

# A Content Based Image Watermarking Scheme Resilient to Geometric Attacks

Latha Parameswaran, and K. Anbumani

**Abstract**—Multimedia security is an incredibly significant area of concern. The paper aims to discuss a robust image watermarking scheme, which can withstand geometric attacks. The source image is initially moment normalized in order to make it withstand geometric attacks. The moment normalized image is wavelet transformed. The first level wavelet transformed image is segmented into blocks of size 8x8. The product of mean and standard and standard deviation of each block is computed. The second level wavelet transformed image is divided into 8x8 blocks. The product of block mean and the standard deviation are computed. The difference between products in the two levels forms the watermark. The watermark is inserted by modulating the coefficients of the mid frequencies. The modulated image is inverse wavelet transformed and inverse moment normalized to generate the watermarked image. The watermarked image is now ready for transmission. The proposed scheme can be used to validate identification cards and financial instruments. The performance of this scheme has been evaluated using a set of parameters. Experimental results show the effectiveness of this scheme.

**Keywords**—Image moments, wavelets, content-based watermarking, moment normalization, geometric attacks.

## I. INTRODUCTION

THE growth of computer networks has resulted in the emergence of the Internet. With the proliferation of the Internet enormous volume of data has been stored in digital format. The nature of data such as text, images, video and audio, collectively known as multimedia data requires being stored in a highly secure manner due to its wide audience.

Digital watermarking is the process of embedding data (watermark) into a multimedia object in order to protect the owner's right to that object. The embedded data may be either perceptible or imperceptible. Some of the desired characteristics of watermarks are listed below [8] [9]:

- An imperceptible watermark must be invisible in both color and monochrome images
- The watermark should be spread in a large or important area of the image in order to prevent its deletion by clipping
- The watermark must be difficult to remove and removing the same should be more expensive and time consuming than purchasing the original image.

- The watermark should be inserted with little human intervention and labor
- The detection or extraction of the watermark should be possible in order to resolve any dispute.

Digital watermarks have three major application areas: data monitoring, copyright protection and data authentication. There are several types of watermarking systems that are categorized based on their inputs and outputs [4]:

*Private watermarking* systems require at least the original image. These systems extract watermark  $W$  from the possibly corrupted image  $I^*$  and use the original image as a hint to find where the watermark could be in  $I^*$ . Another category of systems also require a copy of the watermark for extraction but just yields a 'yes' or 'no' as answer to the query, "Does the Image contain a watermark?"

*Semi-Private watermarking* does not use the original image for detection but yields 'yes' or 'no'. These types of watermarks are used as evidence in court to prove ownership and copy-control applications such as DVD to verify the authenticity of the owner to play the content.

*Public Watermarking* is the most challenging scheme, as it requires neither the source image  $I$  nor the watermark  $W$ . These systems extract exactly a set of bits of information (namely the watermark) from the watermarked image. These schemes are also called *blind* watermarking.

*Asymmetric Watermarking* has the property that any user can read the watermark, without being able to remove it.

Digital watermarking schemes available in literature satisfy many of the above characteristics and are considered to be a helpful technology for securing multimedia data [8] [9] [10] [11].

Robust watermarking is still an important issue as there are already sets of attacks and new attacks will appear in future. Attacks on multimedia data can be broadly categorized into four classes [1]:

- Removal attacks such as lossy compression (JPEG), filtering, de noising and sharpening
- Geometrical attacks such as warping and jitter
- Protocol attacks such as copy attack and watermark inversion
- Cryptographic attacks such as key search and oracle attacks.

Of all these, removal attacks are less challenging and easy to handle. Geometrical attacks are a serious problem and there are not many techniques that have handled this attack. Ruanaidh and Pun [2] have presented a Rotation, Scaling and

Latha Parameswaran is with the Amrita Vishwa Vidyapeetham, Coimbatore, India (phone: 91-422-2656422; e-mail: p\_latha@ettimadai.amrita.edu).

Dr. K. Anbumani is with the Karunya Deemed University, Coimbatore, India (Phone: 91-11-2614370, e-mail: anbumani\_k@yahoo.co.uk).

Translation resilient watermarking scheme based on Fourier-Mellin transforms. Alhoniemy and Twefik [3] have been proposed a method using moment normalization to recover geometrical transformations. The major drawback of their scheme is: (i) it does not preserve image fidelity as it creates contrast variations in the watermarked image (ii) its inability to tolerate changes in aspect ratio and cropping.

The scheme discussed in this paper is a blind (public) watermarking scheme, which does not require either the source image or the watermark to detect the presence of a watermark. This paper will focus on resistance to incidental attacks including the removal attacks and geometrical transformations, and resistance to malicious attacks. The proposed watermarking scheme consists of four major steps: (1) Image Normalization (2) Content-Dependent watermark generation and (3) Watermark Embedding and (4) Watermark Extraction.

This paper is organized as follows: Section II discusses the proposed watermarking scheme. Section III deals with the performance evaluation of the scheme and Section IV shows the experimental results.

## II. THE PROPOSED WATERMARKING SCHEME

In this proposed scheme the watermark is the features derived from the image and is imperceptibly embedded in the image itself. This proposed algorithm works in the discrete wavelet transform domain. Images are connected regions of similar texture and gray level that combine to form objects Grabs [13] has discussed that wavelet transforms are best suited for image analysis. Using wavelet transformations (i) if objects are small in size or low in contrast, it is possible to examine them at high resolution; (ii) if objects are large in size or high in contrast, they can be examined at coarse view; (iii) if objects have combinations, they can be studied at various resolutions. Wavelet is a mathematical function that cuts data into different frequency components and study each component with a resolution matched to its scale [12]. Wavelet functions are useful to analyze the discontinuities and sharp spikes of the signal. Wavelets use filter banks for image analysis. Discrete Wavelet Transform with PSNR > 40dB, the original and reconstructed images are visually indistinguishable to the human observer. Wavelets are much powerful due to their multi resolution analysis capability, which means using the sub band coding features undetected in one resolution may be easily detected in other resolutions [13].

Although Discrete Cosine Transform (DCT) is a better transformation for image analysis, it has a few disadvantages: inside a DCT block only spatial correlation is considered; also correlation from neighboring blocks is ignored and boundary correlation is not possible. It produces undesirable blocked artifacts. DCT uses a fixed function for transformation and not suitable for binary images which have large periods of constant amplitude followed by brief periods of sharp transitions (ex: fax documents)

The Discrete Wavelet Transform (DWT) is a better alternate to DCT due to its advantages as: there is no requirement to divide the input image into non-overlapping 2-D blocks and allows localization in both time and spatial frequency. It transforms the whole image and not on block by block basis. It uses inherent scaling with a high compression

ratio. It also provides higher flexibility in choosing the type of wavelet function such as Daubechies, Coiflet, Harr, Marr, Morlet, etc [12]. It can scale up, to produce changes smoothly and obtain low frequency details. Wavelets can also scale down to produce rapid changes and obtain high frequency details. Fig. 3 shows the multi resolution transformation of the wavelet transformation for an image.

The steps of this proposed watermarking algorithm is shown below. The source image  $I$  is of size  $n \times n$ . The content based watermark is represented as  $W$ . The watermarked image is represented as  $I^*$ .

1. Perform Moment Normalization of the Source Image
2. Compute the Discrete Wavelet Transform
3. Compute the content dependent watermark.
4. Perform Watermark Embedding
5. Perform Inverse DWT. This is represented as  $I_m$
6. Perform inverse moment normalization. This represents the watermarked image  $I^*$ .

### A. Image Moment Normalization

The source image is normalized based on its central moments. Moment normalization is much a useful technique as the moments of an image is used to describe its contents with respect to its axes. Moments can be used to characterize images and to express properties that have analogy in statistics. Moment Normalization is done mainly to resist geometrical attacks [5] [6]. The steps of image moment normalization are below:

1. Compute the centroid of image  $I$   

$$\bar{x} = M_{10} / M_{00}$$

$$\bar{y} = M_{01} / M_{00}$$

where  $M_{ij}$  is defined as

$$M_{ij} = \sum \sum x^i * y^j * I(x,y)$$

2. Compute the central moments

$$\mu_{ij} = \sum \sum (x - \bar{x})^i * (y - \bar{y})^j * I(x,y)$$

3. Compute the covariance matrix for the moments.

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

This matrix is represented as CoV

4. Compute the eigen vectors of CoV

$$\begin{pmatrix} e_1x & e_1y \\ -e_1y & e_1x \end{pmatrix}$$

and the eigen values of CoV

$$\lambda_i = \frac{1}{2} * (\mu_{20} + \mu_{02}) \pm \sqrt{(4\mu_{11}^2 + (\mu_{20} - \mu_{02})^2)}$$

5. Compute the orientation angle

$$\theta = \frac{1}{2} * \tan^{-1} (2 \mu_{11} / (\mu_{20} - \mu_{02}))$$

6. Compute the rotation matrix **R** as

$$\begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$$

7. Compute the scaling matrix **S**

$$\begin{pmatrix} (\lambda_1 \lambda_2)^{0.25} / \sqrt{\lambda_1} & 0 \\ 0 & (\lambda_1 \lambda_2)^{0.25} / \sqrt{\lambda_2} \end{pmatrix}$$

8. The translation matrix **T** is the eigen vector of CoV

9. Construct the moment normalized image

$$I_m = R S T * I(x,y)$$

Thus the source image is moment normalized, so that it can withstand affine transformation attacks. Further details of image normalization using central moments are available in [1] [3].

#### B. Generation of Content Dependent Watermark

Wavelet transforms are perhaps a better method to analyze and understand the image [7]. Hence this scheme uses the wavelet domain to construct a content dependent watermark. The source image is transformed using the Daubechies discrete wavelet transformation (DWT) up to level - 2. The coefficients in the level - 2 are considered for modulation to insert the watermark. The watermark construction algorithm is shown below:

1. Segment the level - 1, approximation band into 8 x 8 blocks
2. Compute the product of mean and standard deviation of each block, represented by Pi
3. Construct the second level DWT
4. Segment the level - 2, approximation band into 8 x 8 blocks
5. Compute the product of mean and standard deviation of each block, represented by Qi
6. Compute the difference between P and Q, represent as the watermark Wi, for the i<sup>th</sup> block.
7. Modulate the middle frequency coefficients of the i<sup>th</sup> block with Wi
8. The watermark Wi is adjusted to the corresponding block coefficients in the mid frequency components of the wavelet transformed image in level - 2 blocks denoted by I<sub>22</sub> and I<sub>23</sub>:  

$$I_{22} = \text{sign}(I_{22}) * W_i * \alpha \quad (\text{Low High Band})$$

$$I_{23} = \text{sign}(I_{23}) * W_i * \alpha \quad (\text{High Low Band})$$
9. Repeat modulating all the blocks in second level DWT
10. Reconstruct the image by performing inverse wavelet transform

Thus content dependent watermark is constructed and the watermark is embedded in the mid frequency coefficients in the wavelet domain.

#### C. Inverse Moment Normalization

The modulated image is inverse moment normalized by computing the inverse of the rotation, scaling and translation matrices **R**, **S** and **T**. The watermarked image **I\*** is constructed and sent to the receiver.

$$I^* = R^{-1} * S^{-1} * T^{-1} * I_m$$

#### D. Watermark Detection

Watermark detection is fairly a simple process. The received image is sent to the detection algorithm. The same steps as that of insertion are followed and the hidden watermark is extracted from the Level -2 coefficients. The watermark is also constructed simultaneously. The extracted and constructed watermarks are compared. If they compare favorably, the image is said to be authentic else the image is declared as tampered. Computing the correlation coefficient between the extracted and the generated watermarks the comparison of the watermarks can be done. The formula for calculating the correlation coefficient given below:

$$\rho = \frac{\sum xy - \frac{\sum x \sum y}{n}}{\sqrt{\left( \sum x^2 - \frac{(\sum x)^2}{n} \right) \left( \sum y^2 - \frac{(\sum y)^2}{n} \right)}}$$

If the correlation coefficient is nearly +1, the watermark can be considered as correctly recovered and if the correlation coefficient is less than +1, the watermark can be considered as tampered and hence the image can be declared as attacked.

#### E. Parameters to be Considered for Watermarking

Kutter and Petitcolas [4] have discussed a set of parameters for designing a watermarking system. The following are the set of parameters to be considered for watermarking:

- *Amount of embedded information* is an important parameter as it directly influences the watermark robustness. The more the information to embed, the lower the watermark robustness.
- *Size and Nature of Image* plays a vital role on the watermark robustness. Internet uses a lot of small size images, which need to be secured. Although very small pictures have not much of commercial value, watermarking scheme should be able to recover watermark from them.
- *Secret Key* has no direct impact on the image fidelity, but plays an important role in the security of the system. The key space must be very large to make exhaustive search attacks impossible. Many security systems fail due to improper choice of secret key.

#### F. Applications

This proposed scheme finds its place in a wide range of applications wherever images are of the essence. Major applications are in validating identity cards, debit and credit

cards, voter identity cards, driving licenses and employee identity cards. Another major application is in authenticating financial instruments such as fixed deposit receipts and financial stocks.

### III. PERFORMANCE EVALUATION

The proposed scheme is a blind watermarking scheme and hence, the watermark extraction procedure can be done without using the original image. The effects of various types of attacks on the proposed scheme are analyzed.

#### A. Resistance to Geometric Attacks

This scheme has the ability to withstand geometrical attacks. As the scheme does block transformation, the scheme can resist the removal of rows or columns and also shifting row or column. In order to withstand other global transformations, moment normalization has been employed so that the image can be transformed to a canonical form before embedding and detection are performed. As the embedding procedure is based on the features of block and moment normalization, this scheme is able to resist geometric distortions including scaling, change of aspect ratio, line removal, flipping and rotation.

#### B. Benchmarking and Performance Evaluation

This section deals with the benchmarking parameters used to verify the robustness of the scheme. Kutter and Petitcolas [4] have discussed a number of parameters benchmark any watermarking scheme. For fair benchmarking and performance evaluation, the visual degradation due to embedding is an important issue. Most distortion measures (quality metrics) used in visual information processing belongs to a group of *difference distortion measures*. Table I lists the commonly used measures. Let  $I$  denote the source image of size  $m \times n$  and  $I^*$  denote the watermarked image of same size.

TABLE I  
COMMONLY USED PIXEL-BASED DISTORTION METRICS

Pixel Based Metrics	
Mean Square Error (MSE)	$1/mn * \sum(I - I^*)^2$
Signal to Noise Ratio (SNR)	$\sum I^2 / \sum(I - I^*)^2$
Peak Signal to Noise Ratio	$mn * \max(I^2) / \sum(I - I^*)^2$
Image Fidelity	$1 - \sum(I - I^*)^2 / \sum I^2$
Correlation Distortion Metrics	
Normalized Cross Correlation	$\sum I I^* / \sum I^2$
Correlation Quality	$\sum I I^* / \sum I$

#### C. Acceptable Attacks

This proposed scheme can resist the attacks listed below. These attacks may be malicious or intentional. The effect of each attack is also given.

- **JPEG Compression** – JPEG is currently one of the most widely used compression algorithm for images and any watermarking scheme should be resilient to some degree of compression. This scheme is capable of tolerating compression.

- **Geometric Transformations:**

- **Horizontal Flip and Vertical Flip-** Images can be flipped horizontally or vertically without losing any value.
- **Scaling-** When a printed image is scanned at high resolution, scaling occurs. Scaling can be uniform or non-uniform and can be in horizontal or vertical direction. This is called as change in aspect ratio.
- **Deletion of rows or columns-** Removal of certain rows or columns is a very common attack, which is not resilient in many watermarking systems.
- **Random Geometric Distortions-** Adding random noise to images can disrupt the hidden watermark.

- **Enhancement Techniques**

- **Low pass filtering-** The application of filters such as median, Gaussian and standard average filters is called low pass filtering
- **Sharpening-** These filters are an effective attack as they are very effective in detecting high frequency noise introduced by some digital watermarking software.
- **Histogram modification-** This includes histogram stretching or equalization, which are sometimes used to compensate poor lighting conditions
- **Gamma Correction-** This is a very frequently used operation to enhance images or adapt images for display after scanning
- **Noise Addition-** Additive noise such as Gaussian noise, salt and pepper noise are acceptable by many watermarking systems. But the level of acceptance has to be mentioned by the scheme.

### IV. EXPERIMENTAL RESULTS

This section discusses the experimental results of the proposed scheme. The algorithm has been implemented using Matlab 6.5 and the attacks on the images have been done using Adobe Photoshop 7.0. The algorithm has been tested on three categories of images namely standard images, natural images and images created using the imaging tools.

#### A. Watermarking Parameters

The cover images considered for the verification of this scheme is Lena, Baboon and clown. The watermarking parameters are assumed as below:

1. **Amount of embedded information:** In this scheme, the number of  $8 \times 8$  blocks in level -2 of the DWT image is the size of watermark.
2. **Size and Nature of Cover Image:** This proposed scheme is applicable to all gray scale images are of size  $512 \times 512$ .
3. **Secret Data:** The difference between the product of mean and standard deviation in the two levels of discrete wavelet transformed image.

**B. Watermarking Scheme**

This section shows the images before and after watermarking. This watermarking scheme has been tested on a set of gray scale images of size 512 x 512. The results for various categories of have been chosen. The categories are standard images; photographs of nature and images created using imaging tools are shown below.

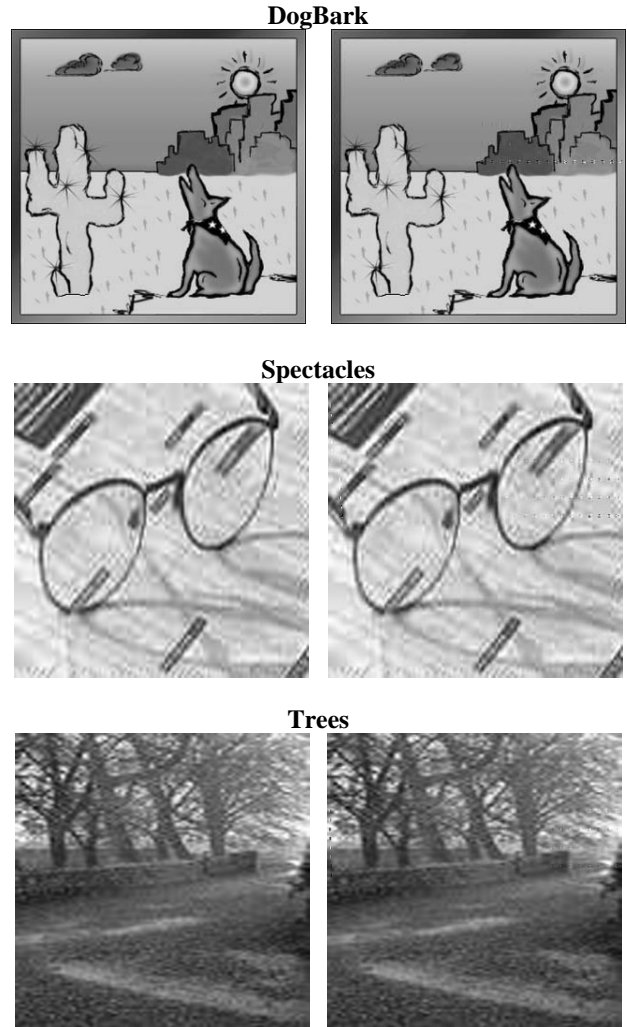
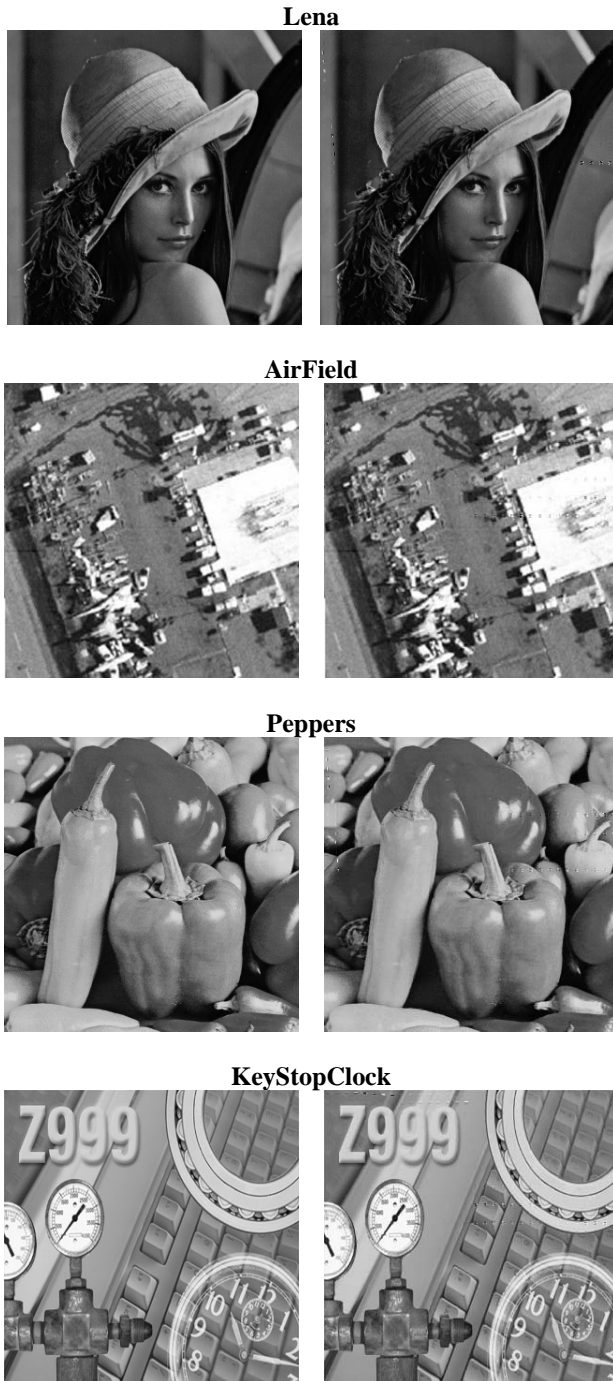


Fig. 1 Images before and Watermark Insertion

**C. Performance Evaluation without Attacks**

The various performance evaluation metrics have been listed in Table I. The values of these metrics for the test images are shown in Table II. The results have been obtained by comparing the cover images with the watermarked images. Table II shows that all these metrics fall within a small range and hence the watermarked image and the original image do not have much of visual degradation.

TABLE II  
PERFORMANCE EVALUATION WITHOUT ATTACKS

Images	MSE	IF	PSNR	NCC
Lena	0.008	0.9998	45.03	1.00
AirField	0.01	0.9998	41.09	1.00
Peppers	0.016	0.9999	42.80	1.00
KeyStopClock	0.018	0.9997	41.38	1.00
DogBark	0.007	1.00	45.42	1.00
Specs	0.01	1.00	43.82	1.00
Trees	0.007	1.00	43.82	1.00

Table II shows that, the scheme is capable of accepting modulations through watermark embedding in any type of

images. Experimental study of the scheme has been on all these three types of images. The watermark extraction results of these images are shown in Table III. The watermark extraction scheme is validated by computing the correlation coefficient between the embedded and the extracted watermark in the wavelet domain.

TABLE III  
WATERMARK COMPARISON

Images	CC
Lena	0.8729
AirField	0.8155
Peppers	0.9027
KeyStopClock	0.9625
DogBark	0.9514
Specs	0.9758
Trees	0.9803

From Table III, it can be inferred that the proposed watermarking scheme is capable of extracting watermark without appreciable error.

#### D. Performance Evaluation with Attacks

The various types of attacks discussed earlier have been done on this same set of watermarked images. The arrived results are tabulated in Table IV with the attacks on Lena. Table IV shows that the scheme tolerates the attacks discussed and hence the scheme is robust not only against compression attacks but also against geometric attacks. The results also show that the scheme can withstand these attacks if done either incidentally or maliciously. Similarly results have been verified for other test images.

TABLE IV  
PERFORMANCE EVALUATION WITH ATTACKS

Lena Attacks	MSE	PSNR	IF	NCC
JPEG (Medium Compression)	0.1040	43.39	0.9982	1.0020
Horizontal Flip	0.0356	41.51	0.9994	1.0049
Vertical Flip	0.0443	41.41	0.9993	1.0054
Random Noise	0.0996	46.41	0.9983	0.9959
Median Filter (3 x 3)	0.0773	43.16	0.9987	1.0008
Gaussian Noise (1%)	0.0378	43.80	0.9977	1.0089
Sharpen	0.0816	42.56	0.9986	0.9991
Histogram Modification	0.0219	45.99	0.9980	1.0324
Gamma Correction	0.0900	42.27	0.9992	1.0023
Salt and Pepper	0.0806	42.77	0.9986	0.9998

#### V. CONCLUSION

The aim of this proposed algorithm is to construct a robust watermarking scheme that can withstand compression, enhancement and geometrical attacks. Discrete Wavelet Transforms have been used to extract features to serve as the contents of the watermark. The concept of central moment normalization is to make the scheme withstand various geometric attacks. Performance of this scheme has been estimating the pixel-based metrics and correlation based

metrics. This scheme is robust against content preserving modifications and easily identifies any content changing modifications. This scheme can be extended to withstand copy attack and cropping attack. Also protocol attacks and cryptographic attacks needs to addressed.

#### REFERENCES

- [1] Tuang-Lam Le and Thi-Huango-Lan Nguyen, "Digital Image Watermarking with Geometric Distortion Correction using the Image Moment Theory", *International Conference, RVIF*, Hanoi, Feb 2004.
- [2] J J K O' Ruanaidh and T Pun, "Rotation Scale and Translation invariant spread spectrum digital watermarking" *Signal Processing*, 1998.
- [3] M Alghoniemy and A H Tewfik, "Geometric distortion through Image Normalization", *Proceedings of International Conference on Multimedia Expo*, 2000.
- [4] M. Kutter, F A P Petitcolas, "A Fair Benchmark for Image Watermarking Systems", *Electronic Imaging, The International Society for Optical Engineering*, Jan 1999.
- [5] M Alghoniemy and A H Tewfik, "Image Watermarking by moment Invariants" *Proceedings of IEEE international conference on Image Processing*, Vancouver, 2000.
- [6] P Bas, J M Chassery and B Macq, "Geometrically Invariant Watermarking using Feature Points", *IEEE Trans. on Image Processing*, Vol. 9, 2002.
- [7] Latha Parameswaran, "Content Dependent Image Signature for Authentication Using Wavelets", *Proceedings of NCIS*, Karunya Deemed University, Coimbatore, Nov.2005.
- [8] Raymond B Wolfgang and Edward J Delp, "Overview of image security techniques with applications in multimedia systems", *ACM Multimedia Workshop*, pp. 303 – 310, 2000.
- [9] Chai Wah Wu, "On the design of Content-Based Multimedia Authentication Systems", *IEEE Transactions on Multimedia*, vol. 4 No.3, Sep 2002, pp. 385 – 393.
- [10] Chai Wah Wu, "Limitations and requirements of content-based multimedia authentication systems", *Proceedings of SPIE* vol. 4314, 2001, pp. 241 – 252.
- [11] J Cox, J Kilian, T Leighton and T Shamoon, "Secure Spread Spectrum Watermarking", *IEEE Trans. on Image Processing*, Vol. 6 no. 12, 1997, pp. 1673-1687.
- [12] Gonzalez and Woods, "Digital Image Processing", *Prentice Hall*, 2000.
- [13] Amara Graps, "An Introduction to Wavelets, *IEEE Trans. On Computational Science and Engineering*", 1995, pp 77-86.