6] N.Tiwari, M. k. Ramaiya, Monika Sharma, “Digital watermarking using DWT and DES”, IEEE (2013).

[7] S.S.Gonge, J. W. Bakal, “Robust Digital Watermarking Techniques by Using DCT and Spread Spectrum”, International Journal of Electrical, Electronics and Data Communication, ISSN: 2320-2084, vol. 1, no. 2, (2013).

[8] Prabhishek Singh, R S Chadha “A Survey of Digital Watermarking Techniques, Applications and Attacks”, International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March (2013) ISSN: 2277-3754

[9] G.Rafael, C. Gonzalez and R. E. Woods, “Digital Image Processing”, Third Edition, (2008).

[10] Amit Kumar Singh, Nomit Sharma, et al. “A Novel Technique for Digital Image Watermarking in Spatial Domain”, 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, (2012).

[11] Sunanda Dutt, Dr. Asoke Nath “ Data Authentication using Digital Watermarking”, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 12, December (2014),

[12] L. Li and X. Li,” Watermarking Protocol for Broadcast Monitoring”, International Conference on E business and E-Government (ICEE) (2010).

[13] D. Zhang, S. Xu, Y. Wang, J. Zhang and Y. Li, ”A Digital Fingerprinting Scheme of Digital Image”. International Conference on Computational Intelligence and Software Engineerin (CISE) (2010).

[14] S. Emmanuel, A. P. Vinod, D. Rajan and C.K. Heng, “An Authentication Watermarking Scheme with Transaction Tracking Enabled”, Digital Ecosystem and Technologies Conference, 2007.DEST’07 Inaugural IEEE-IES.

[15] Y.-C. Wang and J.-f. Niu, “Research on Digital Content Copyright Protection System”, IEEE International

Conference on Network Infrastructure and Digital Content, 2009. IC-NIDC (2009).

[16] S.-L. Hsieh, C.-P. Yeh and I-J. Tsai, "An Image Copyright Protection Scheme with Tamper Detection Capability", Symposia and Workshops on Ubiquitous, Autonomic and trusted Computing, 2009.UIC-ATC'09

[17] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication", IEEE Transactions on Circuits and Systems for Video Technology, vol. 18.

[18] J. Zhu, Q. Wei, J. Xiao and Y. Wang," A Fragile Software Watermarking Algorithm for Content Authentication", IEEE Youth Conference on Information, Computing and Telecommunication, 2009.YC-ICT'09.

[19] Aparna JR, Sonal Ayyappan "Comparison of Digital Watermarking Techniques" International Conference on Computation of Power Energy, Information and Communication (ICCPEIC), 2014

[20] Prasanna Shah, Toshanlal Meenpal, Ankit Sharma, Vivek Gupta, Amit Kotecha," A DWT-SVD Based Digital Watermarking Technique for Copyright Protection", International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) – 2015.