IMAGE WATERMARKING USING VISUAL PERCEPTION MODEL AND STATISTICAL FEATURES

Meenakshi S.[1] **and Akila C.**[2]

[1,2]University Department, Anna University Tirunelveli, India
Email : [1]meenashree1@gmail.com, [2]akilavp@gmail.com

Abstract

This paper presents an effective method for the image watermarking using visual perception model based on statistical features in the low frequency domain. In the image watermarking community watermark resistance to geometric attacks is an important issue. Most countermeasures proposed in the literature usually focus on the problem of global affine transforms such as rotation, scaling and translation (RST), but few are resistant to challenging cropping and random bending attacks (RBAs). Normally in the case of watermarking there may be an occurrence of distortion in the form of artifacts. A visual perception model is proposed to quantify the localized tolerance to noise for arbitrary imagery which achieves the reduction of artifacts. As a result, the watermarking system provides a satisfactory performance for those contentpreserving geometric deformations and image processing operations, including JPEG compression, low pass filtering, cropping and RBAs.

Keywords: Visual Perception Model, RST, RBAs, Histogram, Gaussian filter, artifacts.

1. INTRODUCTION

With the development of the Internet, more and more digital media products become available through different online services. The rapid growth of the multimedia services has created a potential demand for the protection of ownership since digital media is easily reproduced and manipulated. Digital watermarking has been introduced for solving such problems. One of the most prominent applications of watermarking is using robust and practical watermarking to protect image and video data [1].

In the past ten years, attacks against image watermarking systems have become more and more complicated with the development of watermarking techniques. In a desired watermarking system, the watermark should be robust to content-preserving attacks including geometric deformations and image processing operations. From the image watermarking point of view, geometric attacks mainly introduce synchronization errors between the encoder and decoder. The watermark is still present, but the detector is no longer able to extract it. Different from geometric attacks, the content-preserving image processing operations (such as addition of noises, common compression and filtering operations) do not introduce synchronization problems, but will reduce watermark energy. Most of the previous watermarking schemes have shown robustness against common image processing operations by embedding the watermark into the low-frequency component of images, such as the low-frequency sub bands of discrete wavelet transform [2]. In the literature, only a few algorithms have presented the topic of the robustness against geometric attacks. When the original image (not watermarked) is available in the detection, the cost for resynchronization can be reduced by comparing the original image with the watermarked image (which has undergone some geometric attacks), such as [3]–[6]. Because the non blind watermarking schemes are limited for most practical applications, researchers paid little attention to them.

The non blind schemes are effective to compensate for small local distortion, but the computation cost is dramatically increased under global affine transform [7]. When the original image is not available during the detection, several specialized methods have addressed the issue against geometric attacks by relying on

Exhaustive Search

One obvious solution to de-synchronization is to randomly search for the watermark in the space including a set of acceptable attack parameters. One concern in the exhaustive search [8] is the computational cost in the larger search space. Another is the false alarm probability during the search process.

Embedding Watermark in Invariant Domains

In [9]–[11], researchers have embedded the watermark in affine-invariant domains such as the

Fourier– Mellin transform to achieve robustness to affine transforms. In [9] and [10], the implementation of the watermarking algorithms was considered to be a difficult task due to the use of log-polar mapping. In [11], the authors have solved the problem of implementation by using phase correlation and avoiding the inverse log-polar mapping. Watermarking techniques involving invariant domains are usually vulnerable to cropping and random bending attacks (RBAs) and usually difficult to implement [10].

Embedding Template as Side Information

Another way against geometric attacks is to embed a template in addition to the watermark [2], [12], [13] or insert the watermark many times [14]. In [15], the authors presented a possible attack method to those watermarking techniques based on template in the discrete Fourier transform (DFT) domain [2], [12] because the attackers can access the DFT domain and easily delete the template such as by eliminating the peaks. The performance of the template-based watermarking techniques depends on the dimensionality of the attack parameter space. For some complicated geometric attacks such as RBAs, the template-based methods will be incompetent to estimate the attack parameters. As for cropping, due to the permanent loss of parts of image content, the template may lose its role. In [16], the authors have provided a solution for small local geometric distortions by using invariance properties of fractal coding. The use of synchronization bits as part of the hidden information is applied to estimate and compensate small local or global geometric distortion. They mentioned that the watermarking scheme [16] is sensitive to the distortion by global transforms such as an affine transform.

Using Invariant Region Representations

By embedding the watermark in those regions invariant to geometric attacks, the watermark synchronization errors can be avoided. These invariant representations may be the whole image, some invariant regions or invariant feature points. This class of synchronization techniques are also called second generation schemes [17]. For instance, in [18]– [21], the watermark was embedded into normalization-based moments against affine transforms. Moment-based approaches are highly vulnerable to cropping due to the fact that moments are extracted from all pixels. Once part of the pixels is discarded by an attacker, the moment values may be distorted seriously.

In [7], the Harris detector was used to extract the feature points to group local invariant regions (Delaunay tessellations on the set of points). Two other similar cases using the invariant regions are to generate Harris triangles [22] and meshes [23]. In [24], a novel watermarking scheme dedicated to facial color images was introduced by using salient points like the eyes and the mouth. Because the watermark was embedded into a number of local invariant regions or feature points, the watermarking schemes based on invariant regions will be able to increase watermark resistance to cropping. Under local cropping, some regions are destroyed, but the others may remain unchanged. The problem with these watermarking schemes is the computational burden in the detection due to the use of robust descriptor.

The introduction above demonstrates that watermark robustness to some geometric attacks (i.e., RBAs and random cropping) is still challenging in the image watermarking community. As we know, in an image which has undergone geometric attacks, the position of all or some of its pixels may be modified, the number of its pixels may be decreased or increased linearly (i.e., scaling the size of the image1), and the value of its pixels will be slightly distorted due to interpolation errors during geometric attacks. These properties show that all the geometric attacks respect a rule that some or all of the pixels are displaced at a random amount under the constraint of visual coherence. Based on the rule, an invariant watermarking solution to geometric attacks was proposed using the histogram and the mean.

In comparison with those exploited invariant features in the previous watermarking schemes, the histogram shape (interpreted as the ratios in the number of pixels between groups of two neighbouring bins) and the mean are not only invariant to the scaling, but also resistant to rotation, translation and challenging RBAs due to their property to be independent of the position of pixels in the image plane. Also, the scheme is resistant to a smaller local cropping due to the fact that the cropped samples usually have the same or similar data distribution to the remnant samples in probability.

Considering the interpolation errors during geometric attacks, additive noise, common compression and filtering operations, we introduce the Gaussian filter so that the watermark can be embedded into the low-frequency component of images. Consequently, an image watermarking algorithm robust to geometric attacks and common image processing manipulations is developed. Extensive testing shows that the watermark is robust to various geometric attacks and image processing operations.

In the next section, we briefly introduce geometric attacks and recall the previous histogram-based watermarking techniques. This is followed by a description of our proposed watermarking strategy. We then analyse the watermarking scheme in terms of underlying robustness principle, the performance and the robustness to various content-preserving attacks. Finally, we draw the conclusions.

II. RELATED WORK

Secure Spread Spectrum Watermarking for Multimedia

Signal processing operations such as lossy compression, filtering, digital -analog and analog-digital conversion, re quantization, etc., and common geometric transformations such as cropping, scaling, translation and rotation provided that original image is available and that it can be successfully registered against the transformed watermarked image. Many techniques for watermarking of digital images have appeared in numerous publications. Most of these techniques are sensitive to cropping and/or affine distortions (e.g., rotation and scaling).

Geometric Robust Watermarking Based on a New Mesh Model Correction Approach

This method provides a watermarking scheme based on a new deformable mesh model to combat such attacks. The distortion is corrected using the distortion field (DF) estimated by minimizing the matching error between the meshes of the original and attacked image. This scheme can survive wide range of random bending attacks.

Multimedia Watermarking Technique

The most prominent applications of watermarking are using robust and practical watermarking to protect image and video data. A digital watermark is information that is imperceptibly and robustly embedded in the host data such that it cannot be removed. A watermark typically contains information about the origin, status, or recipient of the host data. Applications include copyright protection, data monitoring, and data tracking. In the literature, only a few algorithms have presented the topic of the robustness against geometric attacks. When the original image (not watermarked) is available in the detection, the cost for resynchronization can be reduced by comparing the original image with the watermarked image.

Recovery of Watermarks from Distorted Images

This method does not require the use of the “original” image, but only a small number of salient image points. Using this method, it is possible to recover original appearances of distorted images. The restored image can be used to recover embedded watermarks. While geometric attacks are one of the most challenging problems in watermarking, random bending is probably the most difficult to handle among all geometric attacks.

An Iterative Template Matching Algorithm Using The Chirp-Z Transform For Digital Image Watermarking

In this paper the author suggests another way against geometric attacks is to embed a template in addition to the watermark. Here we can embed a new template along with the watermark or more number of watermarks to the existing one.

Rotation, Scale and Translation Invariant Spread Spectrum Digital Image Watermarking

In this paper researchers have embedded the watermark in affine-invariant domains using Fourier-Millen Transform to achieve robustness to affine transforms. The implementation of these watermarking algorithms was considered to be a difficult task because of using log-polar mapping.

III. VISUAL PERCEPTUAL MODEL

The visual perceptual model is evaluated in the pixel luminance domain, and use the combination of local statistics through two filters to quantify the noise tolerance of each pixel. One filter estimates the entropy of a local region centered at the pixel-of-interest, and the other computes the differential standard deviation. Visual perceptual model achieves the reduction of artefacts.

Entropy Filter

The output of the entropy filter indicates the content complexity of the neighbourhood for a given pixel k and it is called as entropy map E(k). The entropy map identifies pixels that are perceptually less tolerant to noise, and usually works well for pixels with low entropy, i.e., regions with smoothly changing luminance. Entropy map E(k,r) is defined as,

$$(E\,k,\,r)\ \}-\sum_{i/1}^{256}\ (q\,k,\,i)\log[(q\,k,\,i)]\} \qquad \ldots (1)$$

with $(q\,k,\,i)\ \}\,Pr[k\ \}\}\ i]\ k\in\Pi\ )\ k)]\}$

Differential Standard Deviation Filter

The differential standard deviation filter is used to detect the effect of edges on visual fidelity. The differential standard deviation is calculated as the difference of two standard deviations centered at pixel k: D(k) $= |\,S(k,\,r1)\ S(k,\,r2)\,|$ with block size $r1 > r2$. If both $S(k,\,r1)$ and $S(k,\,r2)$ are low, then the $r1$-neighborhood centered around k is considered not tolerant to noise similarly to the entropy filter. On the other hand, if both and $S(k,\,r1)$ and $S(k,\,r2)$ have high values, it is very likely that the visual content around k is noisy and that it is more noise-tolerant. Standard diviation $S(k,r)$ is defined as,

$$(S\,k,\,r)\ \}\sqrt{\frac{1}{r^2-1}\sum_{i\in(\Pi\,k)}\left(i-\frac{1}{r^2}\sum_{j\in(\Pi\,k)}j\right)^2} \qquad \ldots (2)$$

Complexity Map Generation

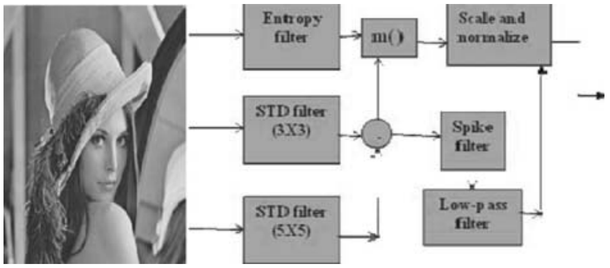

Fig 1: Block diagram of the processing involved in computing a complexity map for a given image.

Complexity Map Generation

Mixing function using Gaussian distribution:

Combine the output of the two filters by employing a mixing function that resembles a smooth AND operator between E(k) and D(k) to arrive at the combined signal of m(D,E). The employed mixing function is nonlinear and has the shape of a 2-D Gaussian distribution

$$m\,(D,\,E)\ \}\exp\left[-\frac{(D-1)^2\ \}\,(E-1)^2}{2s^2}\right] \qquad \ldots (3)$$

where D and E are normalized to be within the range [0,1]and parameter s adjusts the shape of the function. Low values of s raise the complexity value for the pixel with both high E and D while suppressing other pixels. A large s allows pixels with moderate E and D to have moderately high complexity value. In m(D,E) pixels around sharp edges have high values indicating high noise-tolerance. Changes made near sharp edge areas are easily visible and should avoid making changes around those areas. To achieve this, generate a scaling map m'(D,E) which has high values at sharp edge areas and medium to low values at texture and smooth regions to scale down the value of m(D,E) at edge areas.

Spike filter and Lowpass filter:

Generate the scaling map m'(D,E) by applying a 3by-3 spike filter on D(k) followed by a low-pass filter. The spike filter is defined as, $F1 = \{-1/8, -1/8, -1/8; -1/8, 1, -1/8; 1/8, -1/8, -1/8\}$ with "1" in the center and"-1/8" in the remaining places. The final output, called complexity map, is generated as,

$$f\,(I) = \text{m (D, E)/m'(D, E)}. \qquad \ldots (4)$$

As a result, image local region with sharp transitions as well as uniformly or smoothly colored areas are distinguished as "highly sensitive to noise," whereas areas with random texture are identified as "tolerant to noise."

IV. WATERMARK EMBEDDING

Histogram Generation

Histogram is a graphical representation of tonal distribution of an image. The number of pixels with the colour value say 'x' is taken and is placed in the corresponding 'x'th bin in the histogram. The histogram with the bin width 1 will have the histogram range from 0 to 255.In the proposed system, histogram with bin width 2 is considered i.e.) each two neighbouring bins is considered as a same group. So the histogram range is from 0 to 127. The embedding range is given as follows:

$$B = D\,(1 - \lambda)\, A,\ (1 + \lambda)\, A] \qquad \text{... (5)}$$

Where λ is a parameter with value 0.6.Thus maximum range and minimum range is obtained, within which the PN sequence is embedded. PN sequence is used as a private-key and this is inserted by modifying the histogram shape during the embedding process.

Embedding PN sequence

The bits obtained as PN sequence is read one by one and the following procedures takes place. Consider Bin_1 and Bin_2 be two consecutive bins and their population is a and b respectively. The embedding rules are formulated as

$$\begin{cases} \dfrac{a}{b} \geq T, \text{ if } \omega\, i = 1 \\ \dfrac{b}{a} \geq T, \text{ if } \omega\, i = 0 \end{cases}$$

where T is a threshold controlling the number of modified samples which equals 2. If $w(i)$ is "1" and , randomly selected samples from Bin_2 will be modified to Bin_1, achieving $a1/b\,1 = T$. If $w(i)$ is "0" and , randomly selected pixels from Bin_1 will be moved to Bin_2, satisfying $b0/a0 = T$. The strategy of randomly picking up pixels for watermarking is beneficial to coping with the histogram attacks . The rule for watermarking those selected pixels is,

$$\left\{ \begin{array}{ll} f_1'\,(i) = f_x\,(i) + M, & 1 \leq i \leq l_0 \\ f_2'\,(j) = f_2\,(j) - M, & 1 \leq j \leq l_1 \end{array} \right\} \qquad \text{... (7)}$$

Where M is the bin width, $f_1\,(i)$ is the i^{th} selected pixel in Bin_1, and $f_2\,(j)$ denotes the j^{th} selected pixel in Bin_2. The modified pixels $f_1\,(i)$ and $f_2\,(j)$ belong to Bin_2 and Bin_1, respectively. l_0 and l_1 can be computed by the following expressions:

$$l_0 \left\{ \frac{T.b - a}{1T},\ l_1 \right\} \frac{T.a - b}{1T} \qquad \text{... (8)}$$

where $a_1\,(a)\,l_1,\ b_1\,(b - l_1,\ a_0)\ a - l_0,\ b_0\,(b)\ l_0$

V. WATERMARK EXTRACTION

Histogram Based Searching

In the proposed system, histogram with bin width 2 is considered i.e.) each two neighbouring bins is considered as a same group. So the histogram range is from 0 to 127. A searching space SM is calculated based on the Δ value and mean of the Gaussian filtered image. The extracting range is given as follows:

$$SM = \overline{A'}\,1 - |\ \Delta_1\,|\,\overline{A'}\,1\,|\,\Delta_2\,| \qquad \text{... (9)}$$

where Δ is a parameter with value 0.6. Thus maximum range and minimum range is calculated, from which the PN sequence is extracted. Pseudo-random Noise sequence (PN-sequence) is obtained by following the rules,

1. Compute the histogram from range

$$B = [(1{-}\lambda)\,\overline{A'},\ (1 + \lambda)\,\overline{A'}$$

2. Divide histogram bins as groups, two neighboring bins as a group. Suppose that the populations in two consecutive bins are a' and b' respectively. By computing the ratio between a' and b', one inserted bit is extracted in reference to the following equation

3. $$\begin{array}{ll} w'\,(i) = 1\,, & \text{if } a'/b' \geq 1 \\ \quad\ \ 0\,, & \text{otherwise} \end{array} \qquad \text{... (10)}$$

This process is repeated until all the bits are extracted. where w' is an extracted PN-sequence. 3. If the detected sequence is matched with W', the mean based searching process is completed. Otherwise, keep the best matching sequence as W' and let if or if where denotes the searching times and is the step size. Repeat the steps until the search is over.

VI. PERFORMANCE ANALYSIS

Denote the original image and the watermarked image as $F = \{\, f\,(i.j\,|\,i = 1)\ R,\ j = 1 \sim C\,\}$ and $F'' = \{\, f''\,(i.j\,|\,i = 1){\sim}\ R,\ j = 1 \sim C\,\}$. The PSNR value of F versus F^W is,

$$PSNR\ 10\,\log \left(\frac{R.C.255^2}{\sum\limits_{i1}^{R}\ \sum\limits_{j1}^{C}\ |\,f\,(i, j) - f''\ i, j\,|} \right) \qquad \text{... (11)}$$

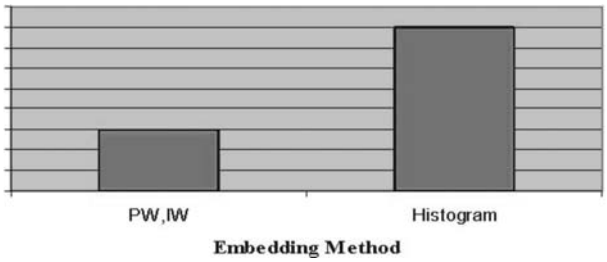

Fig. 2: PSNR value for Different Embedding Methods

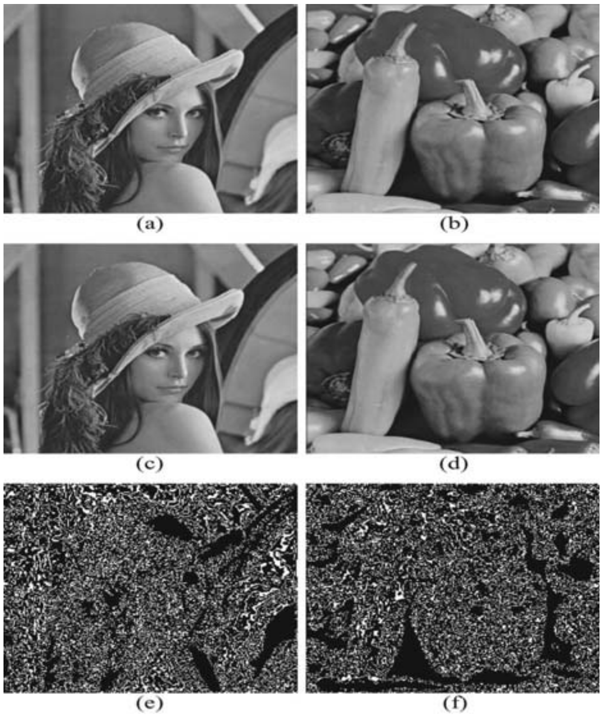

Fig 3 :(a) Original images(Lena and Peppers), the watermarked versions, and the watermark energy in the spatial domain, (a)Lena(original:F1), (b) Peppers(original:F2), (c)Lena(Watermarked:F1w), (d) Peppers(Watermarked:F2w), (e) Watermark $(W=|F1w-F1|)$, (f) Watermark $(W=|F2w-F2|)$.

VII. EXPERIMENTAL RESULTS

The test results show that the proposed watermarking scheme can achieve the requirement of imperceptibility while the watermark is resistant to various geometric attacks and common image processing operations.

VIII. CONCLUSION

A robust image watermarking algorithm against different geometric attacks including challenging cropping operations and RBAs presented by using the property of the histogram shape to be independent of the pixel position, mathematically invariant to the scaling, statistically resistant to cropping. A key-based PN sequence is successfully inserted by modifying the histogram shape, which is computed from the low-frequency component of Gaussian filtered images by referring to the mean. To achieve the high fidelity of the embedded image, a visual perception model is introduced to quantify the localized tolerance to noise for arbitrary imagery. The watermark can be detected without knowledge of original images by sharing the exploited private key in the detector. This watermarking system has a satisfactory performance for different geometric attacks and common image processing operations, including JPEG compression, wiener filtering, cropping, RBAs, etc

REFERENCES

[1] F. Hartung and M. Kutter, “Multimedia watermarking technique,” Proc. IEEE, vol. 87, no. 7, pp. 1079–1107, Jul. 1999.

[2] X. Kang, J. Huang, Y. Shi, and Y. Lin, “A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 776–786, Aug. 2003.

[3] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Proccess., vol. 6, no. 6, pp. 1673–1687, Jun. 1997.

[4] N. Johnson, Z. Duric, and S. Jajodia, “Recovery of watermarks from distorted images,” in Proc. 3rd Int. Workshop Inf. Hiding, 1999, vol. 1768, LNCS, pp. 318–332.

[5] F. Davoine, “Triangular meshes: A solution to resist to geometric distortions based watermark-removal softwares,” in Proc. EURASIP Signal Process. Conf., 2000, vol. 3, pp. 493–496.

[6] P. Dong, J. Brankov, N. Galatsanos, and Y. Yang, “Geometric robust watermarking based on a new mesh model correction approach,” in Proc. IEEE Int. Conf. Image Process., 2002, pp. 493–496.

[7] P. Bas, J.-M. Chassery, and B. Macq, “Geometrically invariant watermarking using feature points,” IEEE Trans. Image Process, vol. 11, no. 9, pp. 1014–1028, Sep. 2002.

[8] M. Barni, “Effectiveness of exhaustive search and template matching against watermark

desynchronization," IEEE Signal Process. Lett., vol. 12, no. 2, pp. 158–161, Feb. 2005.

[9] J. Ruanaidh and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," Signal Process., vol. 66, no. 3, pp. 303–317, 1998.

[10] C. Y. Lin, M. Wu, J. Bloom, M. Miller, I. Cox, and Y.M. Lui, "Rotation, scale, and translation resilient public watermarking for images," IEEE Trans. Image Process., vol. 10, no. 5, pp. 767–782, May 2001.

[11] D. Zheng, J. Zhao, and A. Saddik, "RST-invariant digital image watermarking based on log-polar mapping and phase correlation," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 753–765, Aug. 2003.

[12] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," IEEE Trans. Image Process., vol. 9, no. 6, pp. 1123–1129, Jun. 2000.

[13] S. Pereira and T. Pun, "An iterative template matching algorithm using the Chirp-Z transform for digital image watermarking," Pattern Recognit., vol. 33, pp. 173–175, 2000.

[14] M. Kutter, "Watermarking resisting to translation, rotation and scaling," in Proc. SPIE Multimedia Syst.Appl., 1998, vol. 3528, pp. 423–431.

[15] A. Herrigel, S. Voloshynovskiy, and Y. Rytsar, "The watermark template attack," in Proc. SPIE Electronic Imaging, San Jose, CA, Jan. 2001, pp. 384–405.

[16] J. L. Dugelay, S. Roche, C. Rey, and G. Doerr, "Stillimage watermarking robust to local geometric distortions," IEEE Trans. Image Process., vol. 15, no. 9, pp. 2831–2842, Sep. 2006.

[17] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking schemes," in Proc. IEEE Int. Conf. Image Process., 1999, pp. 320–323.

[18] M. Alghoniemy and A. Tewfik, "Geometric distortion correction through image normalization," in Proc. IEEE Int. Conf. Multimedia Expo, 2000, vol. 3, pp. 1291–1294.

[19] H. S. Kim and H. K. Lee, "Invariant image watermark using Zernike moments," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 766–775, Aug. 2003.

[20] M. Alghoniemy and A. H. Tewfik, "Geometric invariance in image watermarking," IEEE Trans. Image Process., vol. 13, no. 2, pp. 145–153, Feb. 2004.

[21] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Y. Yang, and F. Davoine, "Affine transformation resistant watermarking based on image normalizaton," IEEE Trans. Image Process., vol. 14, no. 12, pp. 2140–2150, Dec. 2005.

[22] J. S. Seo and C. D. Yoo, "Image watermarking based on invariant regions of scale-space representation," IEEE Trans. Signal Process., vol. 54, no. 4, pp. 1537–1549, Apr. 2006.

[23] C. S. Lu, S. W. Sun, C. Y. Hsu, and P. C. Chang, "Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection," IEEE Trans. Multimedia, vol. 8, no. 4, pp. 668–685, Aug. 2006.

[24] A. Nikolaidis and I. Pitas, "Robustwatermarking of facial images based on salient geometric pattern matching," IEEE Trans. Multimedia, vol. 2, no. 3, pp. 172–184, Sep. 2000.

[25] Shijun Xiang, Hyoung Joong Kim and Jiwu Huang "Invariant Image Watermarking Based on Statistical Features in the Low-Frequency Domain," IEEE Transactions on circuits and systems for video technology, vol. 18, no. 6,pp.777-790, june 2008.

[26] Shan He, Darko Kirovski, and Min Wu,"High-Fidelity Data Embedding for Image Annotation," IEEE Trans. Image Process, vol. 18, no. 2, pp. 429–434, Feb. 2009.