

A Robust Color Image Watermarking Scheme Based on Image Normalization

Ibrahim Alsonosi Nasir, *Member, IAENG*, Ahmed b. Abdurman

ABSTRACT- The robustness of watermarks to geometric attacks is considered to be the most challenging design requirements for watermarks. Geometric attacks can desynchronize the location of the watermark and hence cause incorrect watermark detection. In this paper, a new color image watermarking scheme for copyright protection is proposed. It is based on embedding multiple watermark bits into the luminance component or the blue component of a color image in discrete wavelet domain. The proposed scheme uses image normalization technique to reduce the effect of synchronization errors caused by geometric attacks such as rotation. The extraction process does not require the original image. Experimental results show that the proposed scheme successfully makes the watermark perceptually invisible as well as robust to common signal processing and some geometric attacks.

Index Terms— Watermarking, color image, Wavelet domain, normalization, Geometric attacks.

I. INTRODUCTION

Recently, digital watermarking techniques have been utilized to maintain the copyright of digital data by identifying the owner or distributor of digital data. Watermarking is the process of embedding hidden information called a watermark into the digital media, such that the watermark is imperceptible, robust and difficult to remove or alter [1]. Digital watermarking can be used on many types of digital media including images, video, text and audio recordings. In recent years, attacks against image watermarking systems have become more complicated [2]. In general, these attacks can be classified into two broad categories: signal processing and geometric attacks. While signal processing attacks reduce the watermark energy, geometric attacks can induce synchronization errors between the encoder and the decoder of the watermark. As a result, the decoder is no longer able to detect the watermark. Robustness to geometric attacks is still challenging in the image watermarking community.

Many digital watermarking schemes have been proposed for copyright protection. Most existing watermarking algorithms focus mainly on embedding watermarks into grey-scale images in spatial or frequency domain. The

extension to colour images is usually accomplished by marking the image luminance component or by processing each colour channel separately [3, 4]. Kutter et al. [5] proposed an alternative method for watermarking colour images. It is based on embedding a watermark by modifying a selected set of pixel values in the blue channel, since the human eye is less sensitive to changes in this band. To achieve robustness against JPEG compression attack, Lian et al. [6] suggested that the watermark should be embedded into the green component rather than the red or blue components of the colour image. This is because the loss of energy of the blue and red components is higher than the green component when the watermarked image is attacked by JPEG compression. However, the human eye is more sensitive to changes in the green band. In Lian's method, the watermark is embedded into the largest coefficients of the low-frequency subband of the DWT. The watermark capacity is limited, since the watermark is embedded into only the significant coefficient of transformed image, which mostly contains only a few significant coefficients. Fleet and Heeger [7] proposed a method, which takes into account the characteristics of the human visual system (HVS) with respect to colour perception. They suggested embedding the watermark into the yellow-blue channel of colour images and using the S-CIELAB space to measure the color reproduction error. However, their method can only resist printing and rescanning attacks. Barni et al. [8] introduced another colour image watermarking method based on the cross-correlation of RGB channels. However, it has relative high computing costs and low processing speed since the full-frame DCT is used for three colour channels. Tsai et al. [9] provided a solution of embedding the watermark on a quantized colour image. Kutter et al. [10] investigated watermarking of luminance and blue-channels using a perceptual model, which takes into account the sensitivity and the masking behaviour of the HVS. Huang et al. [11] embedded the watermark into DC coefficients of a colour image directly in the spatial domain, followed by a saturation adjustment technique performed in the RGB colour space. Nasir et al. [12] suggested encoding the watermark by using convolution coding and then embedding multiple watermarks into the blue channel of the host color image. However, the detection process in [11,12] required the original images, which may not be available in some application. In [13] the watermark is embedded in luminance component of the color image using discrete wavelet domain. Authors in [14] suggested extracting the watermark by training support vector machine. However, robustness against geometric attack was not addressed by these methods.

Manuscript received Feb. 15, 2013; revised March 26, 2013.

Ibrahim Alsonosi Nasir is with the Electronic and Computer Engineering Department, Sebha University, Sebha, Libya; PO. Box 68 Brak-Libya; (e-mail: ibran103@yahoo.com).

Ahmed b. Abdurman is with the Electronic and Computer Engineering Department, Sebha University, Sebha, Libya; (e-mail: aabousafe@yahoo.com).

As mentioned earlier, geometric attacks may induce synchronization errors between the encoder and the decoder of the watermark. As a result, the decoder is no longer able to detect the watermark. Several grey-scale image watermarking methods have been developed to overcome this problem. These methods can be roughly classified into template-based, invariant transform domain-based, moment-based, histogram-based, and feature extraction-based methods. The template-based watermarking methods are based on embedding a template in addition to the watermark to assist the watermark synchronization in the detection process. This may be achieved using a structured template embedded in the DFT domain to estimate transformation factor to resynchronize the image [15-17]. In [18-19], watermarks are embedded in affine-invariant domains such as the Fourier-Mellin transform or log-polar domain to achieve robustness against affine transforms. In [20, 21], the watermark is embedded in an affine-invariant domain by using generalized random transform and Zernike moment, respectively. However, watermarking methods involving invariant domains are difficult to implement due to the log-polar mapping [22]. Based on the fact, that the histogram is independent of the position of the pixels, the authors in [23, 24] presented histogram-based watermarking approaches. However, these approaches suffer from robustness limitations under histogram enhancement and equalization attacks. To overcome the issue of synchronization, feature points are used as reference points for both watermark embedding and detection. In [25], Mexican hat wavelet method is used to extract feature points. In [26, 27], the Harris detector is used to extract the feature points. However, Mexican hat wavelet or Harris detector are sensitive to image modification. Furthermore, these schemes do not perform well for extremely low texture images due to the insufficient important feature points for self-synchronization.

In this paper we propose a new color image watermarking scheme, which is based on embedding a watermark into a circular normalized image in the discrete wavelet domain. The rest of this paper is structured as follows. Section 2 describes the proposed watermarking scheme and section 3 presents experimental results. Conclusions are drawn in section 4.

II. PROPOSED WATERMARKING SCHEME INTRODUCTION

The block diagram shown in Fig. 1 provides an overview of the proposed watermarking scheme. First, the Luminance (Y) component in YIQ (Luminance, Hue, and Saturation) or the blue component in RGB (Red, Green, and Blue) color models is obtained from the original image for embedding the watermark; second, circular image is obtained from (Y) component or blue component; then the rotation normalization is performed on the circular image. As a result, the watermark synchronization problem during the detection process can be reduced. Next, a square subimage is obtained from the normalized circular image and decomposed in L-decomposition levels using DWT. The watermark is embedded in the highest level of the wavelet decomposition excluding the coarsest LL-subband. After

embedding watermark bits, L-level inverse wavelet transform is applied. Finally, the inverse rotation normalization is performed on the watermarked normalized circular image and the watermarked image is reconstructed.

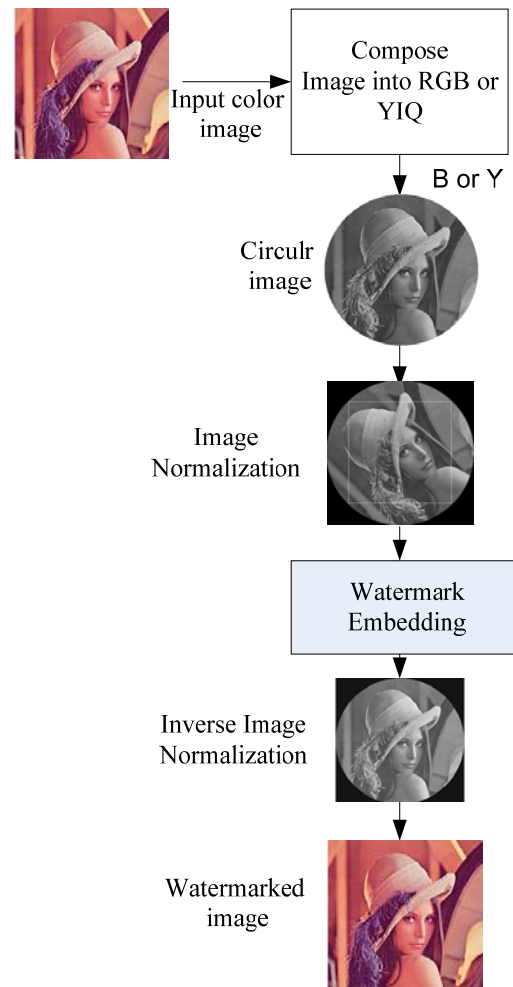


Fig. 1 Watermark embedding scheme.

A. Image Normalization

Synchronization errors between the encoder and the decoder of the watermark may be introduced by geometric attack such as rotation. When the watermarked image has undergone some geometric attacks, the watermark is still present in the watermarked image but the detector is no longer able to detect it due to synchronization errors. To overcome this, we perform rotation image normalization technique given in [28, 29]. As an example, the normalization results for the original and the circular image rotated by 45° and 90° are shown in Fig 2. As can be seen, the equivalent normalized images can be obtained from the original and rotated circular images. Hence, the synchronization error during the detection process is eliminated.

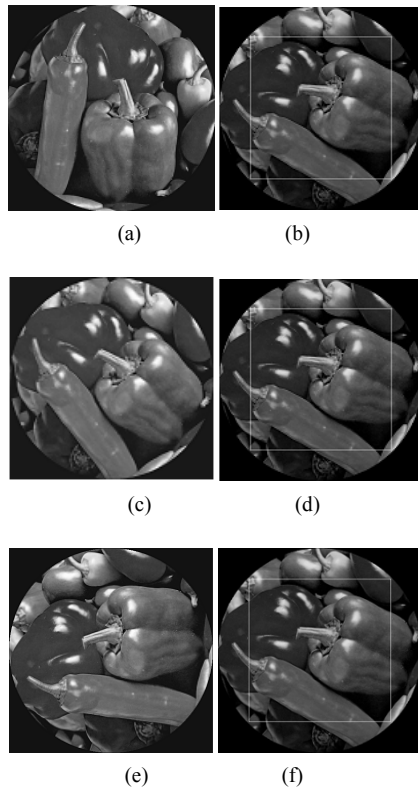


Fig. 2 (a) Original circular image, (b) Normalized circular image, (c) Rotated circular image by 45°, (d) Normalized circular image, (e) Rotated circular image by 90°, (f) Normalized circular image.

B. Watermarking Embedding Process

To improve the robustness of the embedding scheme, each watermark bit is embedded into three different locations, which are determined by using a secret key. The watermarked image may be altered or modified due to intentional and unintentional attacks. During the extraction process, the probability is used to determine the extracted watermark bits. The watermark embedding process can be described as follows:

- (i) The Luminance (Y) component or the blue component of the original image is selected to embed the watermark.
- (ii) A circular image is obtained from the selected component with diameter equal to the size of the original image.
- (iii) The circular image is normalized.
- (iv) The circular image can not be transferred directly into frequency domain. Therefore, in our method, we extract a subimage from the normalized circular image because zero-padding operation will introduce error after applying the inverse transform method such as DWT.
- (v) Decompose the extracted subimage by L-levels using DWT.
- (vi) The watermark is assumed to be of length L. It is denoted by $W = \{w_i, i = 1, \dots, L, w_i \in (0,1)\}$, which is a key-based PN sequence. The private key is shared with the detector to make decision whether a given watermark is present or not.

The watermark bits are embedded by modifying the two largest DWT coefficients V_{Max1} and V_{Max2} in non overlapping blocks of size $m \times m$ in $\{LH_L, HL_L, HH_L\}$ bands. To improve the robustness of the proposed scheme each watermark bit

is embedded into three different locations. The watermark embedding algorithm is defined as follows:

$$Diff = |V_{max1}| - |V_{max2}| \quad (1)$$

$$V_{max1}^* = \begin{cases} |V_{max1}| + \alpha & W = 1 \text{ \& Diff} > T \\ |V_{max1}| + T + \alpha & W = 1 \text{ \& Diff} < T \end{cases} \quad (2)$$

$$V_{max2}^* = \begin{cases} |V_{max2}| + \alpha & W = 0 \text{ \& Diff} \leq T \\ |V_{max2}| + Diff - \alpha & W = 0 \text{ \& Diff} > T \end{cases} \quad (3)$$

where $|V_{max1}|$ and $|V_{max2}|$ are the absolute values of the largest DWT coefficients in selected blocks of size $m \times m$, α is the watermark embedding strength, and T is a pre-determined threshold. The sign of the two watermarked coefficients are determined as follows:

$$V_{max1}^* = \begin{cases} -V_{max1}^* & \text{if } V_{max1} < 0 \\ V_{max1}^* & \text{otherwise} \end{cases} \quad (4)$$

$$V_{max2}^* = \begin{cases} -V_{max2}^* & \text{if } V_{max2} < 0 \\ V_{max2}^* & \text{otherwise} \end{cases} \quad (5)$$

Finally, the inverse wavelet transform (IDWT) is performed to all sub bands. The watermarked image is obtained by adding the inverse normalized watermarked circular image and the remaining image from the original image.

C. Watermark Extraction Process

The proposed watermark extraction process is performed without use of the original image (non-watermarked). Hence, the proposed scheme is able to meet the blindness requirements. In the extraction process, the first five steps are similar to that used in the watermark embedding process. The watermark bits are extracted from the watermarked blocks of size $m \times m$ in $\{LH_L, HL_L, HH_L\}$ bands of the DWT. The watermark bit is extracted as given below:

$$w_i = \begin{cases} 1 & \text{if } |V_{max1}^*| - |V_{max2}^*| > T \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

where $|V_{max1}^*|$ and $|V_{max2}^*|$ are the absolute values of the largest DWT coefficients in selected blocks of size $m \times m$, and T is pre-defined threshold.

Since, each watermark bit is embedded into three different locations; we determine the extracted watermark bits by calculating the probability P_0 and P_1 of detecting bit 0 and bit 1, respectively as given below:

$$W_i^* = \begin{cases} 1 & P_1 > P_0 \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

The extracted watermark is then compared with the original embedded watermark to decide a success detect. The normalized Correlation (NC) given in [23] is used to evaluate the similarities between the original and the extracted watermarks.

III. EXPERIMENTAL RESULTS

The experiments were organized in two phases. The first phase evaluated the watermark Imperceptibility and the second evaluated the robustness of the watermark against various attacks including signal processing and geometric attacks. The watermark imperceptibility and robustness are evaluated by using fifteen different color images of size 512×512 including Lena, Peppers, Baboon, Lake, Walk-bridge, House, Air-plane, etc. In the experiments, a pseudorandom sequence of size 16-bits is used as a watermark. Since, each bit is embedded into three different locations; the total of watermark bits embedded is 48-bits. The block size is 8×8 and the 3-level decomposition of DWT is selected to embed the watermark.

A. The Impact of the Watermark Strength

In the embedding process, the distortion of an image depends on the length of the watermark, the threshold T and the watermark strength α . The threshold T controls the difference between the watermarked coefficients. The greater T, the more embedding distortion is introduced in the watermarked image. Meanwhile, the embedding of the watermark is controlled by the watermark strength α . increasing the value of the watermark strength α induces more distortion in the watermarked image. There is a relationship between the value of the watermark strength, and the visibility and robustness of the watermark. The higher values for α and T, the more distortion is introduced in the watermarked image. Hence, there is trade-off between robustness and imperceptibility. In the YIQ color model, the values of watermark embedding strength $\alpha=0.05$ and $T=0.035$. Whereas, in the RGB color model, the values of watermark embedding strength $\alpha=15$ and $T=25$. These values empirically determined values, and found to be appropriate for the tested images.

B. Watermark Imperceptibility

The Peak Signal to Noise Ratio (PSNR) was adopted to evaluate the perceptual distortion of the proposed scheme. The PSNR values for fifteen watermarked images are between 35 and 50 dB. These values are all greater than 30 dB, which is the empirically tested threshold value for an image without any perceivable degradation [26]. Taking, Peppers, Opera as an example, the un-watermarked and the watermarked images are shown in Fig. 2. It can be seen that the differences between the corresponding watermarked and un-watermarked images are imperceptible and the embedded watermarks are invisible to the human eye. As mentioned before, the distortion on an image relies on the embedding threshold T, the block size for embedding watermark bit, the embedding strength α and the length of the watermark. It is worth mentioning that that the larger the block size, the higher the PSNR value. However, this comes at the expense of the capacity. Table 1 shows the transparency results of the proposed scheme.

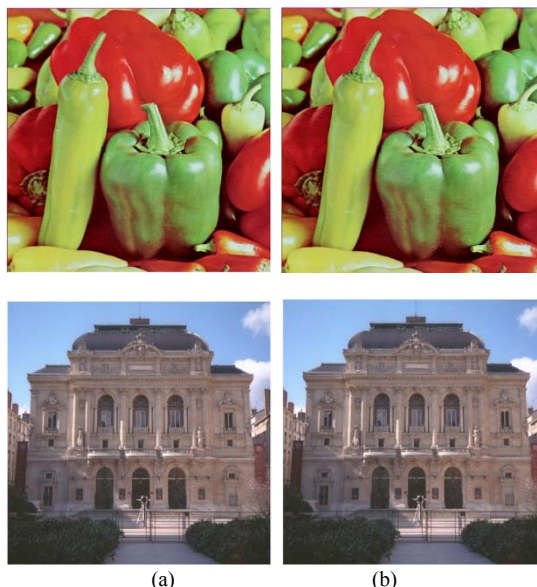


Fig. 2. (a) Original images (b) Watermarked Peppers and Opera images

Table 1
PSNR between watermarked image and the original image (dB)

Image	RGB model	YIQ model
Lena	48.33	42.13
Peppers	44.67	39.66
Baboon	40.04	35.29
Lake	42.84	38.44
House	46.04	40.32
Opera	44.14	41.39
Water	41.80	37.39

C. Watermark Robustness

To evaluate the robustness of the proposed watermarking scheme, various common signal processing and geometric attacks were applied to the watermarked images. These attacks include JPEG-lossy compression, median filtering, low-pass filtering, scaling and rotation attacks. Table 2 and Table 3 summarize experimental results by applying common signal processing attacks on Lena, Baboon and lake images watermarked in RGB model and YIQ model. For JPEG lossy compression attacks, the quality factor varied from 20% (high compression) to 100%. As can be seen from Table 1, the embedded watermark in Y component can be correctly extracted even under JPEG compression with a quality factor as low as 20%. As shown, better performance is achieved when the watermark is embedded in Y component than the B component. This robustness is achieved by embedding the watermark into the middle frequency coefficients of the DWT, which are less affected by JPEG compression attacks. For filtering attacks, the watermarked images were subjected to median and low pass filtering. As shown in Table 1, more robustness to these attacks is achieved when the watermark is embedded in Y component in YIQ model. Table 2 shows that better robustness is achieved when the watermarked in embedded in Y component. As can be seen, the watermark can be correctly detected when the watermarked image rotated by up to 15°. For scaling attack, the attacked images are rescaled back to their original size before watermark extraction. The watermark can be extracted even when the watermarked images are scaled

down to 70% or scaled up 200%. The proposed scheme overcomes the synchronization problem caused by rotation attack by normalizing the embedding circular image as explained in section (2.1).

The performance of the proposed watermarking scheme in YIQ model is better than RGB model due to the following factors:

- (i) Loss of energy of the blue component is high when the watermarked image is attacked by JPEG compression or low pass- filtering attacks [6].
- (ii) The blue component of an image in RGB model is more sensitivity to rotation because such a geometric transformation is based on interpolation which is a low-pass local filtering that affects the high frequency content. Consequently, the watermark is less robust to the rotation attack when is embedded in this component.
- (iii) The more distortion on the blue component, the less accurate normalization angle can be used at extraction.

Table 2
Results of signal processing attacks (NC)

Attacks	RGB Model			YIQ Model		
	Lena	Baboon	Lake	Lena	Baboon	Lake
Jpeg 100%	0.90	0.88	0.87	1.0	1.0	1.0
Jpeg 80%	0.80	0.63	0.73	1.0	1.0	1.0
Jpeg 60%	0.60	0.82	0.53	0.94	1.0	1.0
Jpeg 40%	0.48	0.50	0.33	0.94	0.94	0.94
Jpeg 20%	0.45	0.44	0.50	0.83	1.0	1.0
Median filtering 3×3	0.60	0.80	0.70	1.0	0.68	0.94
Low-pass filtering 3×3	0.45	0.63	0.64	0.83	0.70	0.83

Table 3
Results of geometric attacks (NC)

Attacks	RGB Model			YIQ Model		
	Lena	Baboon	Lake	Lena	Baboon	Lake
Rotation 1°	0.94	0.76	0.80	1.0	1.0	1.0
Rotation 2°	0.94	0.85	0.88	1.0	1.0	1.0
Rotation 5°	0.90	0.86	0.86	1.0	1.0	1.0
Rotation 10°	0.90	0.86	0.86	1.0	1.0	1.0
Rotation 15°	0.90	0.82	0.90	1.0	1.0	1.0
Scaling 0.7	0.56	0.48	0.76	0.89	0.89	0.89
Scaling 0.9	0.64	0.70	0.76	0.94	0.94	0.94
Scaling 1.2	0.72	0.80	0.73	0.94	0.94	1.0
Scaling 1.5	0.74	0.85	0.76	1.0	1.0	1.0
Scaling 2	0.74	0.85	0.82	1.0	1.0	1.0

IV. CONCLUSION

The paper presents a robust color image watermarking scheme, which is designed to be robust both signal processing and geometric attacks. Image normalization technique is used to reduce the synchronization errors caused by rotation attack. The original image is not required at detection. The watermark is embedded into the image luminance in YIQ model or in the blue channel in RGB model by modifying the two largest values of DWT coefficients in the selected blocks. Each bit of the watermark is embedded into three different locations of wavelet bands.

It has been demonstrated that the proposed scheme succeeds in making the watermark perceptually invisible and under most of the commonly used attacks; the proposed scheme is robust. The results demonstrate that more robustness can be achieved when the watermark is embedded into the luminance channel than the blue channel of an image.

Further research is to improve the robustness to more geometric attacks such as cropping, shearing and linear geometric transform.

REFERENCES

- [1] L. M. Marvel, C. G. Bonchelet, Jr., and C. T. Retter, "Spread spectrum image steganography," *IEEE Transactions on Image Processing*, vol. 8 (8), pp. 1075-1083, 1999.
- [2] M. Barni, I.J. Cox, T. Kalker, Digital watermarking, 4th International Workshop on Digital Watermarking, Siena, Italy, *Lecture Notes in Computer Science 3710*, Springer 2005.
- [3] K. I. Hashida and S. A., "A method of embedding robust watermarks into digital color images," *IEICE Transactions Fundamentals*, vol. E81-A(10), pp. 2133-2137, 1998.
- [4] N. Nikolaidis and I. Pitas, "Robust image watermarking in spatial domain," *Signal Processing*, vol. 66(3), pp. 385-403, 1998.
- [5] M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," *Journal of Electronic Imaging*, vol. 7, pp. 326-332, 1998.
- [6] L. Lian-Shan, L. Ren-Hou, and G. Qi, "A new watermarking method based on DWT green component of color image," in *International Conference on Machine Learning and Cybernetics*, vol. 6, 2004, pp. 3949-3954
- [7] D. Fleet and D. Heeger, "Embedding invisible information in color images," in *IEEE Int. Conf. on Image Processing ICIP'97*, vol. 1, 1997, pp. 532-535.
- [8] M. Barni, F. Bartolini, and A. Piva, "Multichannel watermarking of color images," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 12(3), pp. 142-156, 2002.
- [9] P. Tsai, Y. C. Hu, and C. C. Chang, "A color image watermarking scheme based on color quantization," *Signal Processing*, pp. 95-105, 2004.
- [10] M. Kutter and S. Winkler, "A vision-based masking model for spread-spectrum image watermarking," *IEEE Transactions on Image Processing*, vol. 11(1), pp. 16-25, 2002.
- [11] P. S. Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," *IEE Proceedings -Vision, Image and Signal Processing*, vol. 152 (5), pp. 561-574, 2005.
- [12] I. Nasir, Y. Weng, J. Jiang, and S. Ipson, "Multiple spatial watermarking technique in color images", *Signal, Image and Video Processing, (Springer)*, vol. 4(2), pp.145-154, 2010.
- [13] N. Dharwadkar, B. Amberker, " Watermarking scheme for color images using wavelet transform based texture properties and secret sharing", *International Journal of Information and Communication Engineering*, vol. 6(2), pp. 94-101,2010.
- [14] S. Tiwari and A. Dongre, "A superior Support Vector Machine digital watermarking for color image," *Int. Conf. on. Computer, Information and Telecommunication Systems (CITS)*, 2012.
- [15] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Trans. on Image Processing*, vol. 9(6), pp. 1123-1129, 2000.
- [16] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 13(8), pp. 776-786, 2003.
- [17] J. L. Dugelay, S. Roche, C. Rey, and G. Doerr, "Still-image watermarking robust to local geometric distortions," *IEEE Trans. on Image Processing*, vol. 15(9), pp. 2831-2842, 2006.
- [18] C.Y. Lin, M. Wu, J.A. Bloom, I.J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. on Image Processing*, vol. 10(5), pp. 767-782, 2001.
- [19] D. Zheng, J. Zhao, and A. E. Saddik, "RST-invariant digital correlation," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 13(8), pp. 753-765, 2003.

- [20] X. Kang, J. Huang, et al., A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression, *IEEE Trans. on Circuits and Systems for video Technology*, vol. 13, no. 8, pp. 776-786, 2003.
- [21] D. Simitopoulos, D.E. Koutsonanos, Robust image watermarking based on generalized random transformations, *IEEE Trans. On Circuit and Systems for Video Technology*, vol. 13, no. 8, pp. 732-745, 2003.
- [22] C.Y. Lin, M. Wu, J.A. Bloom, I.J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient watermarking for images," *IEEE Trans. on Image Processing*, vol. 10(5), pp. 767-782, 2001.
- [23] S. Roy and E.C. Chang, Watermarking color histogram, in proc. Int. Conf. Image Process, pp.2191-2194, 2004.
- [24] S. Lee, Y. Suh, and Y. Ho, Lossless data hiding based on histogram modification of different images, in *Proc. Pacific-Rim Conf. Multimedia*, vol3, pp. 340-347, 2004.
- [25] S. Xiang, H. Joong, and J. Huang, Invariant Image Watermarking based on statistical features in low-frequency domain, *IEEE Trans. on Circuit and Systems for video Technology*, vol. 18, no. 6, pp. 777-789, 2008.
- [26] X. Qi, J. Qi, A robust content-based digital image watermarking scheme, *Signal processing*, vol. 87, pp. 1264-1280, 2007.
- [27] L. Li, and B. Guo, Localized image watermarking in spatial domain resistant to geometric attacks, *Int. Journal of Elec. And Comm.*, vol. 63, pp. 123-131, 2009.
- [28] S. C. Pei and C. N. Lin, Image normalization for pattern recognition, *Image Vision. Computing*, vol. 13, no. 10, pp. 711-723, 1995.
- [29] M. Alghoniemy, and A. H. Tewfik, Geometric invariant in image watermarking, *IEEE Trans. on Image Processing*, vol. 13, no. 2, pp. 145-153, 2004.