# Comparative Analysis of Normalization based Image Watermarking Techniques

T.Sridevi Associate Professor Dept. of CSE CBIT, Hyderabad. K.Swapna Student (M.Tech) Dept. of CSE CBIT, Hyderabad V.Vijay Kumar Dean, Dept. of CSE&IT Godavari Inst. of Tech., Rajamandry

## ABSTRACT

This paper presents a comparative study of watermarking schemes. The embedding of watermark is performed after the image normalization. By normalization process the normalized image achieves invariance properties against geometric attacks which include rotation, scaling and translation of an image. Watermarking is done using five methods DCT Zigzag, DCT blocks, DWT, Zernike transform, SVD-DCT. Similarity measures are calculated in order to compare the five watermarking schemes.

## **Keywords**

Watermarking, Affine Transformation Matrix, DCT, low frequency, mid frequency, high frequency, Normalized image, zigzag scan, zernike moments.

## **1. INTRODUCTION**

Digital watermarking has been proposed in recent years to prevent illegal and malicious copying and distribution of digital media by embedding unnoticeable information into the media content in the past few years, the need for watermarking has gained significant attention due to the spread of illegal redistribution and unauthorized use of digital multimedia. Watermarking is an information-embedding technique that embeds a secret imperceptible signal directly into original data often called host signal in a robust manner. In general, the watermark contains information that uniquely identifies the content owner.

Three aspects of information hiding systems are: capacity, security and robustness. Watermarking prefers robustness, i.e. it should be impossible to remove the watermark without severe quality degradation of the cover content, while steganography demands high security and capacity, i.e. hidden information is usually fragile and can be destroyed by even trivial modifications.

Recently, the watermark techniques are utilized to keep the copyright protection [1]. As the research area of image watermarking becomes mature, researchers gradually change their target to video watermarking. A great variety of watermarking schemes have been proposed in the literature. Digital video watermarking algorithms can be sorted according to the embedding domain, such as the spatial domain, compressed domain, and bit stream domain. The idea of watermarking is in fact very old that was called

"steganography". For formatted digital text documents, the idea was revived in 1994 by Brassil et al., even before, T. Jack had worked on the first methods for embedding invisible information into digital images [2]. Other watermarking schemes deal with embedding watermarks into images either in spatial domain or in frequency domain like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) etc.

The watermarked image has to be robust against several attacks like: removal attacks, geometric attacks, cryptographic attacks. Geometrical attacks are a serious problem and there are not many techniques that have handled this attack. By normalization process the normalized image achieves invariance properties against geometric attacks which include rotation, scaling and translation of an image. In the experiment, normalization is applied on the original image which changes the pixel intensity values, and then the watermark is embedded into the normalized image. The normalization based image watermarking is implemented using the transforms DCT, DWT, Zernike moments and SVD-DCT. Different attacks like adding noise, rotation, histogram equalization, contrast increase, contrast decrease, scaling are applied on the watermarked image and comparative study of the methods is performed.

The rest of the paper is structured as follows. Section 2 describes the literature survey on Digital watermarking, normalization and transforms like DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), Zernike Transform, SVD (Singular value Decomposition), Zigzag scanning, attacks in watermarking while Section 3 describes watermarking algorithms and details of the attacks used in the project. Section 4 provides the experimentation and results and Conclusion of the results are discussed in Section 5.

## 2. RELATED THEORY

This section describes the details of digital watermarking: classification of watermarks, watermarking methodologies, transforms used in the work: DCT, DWT, Zernike transform, SVD-DCT.

## 2.1 Digital watermarking

Digital watermarking is the process of embedding information into a digital signal in a way that is difficult to remove. Digital watermarking involves embedding a structure in a host signal to mark its ownership. Digital watermarks may be comprised of copyright or authentication codes, or a legend essential for signal interpretation. The existence of these watermarks within a multimedia signal goes unnoticed except when passed through an appropriate detector. Common types of signals to watermark are still images, audio, and digital video. If the signal is copied, then the information is also carried in the copy. A signal may carry several different watermarks at the same time.

A watermarking system is usually divided into two distinct steps, embedding, and detection. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. Detection (often called extraction) is an algorithm which is applied to the signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark is still present and it can be extracted. A general scheme for digital watermarking [3] is shown in Figure 1.



Fig b. Watermark Extraction

Figure 1: General watermarking scheme

#### 2.1.1 Classification of watermarks

Watermarking schemes are classified[4] by visibility – Visible vs. invisible, goals – Robust vs. Fragile vs. semi-fragile, requirement of original for extraction – Blind vs. nonblind/Oblivious vs. non-oblivious/Public vs. private, embedding – Spatial domain vs. transform domain, working region – Global vs. block-by-block, characteristics – Image-adaptive vs. imageindependent. The two most important ways to classify watermarking methods are (see Figure 2):



Figure 2: Classification of watermarking schemes

(a) By requirement of original for extraction – Oblivious vs. non-oblivious. Oblivious - Watermarking schemes that do not

need the original image for watermark extraction are called oblivious. Non-oblivious - Watermarking schemes that need the original image for watermark extraction are called nonoblivious. (b) By embedding – Spatial domain vs. transform domain. Spatial domain techniques – Watermarking schemes that directly perform some transformation on the image pixels are called spatial domain watermarks or spatial watermarks. Transform domain techniques – Watermarking schemes that transform the image in the frequency domain and then modify the transform coefficients are called transform domain techniques or spectral watermarks.

#### 2.1.2 Watermarking methodologies

Watermarking methodologies can be classified based on the cover document, domain and perception of the watermark [5]. Watermarking methodologies are shown in Figure 3.



DOCUMENT: The document where the watermark is embedded is called the cover document. A watermark may carry any information but the amount of information is not unlimited. The size of the document depends on the size of the cover document. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as: Text Watermarking, Image Watermarking, Audio Watermarking, and Video Watermarking

DOMAIN: Watermark can be embedded in the spatial domain or transform domain of the cover document. In spatial domain embedding of watermark is done by accessing the pixel values where as in transform domain, frequency coefficients are used.

PERCEPTION OF THE WATERMARK: Perception of the watermark depends on the value of the watermark strength (k) used in the process of embedding. Based on the value of watermark strength the watermarking is classified as visible and invisible watermarking.

Watermarking is done using a scaling factor called watermark strength k which ranges between 0 and 1. If I(i) and W(i) are the i<sup>th</sup> pixels of cover image I and watermark W, the i<sup>th</sup> pixel of Watermarked Image I' is obtained from

$$I'(i) = I(i) + \alpha^* W(i)$$
 (1)

#### 2.2 Normalization

Normalization is the process which changes the range of pixel intensity values. The image after normalization achieves invariance properties against geometric attacks. The geometric attacks include rotation, scaling and translation of an image. These kinds of attacks can be represented by affine transformations [6], [7]. An affine transformation with scaling parameters (a,b) rotation angle  $\varphi$  and translational parameters (Tx,Ty) is defined using as:

where (x,y) is a pixel coordinates of an input image and  $(x_a, y_b)$  is the corresponding pixel coordinates of the transformed image.

The affine transform parameters can be calculated from image moments [8], [9]. The image moments [7].  $m_{pq}$  of an input image f(x,y) with size of N1 X N2 pixels, is defined in the two dimensional Cartesian coordinates as:

$$m_{pq} = \sum_{y=0}^{N_2-1} \sum_{x=0}^{N_1-1} x^p y^q . f(x, y)$$
(3)

The centriod of the input image is calculated using 0<sup>th</sup> and 1<sup>st</sup> moments as

$$\bar{x} = \frac{m_{10}}{m_{00}}, \, \bar{y} = \frac{m_{01}}{m_{00}}$$
 (4)

The translation effect can be eliminated by shifting the centroid of input image. The central moment is calculated using

$$\mu_{pq} = \sum_{y=0}^{N_2 - 1} \sum_{x=0}^{N_1 - 1} (x - \overline{x})^p (y - \overline{y})^q . I(x, y) \quad (5)$$

And the covariance matrix based on the central moments is constructed as:

$$\begin{pmatrix} \mu_{20} & \mu_{11} \\ \mu_{11} & \mu_{02} \end{pmatrix}$$
 (6)

Based on the covariance matrix, the rotation angle  $\phi$  is calculated using

$$\varphi = \frac{1}{2} \tan^{-1} \left[ \frac{2\mu_{11}}{\mu_{20} - \mu_{02}} \right] \tag{7}$$

The two eigenvalues of the covariance matrix are given by the

$$\lambda_{i} = \frac{1}{2} \left[ (\mu_{20} + \mu_{02}) \pm \sqrt{4\mu_{11}^{2} + (\mu_{20} - \mu_{02})^{2}} \right] i = 1,2$$
(8)

Based on the eigen values, the scaling parameters are calculated as:

$$a = \frac{(\lambda_1 \lambda_2)^{0.25}}{\sqrt{\lambda_1}}, b = \frac{(\lambda_1 \lambda_2)^{0.25}}{\sqrt{\lambda_2}}$$
(9)

Thus, any input image can be transformed to a normalized form by identifying the transform parameters, (a,b),  $\varphi$  and translation parameters.

#### 2.3 Discrete Cosine Transform (DCT)

Digital image watermarking technology is closely related to image coding technology. DCT is a technique for converting a signal into elementary frequency components. It is widely used in image compression [10]. Transform coding is now the defacto standard in image and video coding, while the Discrete Cosine Transform [6] (JPEG, MPEG-1, 2, H.261, H.263) and the Discrete Wavelet Transform (JPEG2000) are mostly used. Given an image A of size *MxN*, the DCT of the image is defined as:

$$B(k_1, k_2) = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} A(i, j) \cos\left[\frac{\pi k_1}{2M}(2i+1)\right] \cos\left[\frac{\pi k_2}{2N}(2j+1)\right]$$
(10)

 $B(k_1,k_2)$  is the DCT coefficient of the image in row  $k_1$  and column  $k_2$ . Larger DCT coefficients are usually located at low frequencies (upper left corner), while coefficients at high frequencies are very small. That is, DCT puts most of an image's energy at low frequencies.

DWT separates an image into several sub-images corresponding to horizontal, vertical and diagonal details at each resolution level and a coarsest resolution level. Like DCT, most energy of an image is put in the coarsest sub-image.

#### 2.4 Discrete Wavelet Transform (DWT)

Using DWT, the signal is split into two parts, usually the high frequency and the low frequency part [11]. This splitting is called decomposition. The edge components of the signal are largely confined to the high frequencies part [12]. The signal is passed through a series of high pass filters to analyze the high frequencies, and it is passed through a series of low pass filters to analyze the low frequencies.

LL2	HL2	HL1
LH2	HH2	
I	.H1	HH2

Figure 4: DWT decomposition

In two-dimensional DWT, each level of decomposition produces four bands (see Figure 4) of data denoted by LL, HL, LH, and HH. The LL sub band can further be decomposed to obtain another level of decomposition. This process is continued until the desired number of levels determined by the application is reached.

### 2.5 Zernike Transform

Shape is a key information to human for distinguishing visual data. To retrieve an image from a large database, we need shape descriptors that have sufficient discriminatory properties and are robust to noise. These descriptors should be invariant to translation, rotation, scale, and perspective of images. Zernike moments have some desirable properties such as rotation invariance, robustness to noise, expression efficiency, and multi-level representation for describing various shapes of patterns [13] but they do not have scale and translation invariance properties. However, with proper preprocessing translation and scale invariance can be achieved.

Zernike transform is performed to calculate Zernike moments [14] over a normalized image. The Zernike moments are a series of complex numbers. The magnitudes of Zernike moments are invariant to image rotation and can be used as watermark. Figure 5 shows the reconstruction results for image samples of English letters with Zernike moments of order 10, 20 and 40 [15].



Figure 5: Reconstructed images using zernike transform

### 2.6 Singular Valued Decomposition

Single valued decomposition [9][16][17] of a matrix X produces a diagonal matrix S of the same dimension as X, with nonnegative diagonal elements in decreasing order, and unitary matrices U and V so that

$$SVD(X) = [U S V] \text{ and } X = U^*S^*V'$$
(11)

Use of SVD in digital image processing [9] has some advantages. First, the size of the matrices from SVD transformation is not fixed. It can be a square or a rectangle. Secondly, singular values in a digital image are less affected if general image processing is performed. Finally, singular values contain intrinsic algebraic image properties.

#### 3. PROPOSED ALGORITHMS

#### 3.1 DCT Zigzag

The embedding of the watermark is done as follows:

Step 1: The normalized image is obtained by applying the image normalization method to the original image.

Step 2: The discrete cosine transform version of the normalized image is obtained and scanned in the zigzag manner. The watermark bits are embedded separately into the low, mid and high frequency coefficients of the normalized-transformed image. Step 3: The watermarked image is restored by inverting the normalized image through the inverse of the matrix in Step 1.

The extraction process is as follows:

Step 1: Normalized image of watermarked image is obtained.

Step 2: The inverse process of embedding is performed to extract the watermark

## 3.2 DCT Blocks

The embedding of the watermark is done as follows:

Step 1: The normalized image is obtained by applying the image normalization method to the original image.

Step 2: The normalized image is transformed to 8x8 DCT blocks.

Step 3: The watermark is embedded in to the low, mid and the high frequency bands separately.

Step 4: The watermarked image is obtained by normalizing the obtained image inversely.

The extraction process is as follows:

Step 1: Normalized image of watermarked image is obtained.

Step 2: The reverse process of the watermark embedding is performed to extract the watermark.

## 3.3 DWT

The embedding of the watermark is done as follows:

Step 1: The normalized image is obtained by applying the image normalization method to the original image.

Step 2: The normalized image is converted to frequency domain by applying DWT and images in four different bands are obtained (LL, LH, HL, and HH).

Step 3: The watermark is embedded separately in to the four bands.

Step 4: The watermarked image is restored by inverting the normalized image through the inverse of the matrix in Step 1.

The extraction process is as follows:

Step 1: Normalized image of watermarked image is obtained.

Step 2: The reverse process of embedding is performed to extract the watermark.

#### 3.4 Zernike Transform

The embedding of the watermark is done as follows:

Step 1: The normalized image is obtained by applying the image normalization method to the original image.

Step 2: Zernike transform is applied into the watermark image and Zernike moments are obtained. The Zernike moments are invariant to rotation and can be used as watermark and embedded into the normalized cover image.

Step 3: The watermarked image is restored by inverting the normalized image through the inverse of the matrix in Step 1.

The extraction process is as follows:

Step 1: Normalized image of watermarked image is obtained.

Step 2: The reverse process of embedding is performed to extract the watermark.

### 3.5 SVD-DCT

The embedding of the watermark is done as follows:

Step 1: The normalized image is obtained by applying the image normalization method to the original image.

Step 2: The normalized image is converted into frequency domain by applying DCT and is divided into blocks and a block is selected for embedding.

Step 3: The watermarking is done using the SVD and inverse normalization is applied on the obtained image.

The extraction process is as follows:

Step 1: Normalized image of watermarked image is obtained.

Step 2: The reverse process of embedding is performed to extract the watermark.

#### 4. EXPERIMENTAL RESULTS

A 256x256 gray scale images is taken as the cover image and watermark of size 64x64 is embedded into the cover image using the five methods (DCT Zigzag, DCT Blocks, DWT, Zernike Transform, and SVD-DCT). In the experiment Figure (6-a) and Figure (6-b) are used as cover images and Figure. (6-c) is used as the watermark.

Different attacks like noise, rotation, histogram equalization, contrast increase, contrast decrease, scaling are applied on the watermarked images. Peak Signal to Noise Ratio, Root Mean Square Error, Signal to Noise Ratio, Mean Square Error are calculated as the comparative measure.

It is observed that in DCT Zigzag and DCT blocks, embedding the watermark in mid ranges is more robust to attacks and in DWT, HL band show more robustness against attacks.



Figure 6: Cover Images (a) Lena (b) CBIT and Watermark Image(c) CS Logo

The watermarked images obtained using the five watermarking schemes with watermark strength 0.5 for Lena image are shown in Figure 7.



# Figure 2: (a-e) Watermarked images, (f-j) extracted watermarks

The watermarked images obtained using the five watermarking schemes with scaling factor 0.5 for CBIT image are shown in Figure 8.



Figure 8: (k-o) Watermarked images, (p-t) Extracted watermarks

The PSNR (dB) values for watermark embedding (Lena) using the five methods for watermark strengths (k) 0.1, 0.5 and 1 are shown in Table 1

Table 1:	<b>PSNR</b>	$(\mathbf{dB})$	values f	or	watermark	embedding
----------	-------------	-----------------	----------	----	-----------	-----------

Method k	DCT Zigzag	DCT Blocks	DWT	Zernike	SVD- DCT
0.1	35.2125	35.5116	34.4193	27.3629	33.1316
0.5	31.1475	35.1632	26.9455	27.2102	22.5418
1	26.7609	34.2370	21.8437	27.2069	16.8346

From Table 1, it can be observed that the PSNR value for cover image and the watermarked image decreases as the scaling factor value is increased. This is because the content of the watermark in watermarked image increases with scaling factor. Maximum value of PSNR is obtained for DCT Zigzag and DCT Blocks. Invisibility of the watermark which is the characteristics of the watermarking can be observed in all the five methods. The graphical representation of the PSNR values obtained for watermark embedding using the five methods is shown in Figure 9.



Figure 9: Watermark embedding

The PSNR (dB) values for watermark extraction (Lena) using the five methods for watermark strength (k) 0.1, 0.5 and 1 are shown in Table 2.

Table 2: PSNR (dB) values for watermark extraction

Method k	DCT Zigzag	DCT Blocks	DWT	Zernike	SVD- DCT
0.1	14.2837	13.7390	13.9483	13.3539	29.5668
0.5	13.9802	13.4656	13.6794	13.3536	34.4366
1	13.9145	13.4289	13.5960	13.3535	33.7098

From Table 2 it can be observed that the PSNR value for the original watermark and the extracted watermark increases as the scaling factor value is increased. Maximum PSNR value for extraction is obtained for SVD-DCT method.

The graphical representation of the PSNR values (Lena) obtained for watermark extraction using the five methods is shown in Figure 10.



Figure 10: Watermark extraction

In order to test the robustness of the watermarking schemes, different attacks like noise, rotation, histogram equalization, contrast increase, contrast decrease and scaling are applied on the watermarked image. After applying attacks, watermark is extracted from the watermarked image with noise.

The PSNR values calculated for original and extracted watermark after attacks for watermark strength are shown in Table 3.

Table 3: PSNR (dB) values for extraction after attacks

Method	DCT	DCT	DWT	Zernik	SVD-
Attack	Zigzag	Blocks		e	DCT
Noise	13.579	13.653	13.736	13.355	20.757
Rotation	13.791	13.495	13.808	13.354	33.473
Histogram Eq	13.832	13.509	13.741	13.352	12.335
Contrast Inc	13.603	13.569	13.577	13.354	-1.7206
Contrast Dec	13.534	13.441	13.561	13.355	-1.2062
Scaling	14.090	13.476	14.223	13.354	34.175

From Table 3 it can be observed that maximum PSNR value is obtained using SVD-DCT method. The SVD-DCT method is robust against the attacks noise, rotation and scaling. Negative PSNR values show that watermark cannot be easily extracted when attacks like contrast increase and contrast decrease attacks are applied on the watermarked image. The visibility of the extracted watermark obtained using the Zernike transform can be hardly recognized even the PSNR values obtained are similar to values obtained for DCT Zigzag, DCT Blocks, and DWT.

The graphical representation of the PSNR values obtained for watermark extraction after applying attacks using the five methods is shown in Figure 11.



Figure 11: Watermark extraction after applying attacks

## 5. CONCLUSION

The images are normalized to be invariant to the geometric attacks. The robustness of the watermarking schemes are verified by applying different attacks like adding noise, rotation, histogram equalization, contrast increase, contrast decrease and scaling. Peak Signal to Noise Ratio (PSNR) is used as a measure for comparing the original image and watermarked image, original watermark and extracted watermark. If the PSNR value is high then the algorithm is robust. Through implementation results, it is observed that embedding the watermark in mid frequencies using DCT Zigzag and DCT Blocks shows robustness to attacks. In DWT, embedding the watermark in Low-High (LH) and High-Low (HL) bands is robust to attacks. The zernike moments obtained by applying zernike transform to an image are invariant to rotation but, the reconstructed images are hardly recognized.

In the process of watermark embedding, the higher PSNR values are obtained for DCT Zigzag and DCT Blocks. But, the watermarks extracted using these two methods are hardly recognized compared to other extracted watermarks. In the process of extraction, the higher PSNR values are obtained for SVD-DCT watermarking scheme. DWT stands next SVD-DCT in PSNR values. In both the processes of embedding and extraction, the minimum PSNR values are obtained for watermarking using zernike transform.

After applying the attacks to the watermarked image, the watermark is extracted from the watermarked image with attack. It is observed that the PSNR values calculated for watermark extraction after applying attacks is high for SVD-DCT. The watermarking scheme is robust to all the attacks except contrast increase and contrast decrease. Again DWT watermarking scheme stands next to SVD-DCT in PSNR values and it is also observed that DWT shows uniform PSNR values for all the attacks which means that DWT is robust to all the attacks.

#### **6. REFERENCES**

- [1] L.ng-Tsun, Digital Watermarking for Multimedia Security management, Encyclopedia of Multimedia Technology and Networking, 2005.
- [2] T. Jack, Electronic Marking and Identification Techniques to Discourage Document Copying, IEEE Journal on Selected Areas in Communication, Vol. 13, No 8, pp. 1495-1503, 1995. C. Jermano, Assuring Ownership Rights for Digital Images, Proceedings of Reliable IT Systems, VIS '95, pp. 94-104, 1995.
- [3] Harsh K Verma, Abhishek Narain Singh, Raman Kumar, "Robustness of digital image watermarking techniques against brightness and robustness attacks", in International Journal of Computer Science and Information Security, Vol. 5, No. 1,2009
- [4] Deepak Sharma, "Classification of Image Watermarking Schemes", Center for Advanced Computer Studies, University of Louisiana at Lafayette, 2003.

- [5] Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC. IEEE, 2006.
- [6] Faraoun Kame, Mohamed1, Rabhi Abbes, "RST robust watermarking schema based on image normalization and DCT decomposition", in Malaysian Journal of Computer Science, Vol. 20(1), 2007 pp. 77 – 90.
- [7] Latha Parameswaran and K. Anbumani, "A Robust Image Watermarking Scheme using Image Moment Normalization", in World Academy of Science, Engineering and Technology 19 2006, pp. 112-116.
- [8] Hwan Il Kang, "Robust Watermarking Method Using the Image Normalization against the General Affine Transformation Attack", in International Conference on Intelligent Computing, August 23-26, 2005. HeFei, China pp. 170-175.
- [9] Say Wei Foo, Qi Dong, "A Normalization-based Robust Image Watermarking Scheme Using SVD and DCT", in International Journal of Information and Communication Engineering 6:4 2010 pp. 205-210.
- [10] Andrew B. Waton, "Image compression using the Discrete Cosine Transform", in Mathematica Journal ,1994, pp.81-88.
- [11] Natasa Terzija, Markus Repges, Kerstin Luck, Walter Geisselhardt, "Digital image watermarking using Discrete Wavelet Transform: Performance comparison of error correction code" in International Conference on Intelligent Computing, 2004.
- [12] Rafael C. Gozalez, Richard E. Woods, "Digital image processing", third edition.
- [13] Gholamreza Amayeh, Shohreh KAsaei, "Improvement of zernike moment descriptors on affined transformed shapes", in vision and computation, 2005, pp.462-469.
- [14] Say Wei Foo, Qi Dong, "A Normalization-based Robust Watermarking Scheme Using Zernike Moments", in International Journal of Computer and Information Engineering 3:4 2009 pp. 255-260.
- [15] Qing Chen, Xiaoli Yang, Jiying Zhao, "Robust Image Watermarking With Zernike Moments", in IEEE CCECE / CCGEI, Saskatoon, May 2005, pp 1282-1285.
- [16] Rafael C. Gozalez, Richard E. Woods, Steven L. Eddins, "Digital image processing using MATLAB", Prentice Hall, 2006.
- [17] Lijie Cao "Singular value decomposition applied to digital image processing", CISSE proceedings , 2006.