*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. VI (Jul – Aug. 2014), PP 98-103*
*www.iosrjournals.org*

# Compression Combined Robust Watermarking Scheme using SVD Replacement Technique

Gangadhar Tiwari[1], Marpe Sora[2]
[1](Department of Information Technology, National Institute of Technology, Durgapur, India)
[2](Department of Computer Science and Engineering, Rajiv Gandhi University, Itanagar, India)

***Abstract:*** *This paper proposes a novel compression combined digital image watermarking scheme based on singular value replacement technique. Image compression is achieved using Huffman encoding technique. Huffman encoding is an entropy encoding algorithm offering lossless image compression. The proposed watermarking scheme combines Integer wavelet transform (IWT) with singular value decomposition (SVD). For watermark embedding, the singular values (SV's) of high frequency (CD) band of cover images are replaced with the singular values of watermark signal. Choosing a sample image as watermark signal depends on the relation between energy of singular value of high frequency component of cover and sample image. The combination of Huffman encoding with IWT-SVD domain watermarking results in a robust watermarking scheme that provides good compression ratio with better signal quality. Experiments suggest that the watermarked and original images are perceptually similar. Also, watermarked images are robust against image processing distortions and geometrical attacks. Further, the recovered images are distortion free.*

***Keywords:*** *Digital Watermarking, Distortion free data hiding, Huffman encoding, Integer Wavelet Transform, Singular Value Replacement*

## I. Introduction

In the age of digital multimedia, contents are distributed over digital communication links. Sharing of information over these networks offers fast access, greater coverage and ease in distribution, storage and retrieval. However, with the advent of multimedia information systems, there exist dedicated softwares that enable content manipulation and alteration thereby arising the need for a secure authentication system that can validate data integrity and credibility. Digital watermarking is a pivotal tool to protect multimedia data in networked environment against content manipulation. A watermark is a digital signal containing information regarding the multimedia content whose integrity it wishes to protect. It is embedded into the multimedia content in such a way that it is detected at acceptable perceptual fidelity of the content [1].

A digital watermarking system comprises of three components viz. Watermark Carrier, Encoder and Decoder. Fig.1 represents a typical watermarking system diagrammatically where the original image is the watermark carrier. The watermark encoder inserts the watermark into the cover image. A secret key is used to protect the system. Decoder extracts the watermark signal from the watermarked image or its distorted version using the secret key and original image.

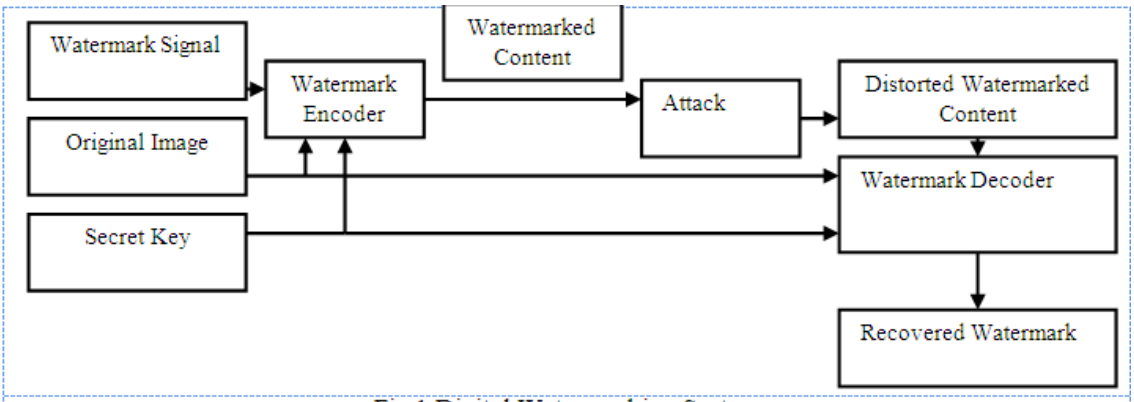


Fig.1 Digital Watermarking System

Depending on requirement of Original Image during watermark extraction, digital watermarking is divided into two groups:

- **Private Watermarking-** Original image is required during watermark extraction.
- **Public Watermarking-** Watermark extraction is achieved without original Image.

Earlier researches in watermarking concentrated on private watermarking due to their higher robustness against distortions compared to their private counterparts. However, such schemes raise serious security concerns. Moreover, it is unfit to be employed for practical application scenarios because it is impossible to guarantee the presence of original content for watermark extraction in all the cases [2].

When watermarking the digital images, it needs to be noted that they have huge sizes with higher inter-pixel redundancy and requirement of real-time responses. To achieve this, we propose to perform image compression before watermarking. Image compression is a technique of converting image data into another form by removing the inter pixel redundancies. It reduces the image size thereby reducing the memory space requirement for storing the image and ensures faster transmission. Moreover, it ensures data reliability against transmission errors. In the proposed work, digital images are compressed using Huffman Encoding technique before watermark embedding and decompressed before watermark extraction. We then develop a public watermarking scheme in IWT-SVD Domain that is as robust and secure as private watermarking schemes.

The remainder of the paper is organized as follows: Section-2 presents survey and analysis of existing watermarking techniques. Section-3 deals in detail description of the proposed watermarking model. Experimental results are presented in Section-4. A detailed discussion on result is presented in section-5. This paper ends in Section-6 with conclusion.

## II. Related Work

To obtain greater robustness with better perceptual quality various watermarking techniques have been proposed in recent past. However, these are insecure against compression attack. To tackle this, JPEG based on discrete cosine transform (DCT) and JPEG2000 based on discrete wavelet transform (DWT) have been deployed. Thus, further researches concentrated on developing compression combined digital watermarking in transform domain. We present below a survey of most relevant existing watermarking techniques:

A method for multi-index decision (maximizing deviation method) based watermarking is proposed in [3]. This watermarking technique is designed and implemented in the DCT domain as well as the wavelet domain utilizing Human Visual System (HVS) models. Their experimental results showed that the watermark based on the wavelet transform more closely approaches the maximum data hiding capacity in the local image compared to other frequency transform domains. Reference [4] suggested using a wavelet packet of image and video watermarking. Here the energy for each sub-band $B_{i,j}$ is calculated. Then, certain sub bands are pseudo-randomly selected according to their energy. The mean absolute coefficient value of each selected sub-band is quantized and used to encode one bit of watermark information. Finally, pseudo-randomly selected coefficients of that sub-band are manipulated to reflect the quantized coefficient mean value. This type of algorithm generates redundant information since the wavelet packet generates details and approximation sub-band for each resolution, which adds to the computation overhead. Reference [5] proposed a DWT based multiple watermarking schemes. Image was decomposed in two levels and watermarks were inserted in low frequency (LL) and high frequency (HH) bands. The scheme showed good results against wide range of attacks like compression, noise addition, histogram equalization but could not resist rotation, scaling and print-scan attacks. Reference [6] proposed a watermarking technique by combining DWT-DCT. Watermarking is achieved by embedding the watermark in 1$^{st}$ and 2$^{nd}$ level sub-bands of cover image sub-sequenced by applying DCT on the selected DWT sub-bands. This scheme has superior performance in comparison to individual watermarking approaches. Further researches suggested combining SVD based watermarking schemes with transform domain techniques to obtain greater robustness against attacks and such schemes are termed hybrid SVD schemes. Reference [7] proposed a hybrid watermarking schemes based on DCT and SVD where they applied DCT to the cover image and used zig-zag scanning technique to map coefficients with frequency bands. Later each band is decomposed using SVD. Finally, the singular values of each band of cover image are replaced by singular values of the DCT-transformed watermark. Their scheme is robust against compression, filtering and cropping but watermark is insecure against geometrical and print-scan attacks. Further, its computational cost is higher and the scheme require original image during watermark extraction. Reference [8] presented another scheme for watermark embedding based on SVD and the DCT into the original image. Here, only the singular values (SVs) of a recognized pattern are embedded into the original image to obtain better perceptuality and higher robustness to attacks.

A watermarking technique combining SVD with DWT was proposed by [9].They decomposed the cover image using DWT into four sub bands and applied SVD to each of them and to the watermark also. During watermark embedding singular values of watermark were replaced with singular values of cover image. This scheme provides reasonably better results with respect to existing schemes. However, it did not perform image compression. Reference [10] presented a novel non-blind image watermarking techniques. They

employed modification on singular values of the original image by embedding DCT coefficients of the watermark image to implement the methods. Reference [11] proposed an optimal DWT-SVD based image watermarking scheme using Pareto-based Multi-Objective Evolutionary Algorithm (MOEA). Here the cover image is DWT decomposed and SVD is applied to each band. Further, to embed watermark, the singular values of each sub-band of the cover image are tailored at different scaling factors which are optimized using a fast Elitist Non dominated Sorting Genetic Algorithm (NSGA-II) to obtain optimum robustness without sacrificing transparency. Experiments showed greater transparency and robustness against attacks. Reference [12] proposed another watermarking scheme combining DWT-SVD with feature template. In this scheme watermark embedding is performed in DWT-SVD domain. Later, the feature points operator extracts the feature points as a template and conserve it. During detection it employs linear transformation between corresponding points in feature template to realize resynchronization. Experiment suggests that the proposed scheme is invisible and robust against common image processing attacks. Reference [13] proposed similar image watermarking scheme in DWT-SVD domain using differential evolution (DE). They performed 3 level wavelet decomposition of cover image and SVD is applied to each sub-band at 3rd level. To embed the watermark, after 1st level decomposition of watermark, singular values of each sub-band of cover image are changed by different scaling factors (SFs). The differential evolution algorithm is employed for optimizing the scaling factor that provides higher robustness with imperceptibility.

From the above analysis it is clear that combining wavelet decomposition with SVD provides greater robustness and imperceptibility. Hence in the proposed work, we employ second generation wavelet known as IWT in combination with SVD to develop a private watermarking scheme. To achieve robustness against compression attack we employ Huffman encoding technique, thereby the scheme would provide compression, robustness and imperceptibility all at the same time. We propose our model in the next section.

## III. Proposed Model

In the proposed watermarking scheme, we first compress the cover image using Huffman encoding technique and then embed watermark in IWT-SVD domain. IWT decomposes the image into four frequency bands: CA, CH, CV and CD band. CA band represents low frequency giving approximate details, CH and CV represent middle frequency giving horizontal and vertical details and CD represents high frequency band highlighting diagonal details of the image, respectively. We select CD band for watermark embedding as it's contribution towards image energy is insignificant. Moreover, watermarks embedded in CD band are resistant to image processing attacks. This scheme replaces singular values of CD band of cover images with the singular values of watermark. In TABLE-I, singular values of the CD band of various test images are given. Sample image selected for watermark is preprocessed to have singular values within the range of 0–180. If a watermark is selected such that its singular values lies within this range, then the energy of singular values of watermark will be nearly equal to energy of singular values of CD band. Hence, replacing the singular values will not affect perceptual fidelity of image and the energy content of CD band. Watermark size is equalized to size of CD band.

**Table-I** Singular Values Of Cd Band Of Various Images

| Image | Singular Values | |
|---|---|---|
| | **Max** | **Min** |
| Airplane | 178.93 | 0.06 |
| Cameraman | 220 | 0 |
| Elaine | 198.76 | 0.15 |
| Lena | 182.40 | 0 |
| Peppers | 121 | 0 |
| Copyright | 200 | 0 |

During watermark extraction we first decompress the image and then extract the watermark. In the following section we present the image compression scheme using Huffman Encoding technique, watermark embedding and extraction and its block diagram.

### 3.1 Huffman Encoding Technique

Huffman coding is an entropy encoding algorithm based on bottom up approach providing lossless image compression. It uses a variable-length code table for encoding an image. It aims at finding the minimum length bit string that can be used to encode an image [14]. Huffman coding is based on the principal that in an optimum code, symbols with greater probability have shorter code words and in optimum prefix code, the two symbols that occur least frequently has equal size. Generation of Huffman code involves following steps [15]:

**Step1**. Initiate with two least probable symbols, α and β, of an alphabet A, such that the codeword for α and β are [t]0 and [t]1 respectively where [t] is a binary string of 0s and 1s.

**Step2.** Combine the two symbols into a group denoted by another symbol γ in the alphabet set such that the

probability for γ is sum of probabilities of α and β.
**Step3.** Determine the bit sequence [t] recursively by using the new alphabet set.
Decompression basically involves translation of the stream of prefix codes to individual byte values, accomplished by traversal of Huffman tree node by node where each bit is read from the input stream.

### 3.2. Watermark Embedding

Watermark embedding algorithm involves following steps:
**Step1.** Apply CDF (2, 2) wavelet and decompose the cover image into four sub-bands: CA, CH, CV and CD.
**Step2.** Apply SVD to CD band using (1)

$$H = U_H * S_H * V_H^T \qquad (1)$$

**Step3.** Apply SVD to Watermark Signal W using (2)

$$W = U_W * S_W * V_W^T \qquad (2)$$

**Step4.** Replace singular values of CD band with singular values of watermark [16].
**Step5.** Obtain modified CD band by applying inverse SVD according to (3).

$$H' = U_H * S_W * V_H^T \qquad (3)$$

**Step6.** Apply inverse IWT to generate watermarked image.
**Step7.** Compress the watermarked image using Huffman Encoding described as above.

### 3.3. Watermark Extraction

**Step1.** Decompress the distorted watermarked image using Huffman Decoding.
**Step2.** Using CDF (2, 2) wavelet decompose the decompressed distorted watermarked image into four sub-bands: CA, CH, CV and CD.
**Step3.** Apply SVD to CD band using (1)
**Step4.** Extract the singular values from CD band.
**Step5.** Construct the watermark using (4) from singular values and orthogonal matrices $U_w$ and $V_w$ obtained using SVD of original watermark.

$$W_E = U_W * S_H * V_w^T \qquad (4)$$

### 3.4 Block Diagram

The block diagram for proposed model is given by Fig.2 as below.

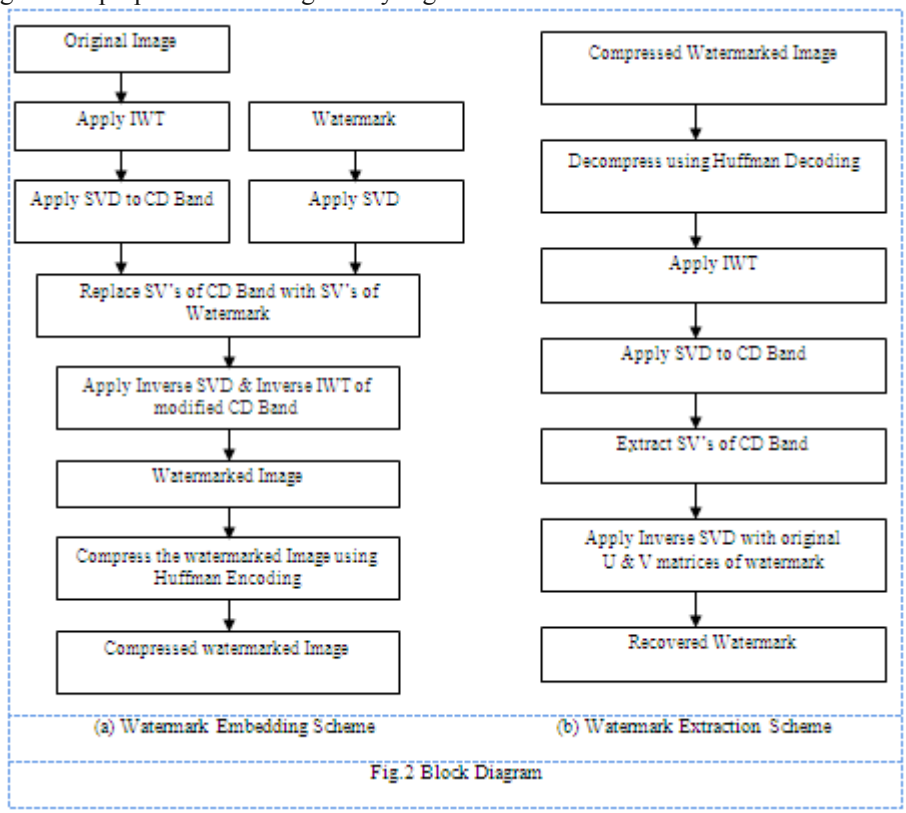


Fig.2 Block Diagram

## IV. Simulation Results

We performed simulation on Matlab R2011a, under the Windows 7 professional with dual Core CPU and 4 GB RAM. The test images are taken from USC SIPI image database and are 8 bit gray scale images with size 512×512. Gray scale DA-IICT logo of size 256 × 256 is used as a watermark. The watermarked images were subjected to various attacks to check the robustness of the scheme and the results in terms of standard metrics are listed in TABLE-II. The standard metrics are Peak Signal to Noise Ratio (PSNR) and Mean Structural Similarity Index (MSSIM). To measure the performance between original and recovered watermark we calculate Correlation Coefficient (CC). The value of Correlation Coefficient lies between -1 and 1. The correlation coefficient value from 0.4 to 0.9 indicates key resemblance among the watermarks. Simulation results for Lena Image and its attacked version are presented in Fig.3 to prove the validity of watermarking scheme. (Lena image is referred here as its properties are is most widely reported in watermarking literature.)

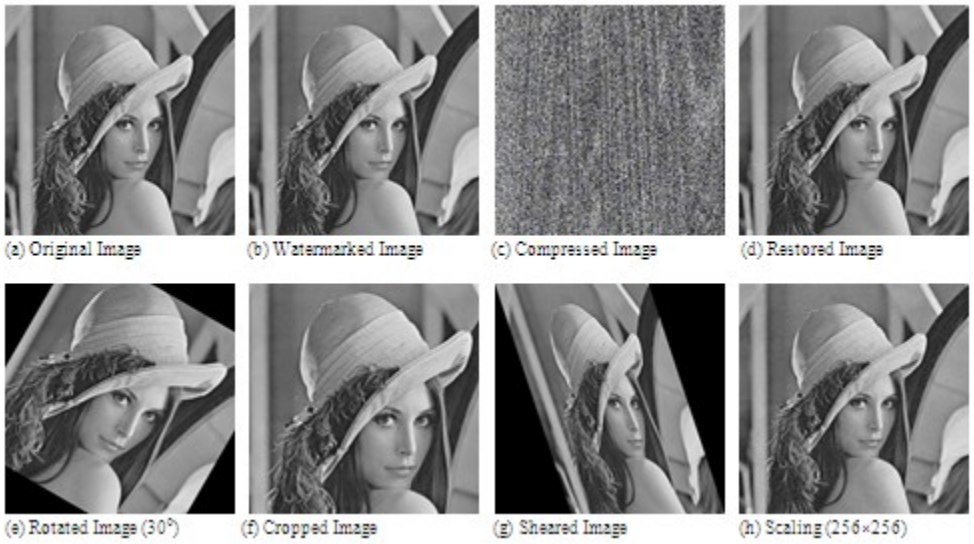


**Fig.3** Simulation Results

**Table-II** Values Of Quality Metrics Under Different Test Conditions

| Original Image (512×512) | Watermarked Image | | PSNR value for Attacked Images | | | | Correlation Coefficient between embedded and extracted watermark |
|---|---|---|---|---|---|---|---|
| | PSNR (in dB) | MSSIM | Salt & Pepper Noise | Poisson Noise | Gaussian Noise | Speckle Noise | |
| Airplane | 45.61 | 0.9995 | 25.88 | 25.62 | 30.03 | 32.31 | 0.9321 |
| Cameraman | 47.34 | 0.9997 | 25.04 | 27.37 | 30.17 | 35.42 | 0.9208 |
| Elaine | 42.68 | 0.9986 | 25.23 | 25.36 | 30.15 | 31.70 | 0.9201 |
| Lena | 43.88 | 0.9989 | 25.52 | 27.18 | 29.92 | 35.63 | 0.9289 |
| Peppers | 51.40 | 0.9997 | 25.18 | 28.20 | 30.90 | 35.49 | 0.9421 |

## V. Discussion On Simulation Results

Simulation results presented in Fig.3 and TABLE-II clearly indicates that the watermarking scheme provides higher perceptual quality with greater robustness. In addition, the restored images are distortion free.

### 5.1. Perceptual Quality

Reference [17] suggested that the acceptable value of PSNR for original and watermarked image should be between 25dB to 50dB. The higher value represents better signal quality. Similarly, the MSSIM and CC value lies between −1 and +1. Thus, from TABLE-II, it is evident that the watermarked scheme is effective and has good perceptual fidelity.

### 5.2 Robustness

To measure the robustness of the scheme, various geometric and image processing attacks are employed on the watermarked images. The result for rotation, crop, shear, and scaling attacks are presented in Fig.3. The results for Salt & Pepper, Gaussian, Speckle and Poisson Noise attacks are presented in TABLE-II and PSNR value is used as a metric to measure the robustness. Thus from TABLE-II and Fig.3 it is clear that the watermarking scheme is robust against different types of attacks.

### 5.3. Compression

Huffman encoding is applied to achieve compression of watermarked images. It is observed that for an 8 bit gray scale Lena image with size 512*512, the compression scheme provides 0.58% compression. After decompression the restored images are distortion free. Further, the compression of watermarked images provides faster transmission and ensures data reliability against transmission errors.

## VI. Conclusion

This paper presents a novel image watermarking scheme that performs compression along with watermarking the digital content. The proposed method can successfully resist geometric attacks and various image and signal processing distortions. Besides, hiding the watermark in IWT-SVD domain provides for better signal quality and application of Huffman encoding provides data compression simultaneously. Also, the recovered images are near distortion free. It offers higher robustness which is validated by recovery of the watermark having significant correlation coefficient value. Although this scheme is blind in nature it's performance is superior compared to non-blind techniques. Thus, this technique meets most of the key requirement of an ideal watermarking system including imperceptibility, robustness and compression.

## References

[1]. I Cox, M Miller and J Bloom, Digital Watermarking (Academic Press, San Diego, USA, 2002)
[2]. C.S. Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property (Idea Group Publishing, 3 Henrietta Street, London, 2005)
[3]. Wei Zhihui and Xiao Liang, An Evaluation Method for Watermarking Techniques, IEEE International Conference on Multimedia and Expo, New York, USA, 2000, 373 – 376
[4]. E.Masataka and M.Akio, A Wavelet-Based Watermarking for Digital Images and Video, IEICE Trans .Fundamentals, E83–A, 2000, 532-540
[5]. M S Raval and P P Rege, Discrete wavelet transform based multiple watermarking scheme, TENCON Conference on Convergent Technologies for Asia-Pacific Region, 2003, 935–938
[6]. Ali Al-Haj, Combined DWT-DCT Digital Image Watermarking, Journal of Computer Science , 3 (9), 2007, 740-746
[7]. Q Liu and Q Ai, Combination of DCT-based and SVD-based watermarking scheme, 7th International Conference on Signal Processing Proceedings, 2004, 873–876
[8]. F. Huang and, ZH Guan, A hybrid SVD-DCT watermarking method based on LPSNR, Pattern Recognition Letters, Elsevier Ltd, 25, 2004, 1769–1775
[9]. G Emir and A Eskicioglu, Robust DWT-SVD domain image watermarking: Embedding data in all frequencies, Proceedings of the workshop on Multimedia and Security, 2004, 166–174
[10]. A Mansouri, A M Aznaveh, and FT Azar, Secure Digital Image Watermarking Based on SVD-DCT, Springer-Verlag, 2008, 645–652
[11]. M. Monemizadeh and S.A. Seyedin, Optimal DWT-SVD Domain Image Watermarking Using Multi-objective Evolutionary Algorithms, World Congress on Computer Science and Information Engineering, 2009, 259-263
[12]. S. Hao and TG Ming, A DWT-SVD domain watermarking algorithm based on feature template, International Conference on Computer Science and Network Technology, 2011, 2010 – 2013
[13]. Ali, Ahn and Pant, An optimized watermarking technique based on DE in DWT-SVD domain, IEEE Symposium on Differential Evolution, Singapore, 2013,99 – 104
[14]. David A. Huffman, A Method for the Construction of Minimum-Redundancy Codes, Proceedings of the I.R.E., 1952,1098–1102
[15]. TH Cormen, CE Leiserson, RL Rivest, and C Stein, Introduction to Algorithms ( MIT Press and McGraw-Hill, 2001) 385–392.
[16]. A.K. Gupta and M.S. Raval, A robust and secure watermarking scheme based on singular values replacement, Indian Academy of Sciences, Sadhana ,37 (4), 2012, 425–440,.
[17]. D.Salomon, Data Compression: The Complete Reference (Springer, 2007)