Image Adaptive Watermarking Using Feature Point Extraction Model

Yarabham Gangadhar[1]*   **Venkata Sesha Giridhar Akula[2]**   **Chenna Reddy Pakanati [3]**

[1]Department of CSE, Jawaharlal Nehru Technological University, Hyderabad, India
[2]Methodist college of Engineering and Technology, Hyderabad, India
[3]Department of CSE, Jawaharlal Nehru Technological University Ananthapuramu, Anantapur, India

* Corresponding author's Email: ygdhar@gmail.com

Abstract: Watermarking is one of the efficient approaches for digital authentication. An adaptive feature point extraction model is proposed in this paper for robust watermarking. The host image is treated with number of geometric attacks for extracting the consistent feature points form the image. The proposed watermarking scheme follows the adaptive feature point extraction method to retrieve the feature points from the host image. The response value of the feature points is calculated for improving the selection of feature points. The watermark insertion procedure is employed by inserting the watermarking bits with in the place of feature points. The feature point portion is extracted from the image and replaces the portion with watermarking bits. The watermark extraction procedure is used to restore the original image from the watermarked image. The watermarking bits in the image are replaced by the feature point portion for restoring the original image. The simulation experiment is carried with the MATLAB simulator. The proposed algorithm is tested with geometric attacks such as scaling, rotation, noise pollution and JPEG compression. The proposed method proved its efficiency when compared to other remaining algorithms.

Keywords: Feature point extraction, Geometric attacks, Image, Robust, Watermarking.

1. Introduction

Image Authentication and privacy protection plays a major role in the field of multimedia. The major advantages of digital watermarking are content authentication, copyright protection and content description. In the current trend, the watermarking schemes are concentrated on the invisible and robust image watermarking. The defence against geometric attacks is problematic and perplexing.

Geometric attacks had the ability to change the physical position and pixels spatial positions of watermark when compared to the common signal processing attacks. The geometric attacks destroy the synchronization behaviour of the image which is very crucial for the watermarking algorithms. To defend the geometric attacks, some of the mechanisms are already implemented. Lin et al. [1] presented the 1-dimentional watermarking mechanism for defending the RST attacks (rotation, scaling and transformations). The implementation is explained with simple mechanism and more enhancements are needed. Lu et al. [2] proposed the hash based mechanism for image watermarking. They claimed that this mechanism is resistant with estimation attacks and geometric attacks. But the cons of the hash based mechanism are the complexity of the procedure and it is not suitable for the real time applications. Kang et al. [3] proposed the informative watermarking which is robust against the JPEG compression and affine transformation; still it is need to be proved against the median filtering.

Meanwhile, image histograms are not sensitive to the geometric transformations [4]. Some of the algorithms are proposed for histogram based image watermarking which can defend against the geometric attacks. To defend against the geometric distortions, pun et al. [5] proposed the histogram based watermarking scheme in DWT domain for

grey scale images using the intensity level histograms and block based histograms. The proposed approach works with image cropping, scaling, JPEG compression and flipping, but it failed with image rotation. An invariant image watermarking scheme was proposed by Xiang et al. [6] for defending the geometric attacks. The proposed method utilizes the Gaussian filtered components and the histogram shape of images for effective handling of image distortions. In the watermarked images, the watermark can be detected by the private key without the help of original images. A reversible blind image watermarking algorithm was proposed by Lee and Kim, [7] for preserving the secret key. The proposed algorithm utilizes the binary information of the watermark which is to be embedded in the Discrete Fractional Random Transform (DFRT) domain. The retrieving of the original image from the watermarked image is very complex in the proposed procedure. If there is any small error in the DFRT function, it is not possible to retrieve the original image from the transformed image.

In this paper, we made a contribution to extract the feature points using image adaptive watermarking scheme. The approach calculates the response value of each point in the host image and orders them in the descending order. Based on these response values, the watermarking insertion and watermarking extraction procedure has been carried out.

The rest of the paper is organized as follows. Section 2 deals with the related work regarding the existing watermarking techniques. Section 3 deals with histogram invariant transformations for geometric attacks. Section 4 deals with the adaptive feature point extract model based on response values. Section 5 and 6 explains about the watermarking insertion and extraction rules. Section 7 presents the simulation experiments carried out with the MATLAB 2013. Finally the conclusion is presented in section 8.

2. Related Work

The robust watermarking technique is an efficient approach for preserving the privacy in the digital world. Lot of research has been done in the recent years regarding the watermarking approaches. In [14], Tsai et al. proposed optimal feature region selection based on the corner response. This method doesn't guarantee the robustness due to the expose of feature points for the increase of watermarking quality. The expose of feature points causes the geometric attacks on the images. In [15], Priya et al.

proposed the robust watermarking scheme against the rotation invariant attacks. A Bayesian segmentation method is used for segmenting the image for homogeneous areas. After selecting the homogeneous areas, the feature points are extracted using the Gaussian rule. This method shows the improved results against the noise pollution in the images. But, this method is not concentrated on rotation, scaling and transformation attacks. In [16], Gao et al. proposed affine transformations for extracting the feature points form the watermarking image. The affine transformations find the non-overlapping regions in the image and transform the ellipses in to circles for better quality insertion of the image. The major drawback of this method is, it will not have good performance against the geometric attacks. In [17], Yuan et al. proposed Robust Feature Point Extraction (RFPE) model for image watermarking. In order to extract the feature points from the proposed model, they used the Scale Invariant Feature Transform (SIFT). The SIFT points are used for inserting the watermark into the image. This method is tested under different geometric attacks and signal processing attacks. The proposed method achieved better results against the different types of attacks. This method is not sufficient to address the transformation issues which arise at the time of watermark insertion.

3. Histogram Invariant for Geometric Transformations

The geometric transformations are defined as the set of parameters decides the operation which has to be performed on the host image. In general, the geometric transformations are divided in to three categories [8] such as non- invertible attacks, local invertible attacks and global invertible attacks. The non-invertible attacks are those applied using cropping. The original image cannot be recovered once the partial part of the image is modified. The local invertible attacks are given as random displacement, random bending attacks, curved transform, bilinear transform, high linear bending and global bending. The global invariant attacks are rotation, scaling and transformation which are also called as affine transformations. The image distortions are categorized in to two types, one is alteration of pixel values in the image and another is shifting of pixels in the image.

With watermarked images attacks such as scaling and rotation, the position of the pixel is moved but not the watermark information. But, when image is prone to shearing attack there is a partial loss in the watermark information.
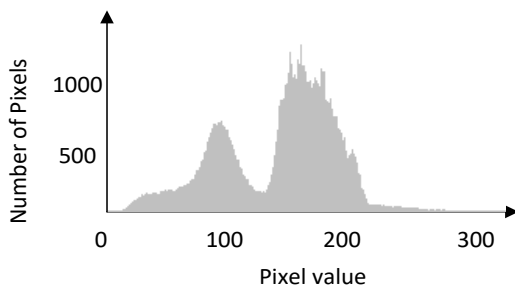
Figure. 1(a) Original Image of City

Figure. 1(b) Histogram Representation

This leads to the failure condition of watermark extraction from the image. Image histogram represents the ratio of number of pixels and the level of grey scale. Though, there is a change in the number of pixels, the histogram remains static. In this paper, we are considering 256 grey level images for histogram representation. To understand the image histogram in a detailed way, the original image of city and the corresponding histogram are given in Figure 1(a) and 1(b).

4. Adaptive Feature Point Extraction Model

The adaptive feature point extraction model was developed by modification of traditional Harris and Stephens method [9]. This method uses the salient features of the image to extract the feature points. In our proposed feature point extraction model, in order to extract the feature points the detailed steps that are followed are given in algorithm 1. First, the simulated attacked image has been given as input to the algorithm. Then, extract the feature points within the image. As a next step, for the image, the algorithm calculates the response threshold value and adjusts the image pixels based on the number of watermarking bits. After calculating the response

value to all the feature points, then the feature points with highest value is selected for watermarking.

Algorithm 1: Adaptive feature point extraction model

Input: Image which is prone to simulated attacks
Output: K number of feature points extracted

Begin
1. Initialize the host image
2. Initialize the threshold value for extracting the feature points. The threshold value limits the feature points which can be neither too high nor too low. The threshold value is taken as 10.
3. Compute the response value for each extracted point. Then, arrange the extracted points according to the descending order based on the response value.
4. Select the extracted points with highest response value and form as a dataset.
5. Remove the adjacent points in the image which are having the highest value on the data set.
6. Count the number of extracted points with in the dataset.
7. According to K, adjust the threshold value.
End

The proposed algorithm has a robust and stable mechanism when compared to the other existing algorithms. The algorithm extracts the feature points for reliable watermarking in the image. Algorithm 2 shows the calculation of response values to the extracted feature points. Based on the response value, the feature points are selected for the watermarking. Here X and Y represent the coordinates of the image, α represents the feature points extracted from Algorithm 1. P, Q and R are the calculated coordinates from the image. 'w' represents the predefined window of size 3×3. M is the determinant value, N is the trace value, L is the constant value which ranges from 0.03 to 0.06 and V is the feature point response value.

Algorithm 2: Feature points response value [9]

Begin

1. Calculate the x and y coordinates of the image

$$X = \alpha \times (-1,0,1) \approx \frac{\partial \alpha}{\partial x}$$

$$Y = \alpha \times (-1,0,1)^T \approx \frac{\partial \alpha}{\partial y}$$

$$(1)$$

2. Calculate the sum of product of the coordinates of the pixels in the image.

$$P = X^2 \times w$$

$$Q = Y^2 \times w$$

$$R = (XY) \times w \tag{2}$$

3. Assign P, Q and R values to the 2×2 matrix and calculate Z for each point.

$$Z = \begin{pmatrix} P & R \\ R & Q \end{pmatrix} \tag{3}$$

4. Compute the det value to the matrix Z.

$$M = \det(Z) = P \times Q - R^2 \tag{4}$$

5. Compute the trace value to the matrix Z.
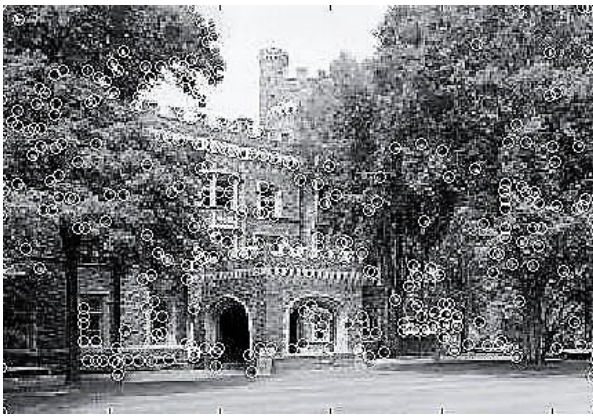
$$N = Tr(Z) = P + Q \tag{5}$$

6. Finally, calculate the response value of each feature point using the formula given in equation 6.

$$V = M - L \times N \tag{6}$$

Where L is the constant value and it is range from 0.03 to 0.06.
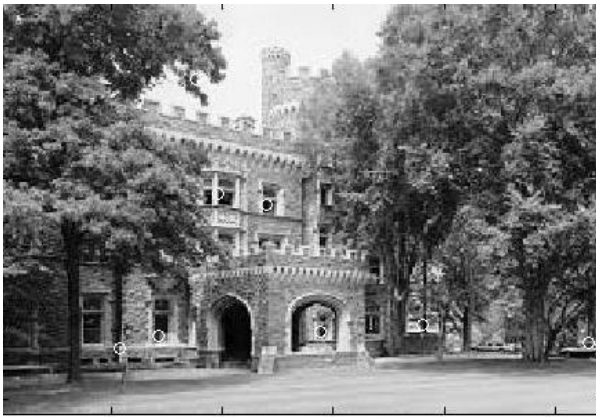
End

(a)

(b)

(a1)

(b1)

Figure. 2(a) and 2(b) feature point extraction with an existing method. 2(a1) and 2(b1) Feature point extraction with proposed method
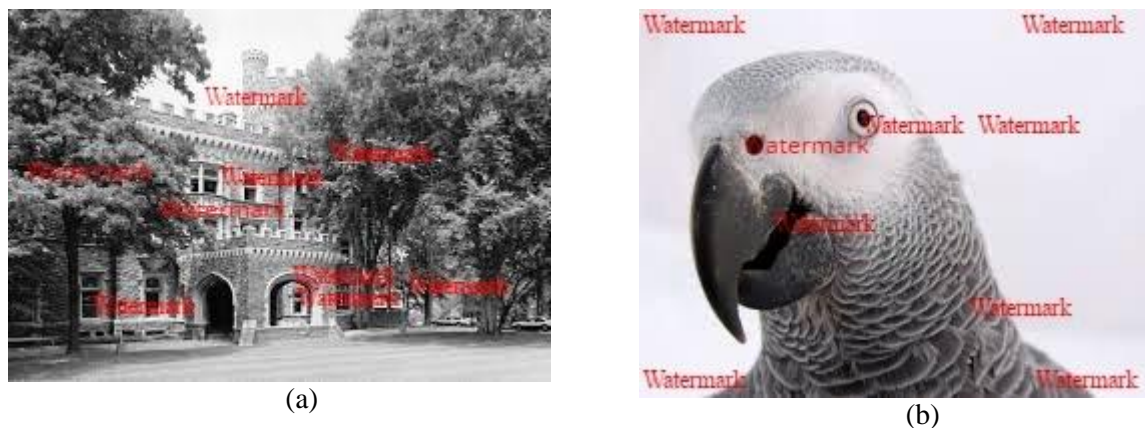
(a)

(b)

Figure. 3(a) and 3(b) Watermarking insertion images using the proposed method

(a)

(b)

Figure. 4(a) and 4(b) Watermark extracted images using the proposed method

Figure 2 shows the feature point extraction in the existing method and the proposed adaptive feature point model. In both the algorithms, the threshold value is taken as 10. Figure 2(a) and 2(b) shows the feature point extraction of the original images which adapts the traditional existing method (Harris and Stephens, 1988) and the Figure 2(a1) and 2(b1) shows the feature point extraction by adapting the proposed feature point extraction method.

5. Watermarking Insertion Rule

The feature points extracted from the proposed algorithm are more robust and secure. But, there is a chance of exposing to the high signal and geometric attacks. So, a histogram based insertion procedure is employed for inserting the watermark in to the image. This method considers the extraction of the feature points from the image and replaces them with watermarking. Algorithm 3 shows the complete procedure of watermark insertion in the image. As an initial step, the feature point's extracted image is given as input to the algorithms (i.e., K feature points are extracted from the image) and identify the

region where the watermark has to be inserted. Then, replace the region with the watermarking portion. The number of feature points K is equal to the number of watermarking bits and then only we can replace the feature points with the watermarking bits. The process of inserting the watermarking bits is done by using the histogram based embedding algorithm [10].

Algorithm 3: Watermark Insertion

Step 1: Identify K number of feature points from the algorithm 1

Step 2: Find out the central point to the image and calculate the Euclidian distance from the central point to the extracted feature points.

$$ED = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \tag{7}$$

Here x_1 and y_1 are the central point coordinates and x_2 and y_2 are the feature point coordinates.

Step 3: Identify the four feature points with highest Euclidian distance from the central point.

$$FP1 \geq FP2 \geq FP3 \geq FP4 \geq FP5 \qquad (8)$$

Step 4: Calculate the slopes for the four feature points from the central point.

$$S1 = \frac{(y_2 - y_1)}{(x_2 - x_1)},$$

$$S2 = \frac{(y_3 - y_1)}{(x_3 - x_1)},$$

$$S3 = \frac{(y_4 - y_1)}{(x_4 - x_1)},$$

$$S4 = \frac{(y_5 - y_1)}{(x_5 - x_1)} \qquad (9)$$

Step 5: Create the square regions for feature points which is identified at step 3, these square regions are used for inserting the watermark.

Step 6: Insert the watermark bits in to the square regions of the image.

Step 7: Substitute the extracted squared region with corresponding watermarking region and finally it generates the water marked image.

Step 8: Encrypt the extracted feature points and calculated slopes s1, s2, s3 and s4 as a key for extracting the watermarked image.

6. Watermarking Extraction Rule

The watermarking extraction procedure is used to extract the watermark bits from the host image. The watermark bits are extracted based on the keys to restore the original image. The regions which are extracted from the feature points act as the keys for the decryption of the image. Algorithm 4 shows the procedure of watermark extraction from the image. As an initial step, the watermark image is given as input to the algorithm. Then apply the adaptive feature point extraction model for identifying the feature points in the watermarked image. Then, replace the watermark bits with the key which was extracted from the algorithm 3. Finally, the original image will be restored. Figure 4 shows the original images after watermark extraction.

Algorithm 4: Watermark Extraction

Begin

Step 1: Decrypt the key to retrieve the feature points and slopes s1, s2, s3 and s4.

Step 2: Apply the algorithm 1 for watermarked image for extracting the feature points $X^{'}$.

Step 3: Find out the central point ED' to the image and calculate the Euclidian distance from ED to the extracted points.

Step 4: Identify the four extracted points with the highest Euclidian distance from the central point.

$$FP1^{'} \geq FP2^{'} \geq FP3' \geq FP4' \geq FP5' \qquad (10)$$

Step 5: Calculate the slopes to the four feature points from the central point.

$$S1' = \frac{(y_2' - y_1')}{(x_2' - x_1')}$$

$$S2' = \frac{(y_3' - y_1')}{(x_3' - x_1')}$$

$$S3' = \frac{(y_4' - y_1')}{(x_4' - x_1')}$$

$$S4' = \frac{(y_5' - y_1')}{(x_5' - x_1')} \qquad (11)$$

Step 6: Compute the rotation angles RA_1, RA_2, RA_3 and RA_4

$$RA_1 = (\tan((S1 - S1')/(1 + S1 \times S1'))) \times \frac{180}{\pi}$$

$$RA_2 = (\tan((S2 - S2')/(1 + S2 \times S2'))) \times \frac{180}{\pi}$$

$$RA_3 = (\tan((S3 - S3')/(1 + S3 \times S3'))) \times \frac{180}{\pi}$$

$$RA_4 = (\tan((S4 - S4')/(1 + S4 \times S4'))) \times \frac{180}{\pi}$$

Step 7: Compute angle A, where A = avg{ A1,A2},

$$\{A1, A2\} = \{RA_1, RA_2, RA_3, RA_4\} - \text{diff}\{ RA_1, RA_2, RA_3, RA_4\} \qquad (12)$$

here diff{ RA_1, RA_2, RA_3, RA_4} is used to find the most unique element from the dataset.

Step 8: Restore the region with the angle A in the region by applying the feature points which are extracted from the key.

Step 9: Finally, the original images will be extracted.

End

7. Results and Discussion

The proposed model is tested using the MATLAB 2013 with CPU 2.8 GHz. The proposed method takes on an average of 0.8 sec to extract the feature points from the image. A diversity of grey scale images are used for the watermark procedure. The experiment is conducted with four images with

their sizes of 256×256. The distortion of the image is calculated by using the Peak Signal to Noise Ratio (PSNR). The value of the PSNR decides the distortion in the image, if the PSNR value is large; it means the distortion in the image is less.

7.1 Performance Evaluation

The performance of the proposed model is tested under four types of attacks such as scaling, rotation, noise pollution and cropping which is applied at the tested image. 8 bit watermark is embedded in to the image and the k value is taken as 8. The obtained results are given below.

Scaling: The proposed method is tested under different scaling distortions. The range of the scaling factor is taken from 2 to 0.2. The proposed method follows the histogram based image watermarking and it is robust against the scaling attacks. Therefore, an extracted feature points and central points are not distorted from the image. The experimental results for scaling attacks are given in Table 1.

Rotation: The proposed method is tested under different rotation angles which are in range from 0º

to 30º with a difference of 10º. The regions of feature points and central points don't change when the image is subject to rotation. Therefore the proposed method is said to be robust against the rotation. Table 2 shows the experimental results of the proposed scheme under rotation.

Noise pollution: The image is added with noise pollution. The type of noise pollution is salt and pepper. For an experimental analysis, the noise range is taken from 0.1 to 0.5 with a variance of 0.1. The obtained results show the effectiveness of the proposed scheme under noise pollution. Table 3 shows the experimental results of proposed scheme against the noise pollution.

JPEG Compression: Table 4 shows the experimental analysis of the proposed scheme against the JPEG Compression. For an experimental analysis, the quality factor is taken as 80 to 20 and the variance is -10. The value of the quality factor will decide the compression quality. The experimental result shows that the JPEG compression will not affect the robustness of the proposed scheme.

Table 1. Watermark insertion ratio against the Scaling attack

Scaling Factor	Image_1	Image_2	Image_3	Image_4
2	8/8	8/8	8/8	8/8
1.8	8/8	8/8	8/8	8/8
1.6	8/8	8/8	8/8	8/8
1.4	8/8	8/8	8/8	8/8
1.2	8/8	8/8	8/8	8/8
1	8/8	8/8	8/8	8/8
0.8	8/8	8/8	8/8	8/8
0.6	6/8	**5/8**	6/8	6/8
0.4	**5/8**	**4/8**	**5/8**	**4/8**
0.2	**3/8**	**3/8**	**4/8**	**4/8**

Table 2. Watermark insertion ratio against the Rotation attack

Angle of Rotation	Image_1	Image_2	Image_3	Image_4
0	8/8	8/8	8/8	8/8
10	7/8	8/8	7/8	7/8
20	6/8	7/8	7/8	7/8
30	6/8	6/8	7/8	6/8

Table 3. Watermark insertion ratio against the Noise Pollution

Noise pollution	Image_1	Image_2	Image_3	Image_4
Salt & pepper (0.1)	8/8	8/8	8/8	8/8
Salt & pepper (0.2)	8/8	8/8	8/8	8/8
Salt & pepper (0.3)	8/8	8/8	8/8	8/8
Salt & pepper (0.4)	8/8	8/8	8/8	8/8
Salt & pepper (0.5)	8/8	7/8	7/8	7/8

Table 4. Watermark Insertion ratio against the JPEG Compression

Quality Factor	Image_1	Image_2	Image_3	Image_4
80	8/8	8/8	8/8	8/8
70	8/8	8/8	8/8	8/8
60	8/8	8/8	8/8	8/8
50	8/8	8/8	8/8	8/8
40	8/8	8/8	8/8	8/8
30	8/8	8/8	8/8	7/8
20	8/8	8/8	8/8	7/8

Table 5. Comparison of Experimental Results

	(Zheng et al., 2009) [11]	(Su et al., 2013) [12]	(Tang and Hang, 2003) [13]	Proposed Method
Rotation	0-360	0-360	1-5	0-360
Scaling	0.5-2.0	0.4-1.5	-	0.2-2.0
Noise Pollution (Salt and pepper)	-	-	<=0.2	<=0.5
JPEG Compression	40-80	20-80	40-80	20-80
Image size	256×256	256×256	256×256	256×256
Host image type	Grey	Grey	Grey	Grey
Capacity (bits)	4	8	16	64

7.2 Results Comparison

To validate the proposed method, geometric attacks are performed on different images. The results obtained from the simulation environment proved the efficiency of the proposed scheme.

Figure 5 shows the comparison between the transparency and the capacity. The images are tested under varying bit rates from 8 bits to 64 bits. The PSNR values are calculated for each image with different bit rates. It is clearly shown that, the PSNR value decreases when the bit rate increases.
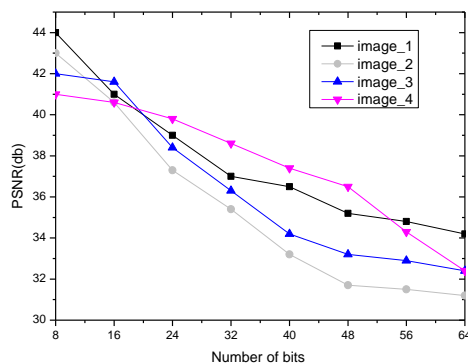

Figure. 5 The number of Bits Vs PSNR

As Table 5 shows that, the proposed scheme has better performance against the existing methods in terms of geometric attacks and signal processing: the rotation angle ranges from 0-360, Scaling ranges from 0.2- 2.0, the noise pollution in image is less than 0.5, JPEG compression with low quality factor as 20.

For better understanding purpose, the performance of the proposed method is compared with the other existing feature extraction methods, such as (Zheng et al., 2009) [11], (Su et al., 2013) [12] and (Tang and Hang, 2003) [13].

8. Conclusion

This paper proposed the adaptive feature point extraction model for robust image watermarking. The adaptive feature point extraction model was employed to extract the reliable feature points form the image. The proposed model utilizes the histogram distribution for watermarking insertion and extraction for the image. The simulation results are carried out with the grey scale images and the geometric attacks such as scaling, rotation, noise pollution and JPEG compression are performed on the watermarked images. The range of scaling factor is taken from 2.0 to 0.2. The proposed method is tested under different rotation angles which is range from 0º to 30º with a difference of 10º. The salt and pepper noise pollution is added to the image and the noise is varied from 0.1 to 0.5 with a variance of 0.1. The quality factor is taken as 80 to 20 and the variance is -10 for the JPEG compression. The experimental results proved that the proposed method is robust against simulated attacks and the geometric attacks. In Future, the proposed method is extended with medical images. The medical image

carries more sensitive information than the normal images. So, protecting medical images is more crucial when compared to the normal images. In future, the adaptive image watermarking model is extended for medical images for preserving the patient's information.

References

[1] Y. Lee, and K. Jongweon, "Histogram rotation-based image watermarking with reversibility", *International Journal of Security and Its Applications*, Vol. 6, No. 2, pp.197-201, 2012.

[2] C.S. Lu, S. W. Sun, and P. C. Chang, "Robust hash-based image watermarking with resistance to geometric distortions and watermark-estimation attack", *Electronic Imaging 2005*. International Society for Optics and Photonics, 2005.

[3] X. Kang, J. Huang, Y. Q. Shi and Y. Lin, "ADWT–DFT composite watermarking scheme robust to both affine transform and JPEG compression", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 13, No. 8, pp. 776–786, 2012.

[4] H. A. Ali, and S. A. K. Khamis, "Robust digital image watermarking technique based on histogram analysis", *World of Computer Science and Information Technology Journal*, Vol. 2, No. 5, pp. 163–168, 2012.

[5] C. M. Pun, and X. C. Yuan, "Geometric invariant digital image watermarking scheme based on histogram in DWT domain", *Journal of Multimedia*, Vol. 5, No. 5, pp. 434–442, 2010.

[6] S. Xiang, H. J. Kim and J. Huang, "Audio watermarking robust against time-scale modification and MP3 compression", *Signal Processing*, Vol. 88, No. 10, pp. 2372–2387, 2008.

[7] Y. Lee and J. Kim, "Histogram rotation-based image watermarking with reversibility", *International Journal of Security and Its Applications*, Vol. 6, No. 2, pp.197–201, 2012.

[8] A. Suhail, Mohamed., and M. S. Obaidat, "Digital watermarking-based DCT and JPEG model", *IEEE Transactions on Instrumentation and Measurement*, Vol. 52, No. 5,1640-1647, 2003.

[9] C. Harris and M. Stephens, "A combined edge and corner detector", *Paper presented at the Proceeding of the 4th Alvey Vision Conference,* 1988.

[10] C. M. Pun, and X. C. Yuan, "Robust Block and Gray-Level Histogram Based Watermarking Scheme", In: *Advances in Multimedia Information Processing-PCM2009.Springer, Berlin*, 2009.

[11] D. Zheng, S. Wang, J.Y. Zhao," RST Invariant Image Watermarking Algorithm With Mathematical Modeling and Analysis of the Watermarking Processes", *Image Processing, IEEE Transactions on*, Vol .18, No. 5, pp. 1055–1068, 2009.

[12] P. Su, Y. Chang and C. Wu, "Geometrically Resilient Digital Image Watermarking by Using Interest Point Extraction and Extended Pilot Signals", *Information Forensics and Security, IEEE Transactions on,* Vol. 8, No. 12, pp. 1897–1908, 2013.

[13] C. W. Tang, H. M. Hang, "A feature-based robust digital image watermarking scheme", *Signal Processing, IEEE Transactions on*, Vol. 51, No. 4, pp. 950–959, 2003.

[14] J. S. Tsai, W.-B. Huang, and Y.-H. Kuo, "on the selection of optimal feature region set for robust digital image watermarking*", Image Processing, IEEE Transactions on*, Vol. 20, No. 3, pp. 735-743, 2011.

[15] N. N. Priya, and S.L. Stuwart, "Robust feature based image watermarking process", *International Journal of Computer Applications,* pp. 13-16, 2010.

[16] X. Gao, "Geometric distortion insensitive image watermarking in affine covariant regions", Systems*, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on,* pp. 278-286, 2010.

[17] X. C. Yuan, and C.-M. Pun, "Feature extraction and local Zernike moments based geometric invariant watermarking", *Multimedia Tools and Applications,* pp. 777-799, 2014.