ROBUST COLOUR IMAGE WATERMARKING SCHEME BASED ON FEATURE POINTS AND IMAGE NORMALIZATION IN DCT DOMAIN

Ibrahim Alsonosi Nasir

Department of Electronic and Computer Engineering,
Sebha University, Sebha, Libya
Ibrn103@yahoo.com

ABSTRACT

Geometric attacks can desynchronize the location of the watermark and hence cause incorrect watermark detection. This paper presents a robust colour image watermarking scheme based on visually significant feature points and image normalization technique. The feature points are used as synchronization marks between watermark embedding and detection. The watermark is embedded into the non overlapped normalized circular regions in the luminance component or the blue component of a color image. The embedding of the watermark is carried out by modifying the DCT coefficients values in selected blocks. The original unmarked image is not required for watermark extraction Experimental results show that the proposed scheme successfully makes the watermark perceptually invisible as well as robust to common signal processing and geometric attacks.

KEYWORDS

Watermarking, DCT domain, image normalization, feature points.

1. INTRODUCTION

Visual data such as image and video can be easily copied, altered and distributed over the internet without any loss in quality. Therefore, the protection of the ownership of multimedia data has become a very challenging issue. 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]. 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. 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] suggested embedding the watermark in the blue channel, because the human eye is less sensitive to changes in this band. Lian et al. [6] suggested that the watermark should be

Dhinaharan Nagamalai et al. (Eds) : CSE, DBDM, CCNET, AIFL, SCOM, CICS, CSIP- 2014
pp. 217–227, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4419

embedded into the green component. 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. Barni et al. [7] 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. Kutter at al. [8] investigated watermarking of luminance and blue-channels using a perceptual model, which takes into account the sensitivity and the masking behaviour of the HVS. Nasir et al. [9] suggested embedding the watermark into luminance component of the color image and use image normalization technique to reduce the effect of synchronization errors. However, this method cannot resist cropping attacks. Several grey-scale image watermarking methods have been developed to overcome of synchronization errors caused by geometric attacks. 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 [10-12]. In [13-14], watermarks are embedded in affine-invariant domains such as the Fourier-Mellin transform or log-polar domain to achieve robustness against affine transforms. In [15, 16], 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 [17]. Based on the fact, that the histogram is independent of the position of the pixels, the authors in [18, 19] 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 [20], Mexican hat wavelet method is used to extract feature points. In [21, 22], the Harris detector is used to extract the feature points. However, Mexican hat wavelet or Harris detector are sensitive to image modification. In [23], the end-stopped wavelets feature detector is used to extract feature points. To resist image geometric attacks and to eliminate synchronization errors between the watermark embedding and the detection, this paper presents a robust color image watermarking scheme, which combines the advantages of feature points extraction and image normalization and investigates watermarking of luminance and blue-channels by modifying the DCT coefficients values in selected blocks.

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.

2. THE PROPOSED WATERMARKING SCHEME

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, wavelet based feature detector is utilized to extract steady feature points from the B or Y component of the original image; then the circular regions are normalized by image normalization process. To enhance the robustness, the watermark bits are embedded into all circular images. Finally, the watermarked image is reconstructed. During the detection process, we claim the existence of the watermark if one copy of the embedded watermark is correctly detected in one embedding circular region.

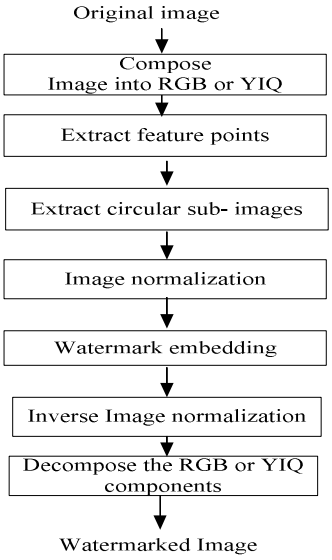


Figure 1. Watermark embedding scheme

2.1. Feature Extraction Detector

Monga et al, [24] proposed an iterative feature detector to extract significant geometry preserving feature points. The detector determine the feature points by computing a wavelet transform based on an end-stopped wavelets obtained by applying the first-derivative of Gaussian (FDoG) operator to the Morlet wavelet. Monga et al, [24] evaluate the performance of this detector with three commonly used detectors that are Harris corner detector, the maximally stable extremaly region (MSER) detector and Hessian Affine and conclude the feature detector based on end-stopped wavelets is the most robust. Therefore, in the present scheme, this detector has been adopted to extract the feature points. The feature detection process can be divided into the following steps:

(i) For each image location, the wavelet transform is computed as given in reference [24]
(ii) The significant features points are identified by looking for local maxima of the magnitude of the wavelet coefficients in a pre-selected neighbourhood.
(iii) A threshold is applied to eliminate spurious local maxima in featureless regions of the image.

To determine the regions for each determined feature point for embedding the watermark, a search is carried out within a circular neighbouring region whose radius is set to be R. If the detector response at the centre of the region achieves local maximum, the feature point is selected. Otherwise, it is discarded. To obtain non-overlapping regions, the most stable feature points are first selected. Then, any feature points whose corresponding region overlaps with the selected feature points are excluded.

2.2. Image Normalization

Synchronization errors between the embedding and the detection of the watermark may be introduced by geometric attacks such as rotation, shearing and translation and although the watermark is still present in the watermarked image, it can no longer be detected. Image

normalization techniques developed for pattern recognition [25] can be used to overcome this problem as suggested in [26]. In the proposed scheme, an image normalization technique is performed on extracted circular images.

2.3. Watermarking Embedding Process

We assume that the watermark of length N_w is a binary and denoted by $W = \{w_i , i = 1,.....,N_w , w_i \in (0,1)\}$, 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 is embedded into DCT coefficients of M×M block. The proposed watermark embedding process is described as follows.

- The Luminance (Y) component or the blue component of the original image is selected to embed the watermark.
- The feature detector based on end-stopped wavelets is applied to the image to determine the feature points as described in section 2. These feature points are used for the reference centers of circular subimages for watermark embedding and detection.
- For each determined feature points, search within a circular neighbouring region, whose radius is set to be R to extract non overlapped circular images for embedding the watermark.
- The normalization process is applied to each extracted circular image.
- The normalized circular image can not be transferred directly into frequency domain. Therefore zero-padding operation could be performed on the normalized circular image. In the proposed method, a subimage is extracted from the normalized circular image because zero-padding operation will introduce error after applying the inverse DCT transform method.
- The discrete cosine transform (DCT) is applied to a selected 8×8 blocks of the sub-images.
- To achieve robustness against common signal processing attacks, the low frequency coefficient of the selected DCT block is used to embed the watermark. In the proposed scheme, the DC coefficients are kept unmodified and the first four AC coefficients in zigzag order are selected to embed the watermark. In order to reduce the visual degradation on the watermarked image, the number of AC coefficients for embedding a watermark bit in each selected DCT blocks is set to 4. This is because using more coefficients for embedding a watermark bit will cause more distortions of the watermarked image.

  The watermark embedding process is carried out by quantizing the absolute value of the second largest DCT coefficients in the selected DCT blocks to the nearest values M_0 or M_1 as shown in Figure 2 by dashed vertical lines. The watermark embedding algorithm can be described as follows:
  Firstly, the length of embedding intervals for bit 0 and bit 1 is defined as given in (1)

$$L_0 = L_1 = \frac{|AC_1|}{L} \qquad (1)$$

  where L_0 and L_1 are the length of embedding intervals for bit 0 and bit 1, respectively. L represents the number of embedding intervals and $|AC_1|$ is the absolute value of the largest DCT coefficients selected from the first four AC coefficients in zigzag order. Secondly, to embed watermark bit 0 or bit 1, the absolute value of the second largest DCT

coefficient $|AC_2|$ is quantized to the nearest M_0 to embed '0' or to the nearest M_1 to embed '1' as follows:

$$AC_2^* = \begin{cases} M_0 & \text{if } w = 0 \\ M_1 & \text{otherwise} \end{cases} \quad (2)$$

Where AC_2^* is the watermarked coefficient, M_0 and M_1 are the middle values of the quantization level '0' and level '1', respectively. The $|AC_3|$ and $|AC_4|$ coefficients are only quantized to the value AC_2^* if they are greater than the watermarked coefficient AC_2^*. The signs of the watermarked coefficients are determined as given in (3)

$$AC_2^* = \begin{cases} -AC_2^* & \text{if } AC_2 < 0 \\ AC_2^* & \text{otherwise} \end{cases} \quad (3)$$

The watermarked subimages are obtained by applying the IDCT transform. Finally, the inverse normalized process is applied to each watermarked circular image and the watermarked image is reconstructed.

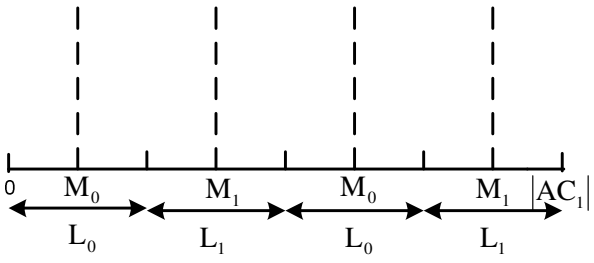


Figure 2 Quantization process for watermarking
Watermark Extraction process

2.4. Watermark Extraction Process

The proposed watermark extraction process is performed without use of the original image. In the extraction process, the first six steps are similar to that used in the watermark embedding process. The watermark bit is extracted as given in (4)

$$W_i^* = \begin{cases} 0 & \text{if } |AC_2^*| \in L_0 \\ 1 & \text{if } |AC_2^*| \in L_1 \end{cases} \quad (4)$$

where $|AC_2^*|$ is the absolute values of the second largest DCT coefficients of the first four AC coefficients in the selected DCT blocks of size 8×8. The AC coefficients are selected in zigzag order, W_i^* is the extracted watermark bit and L_0 and L_1 are the embedding intervals for bits 0 and 1, respectively. The extracted watermark is then compared with the original embedded watermark to decide a success detect. The normalized (NC) given in [22] is used to evaluate the similarities between the original and the extracted watermarks.

Main-body text is to written in fully (left and right) justified 11 pt. Times New Roman font with a 6pt. (paragraph) line spacing following the last line of each paragraph, but a 12pt. (paragraph) line spacing following the last paragraph. Do not indent paragraphs.

3. EXPERIMENTAL RESULTS

The watermark imperceptibility and robustness are evaluated by using 10 different colour images of size 512×512 including Lena, Peppers, Baboon, Lake, etc. In the experiments, a pseudorandom sequence of size 16-bits is used as a watermark and the radius of each circular image is 71.

3.1 Watermark Imperceptibility

The distortion of an image depends on the watermark length, the number of quantization levels for embedding the watermark, the number of extracted sub-images and the number of AC coefficients for embedding a watermark bit in each 8×8 DCT block. The larger the number of AC coefficients used for embedding, the more significant the distortion. Also the more the quantization levels (L) for embedding watermark bits, the smaller the distortion. In the other words, increasing the number of quantization levels leads to a small change in the AC coefficients. Hence there is a trade off between robustness and imperceptivity. The Peak Signal to Noise Ratio (PSNR) is adopted to evaluate the perceptual distortion of the proposed scheme. The PSNR values for ten watermarked images are between 39 and 53 db. These values are all grater than 30 db, which is the empirically tested threshold value for the image without any perceivable degradation [21]. Taking Lena, Peppers, as an example, the watermarked images and circular feature regions from Y component are shown in Figure 3.

Table I. PSNR between watermarked image and the original image (db)

Image	RGB model	YIQ model
Lena	52.63	44.93
Peppers	51.69	43.08
Baboon	44.57	39.19

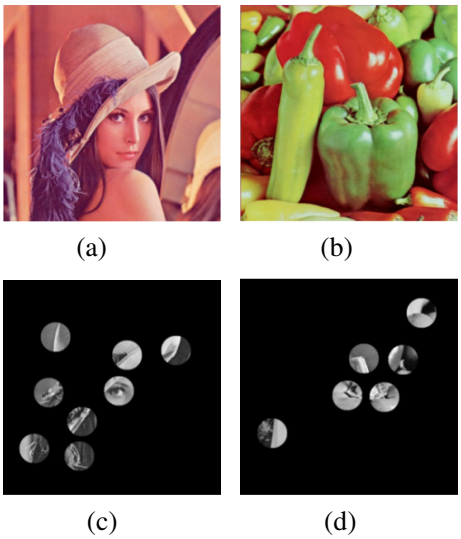
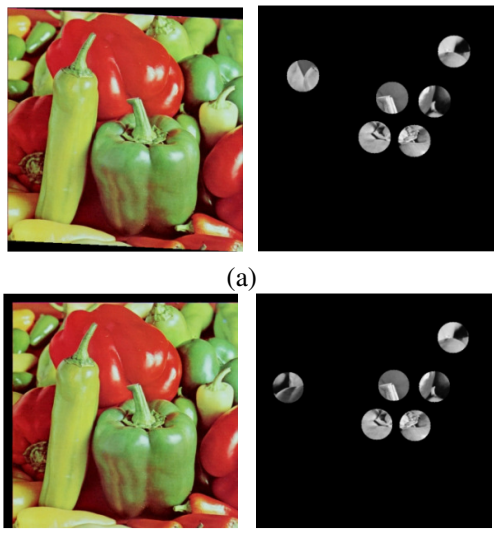


Figure 3. (a) and (b) Watermarked Lena and Peppers images; (c) and (d) circular feature regions

3.2 Watermark Robustness

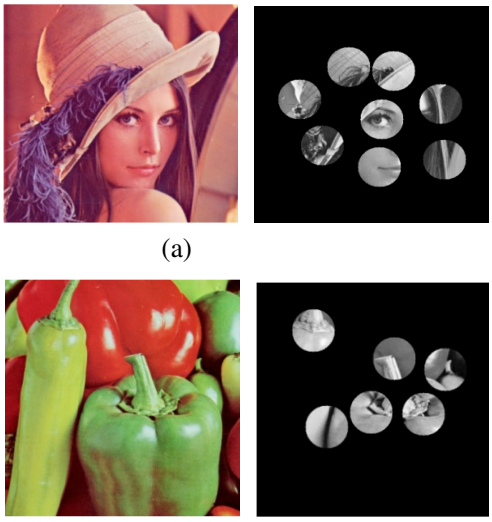
To evaluate the robustness of the proposed watermarking scheme, various common signal processing and geometric attacks were applied to the watermarked images. These attacks include JPEG-lossy compression, median filtering, low-pass filtering, Gaussian filtering, and cropping, shearing, rotation, row and column removal attacks. As an example, results for some geometric attacks are shown in Figure 4 and Figure 5.



(a)

(b)

Figure 4. Results of geometric attacks; (a) shearing x-0%, y-5%, (b) Translation-x-20 and y-20.



(a)

(b)

(c)

Figure 5. Results of cropping attacks; (a) cropping Lena 25 % off , (b) cropping Peppers 25 % off, (c) centred cropping 10%.

Table 2 and Table 3 summarize experimental results by applying common signal processing attacks on Lena, Peppers and Baboon images watermarked in RGB model and YIQ model. For JPEG lossy compression attacks, the quality factor varied from 30% (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 30%. 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 low frequency coefficients of the DCT, which are less affected by JPEG compression attacks. For filtering attacks, the watermarked images were subjected to median, low pass and Gaussian filtering. As shown in Table 2, more robustness to these attacks is achieved when the watermark is embedded in Y component in YIQ model.

Table 3 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 attacked by geometric attacks. The proposed scheme overcomes the synchronization problem caused by geometric attacks by combining the advantages of using image normalizing and geometrically invariant feature points. Robustness against cropping attacks is achieved because the normalization process is applied into sub-images rather than the entire image.

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.

The more distortion on the blue component, the less accurate normalization angle can be used at extraction.

Table 2 Watermark detection results for signal processing attacks (detection rates)

Attacks	RGB Model			YIQ Model		
	Lena	Peppers	Baboon	Lena	Peppers	Baboon
Jpeg 100%	2/8	1/6	5/11	4/8	4/6	3/11
Jpeg 80%	1/8	1/6	2/11	4/8	4/6	3/11
Jpeg 60%	1/8	1/6	3/11	5/8	4/6	2/11
Jpeg 50%	1/8	0/6	2/11	3/8	4/6	2/11
Jpeg 30%	1/8	1/6	1/11	3/8	4/6	1/11
Median filtering 3×3	1/8	0/6	0/11	3/8	3/6	3/11
Low-pass filtering3×3	0/8	1/6	0/11	3/8	2/6	3/11
Gaussian filtering 3×3	0/8	1/6	1/11	2/8	2/6	4/11

Table 3 the watermark detection results for geometric attacks (detection rates)

Attacks	RGB Model			YIQ Model		
	Lena	Peppers	Baboon	Lena	Peppers	Baboon
Rotation 1°	1/8	0/6	2/11	3/8	3/6	4/11
Rotation 5°	2/8	2/6	2/11	3/8	2/6	2/11
Shearing x-1%,y-1%	1/8	1/6	3/11	3/8	2/6	3/11
Shearing x-0%,y-5%	1/8	1/6	2/11	2/8	3/6	3/11
Shearing x-5%,y-5%	1/8	1/6	2/11	1/8	3/6	3/11
Translation-x-5 y-5	1/8	1/6	3/11	5/8	4/6	2/11
Translation-x-10 y-10	1/8	1/6	3/11	5/8	4/6	2/11
Translation-x-20 y-20	1/8	1/6	2/11	5/8	4/6	2/11
Centered cropping 5%	1/8	3/6	6/11	3/8	3/6	1/11
Centered cropping 10%	1/8	2/6	4/11	1/8	3/6	2/11
Centered cropping 20%	1/8	1/6	1/11	2/8	1/6	1/11
Cropping 25% off	1/8	2/6	1/11	3/8	2/6	1/11
Remove 1Row & 5 Col	1/8	1/6	2/11	4/8	4/6	2/11
Remove 5Row & 17 Col	1/8	1/6	1/11	3/8	3/6	2/11
Remove 17Row & 5 Col	0/8	1/6	1/11	4/8	2/6	2/11

4. CONCLUSIONS

This paper presents a robust colour image watermarking scheme, which is designed to be robust against both signal processing and geometric attacks. In order to eliminate synchronization errors between the watermarks embedding and the detection, perceptually significant feature points and image normalization technique were used. The reference image is not required at the detector. The watermark is embedded into the image luminance in YIQ model or in the blue channel in RGB model by modifying the DCT coefficients values in selected blocks.

Experimental results show that the proposed scheme succeeds in making the watermark perceptually invisible and also robust against various signal processing and geometric attacks. Further research is to improve the results by using the color components of YIQ model to determine the feature points.

REFERENCES

[1] L. M. Marvel, C. G. Boncelet, 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] 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.

[8] 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.

[9] I. Nasir and A. Abdurrman, "A Robust Color Image Watermarking Scheme Based on Image Normalization, " World Congress on Engineering, pp. 2238-2242, 2013.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] S. Roy and E.C. Chang, Watermarking color histogram, in proc. Int. Conf. Image Process, pp.2191-2194, 2004.

[19] 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.

[20] 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.

[21] X. Qi, J. Qi, A robust content-based digital image watermarking scheme, Signal processing, vol. 87, pp. 1264-1280, 2007.

[22] 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.

[23] I. Nasir, F. Khelifi, J. Jiang, and S. Ipson, "Robust image watermarking via geometrically invariant feature points and image normalisation", Image Processing, IET, vol.6, no.4, pp.354-363, 2012.

[24] V. Monga and B. Evans, Percetual image hashing via feature points: performance evaluation and tradeoffs, IEEE Trans. on Image processing, vol. 15, no. 11, pp. 3453-3466, 2006.

[25] M. Alghoniemy, and A. H. Tewfik, "Geometric invariant in image watermarking", IEEE Trans. on Image Processing, vol. 13, no. 2, pp. 145-153, 2004.

[26] S. C. Pei and C. N. Lin, "Image normalization for pattern recognition", Image Vision. Computing, vol. 13, no. 10, pp. 711-723, 1995.

Authors

Ibrahim Nasir received B.Eng. from Sebha University, Libya in 1994, M.Sc. degree from Heriot-Watt University, Edinburgh, UK in 2005, and PhD from the University of Bradford, UK in 2010. In 2011, He joined the Department of Electronic and Computer Engineering, University of Sebha, Libya. His interest research topics are Image processing, Mobile robotic and Embedded system.