Proc. of The Third Intl. Conf. on Advances in Computing, Control and Networking - ACCN 2015.
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-082-8 doi: 10.15224/ 978-1-63248-082-8-80

Taxonomy and Performance Evaluation of Feature Based Extraction Techniques in Digital Image Watermarking

Tanya Koohpayeh Araghi[1], Azizah BT Abdul Manaf [1,] Mazdak Zamani[1] Sagheb Kohpayeh Araghi[2]

***Abstract*—Feature based extraction techniques attract a great attention in digital image watermarking to survive against various removal and geometric attacks. Due to information hiding according to the image content, these techniques find a huge popularity amongst different image watermarking techniques during the recent years. In this paper a survey is investigated in feature based extraction techniques to check, evaluate and compare the recent developments in this area. The aim is to find the vital influential factors on robustness, imperceptibility, capacity, security and speed of the watermarking algorithms proposed based on feature based extraction techniques as a recommendation for future researches. The experimental results prove the robustness of the selected features in each technique against the mentioned geometric and removal attacks.**

Keywords—Digital image watermarking, Geometric attacks and feature extraction

I. Introduction

In recent years, development of multimedia technology, high equipped devices like digital cameras, easy access to cameras on mobile devices, and rapid data transition over the Internet enriches people's lives. However, digital media can be duplicated and shared quickly on the Internet. So, the necessity of effective solutions to protect intellectual property and hinder data piracy, illegitimate access and illegal tampering of data seems to be extremely crucial [1, 2]. In order to answer these requirements digital image watermarking is introduced. It embeds the information within the digital media such that the embedded data becomes a component of its medium. Digital image watermarking has various applications like copy right protection, data authentication, broadcast monitoring and fingerprinting [3, 4].

In a digital watermarking system a tradeoff should be fulfilled amongst perceptual transparency, data capacity and the resistance of the watermark against attacks calls robustness. These requirements are varies depending on the application. For example, for data authentication, imperceptibly and robustness are more significant than data capacity[5].To effectively hide the information, some approaches are introduced like inserting the watermark in spatial domains or transform domains.

In spatial domain techniques, the watermark is inserted directly to the cover image by manipulating some bits of the cover image [6, 7]. they are simple , straightforward and fast techniques [8, 9], easy implementation and low rate of cost and complexity are the other characteristics of these techniques [10] but, they are not robust enough to resist against image processing or geometric attacks [11].Transform domain techniques such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT), concentrate the energy of the host signal in fewer components. They are more robust and provide more capacity in data embedding in comparison to spatial domain techniques [5].

There has been great effort in the last decade to develop the image watermarking resist against geometrical transforms and researchers developed some geometrically invariant transformations [12].Geometric attack is the most serious one of all watermark attacks. For still images, there have been various watermarking proposals against geometrical attacks. The watermark embedding process should be synchronized with the extracting process[1, 13].

Feature extraction is a novel technique to revert the effect of synchronization problems by selecting the features based on the content of the cover image [14]. The main strategy for this purpose is to insert the watermark into the features of the cover image which are geometrically invariant [14-16]. Feature detectors extract some local features of an image by the use of specific transformations. These local features are varied from a point to an object and used for the applications like object recognition, database retrieval, and motion tracking [17].

In this paper, a literature review and a survey is performed to identify the effectiveness of the feature based extraction techniques against synchronization problem and geometric attacks. The most significant feature based extraction techniques are investigated to determine which solution should be emphasized in order to decrease the effect of geometric attacks.

II. Feature Based Extraction Techniques

For solving watermark synchronization problems, feature region detection is one of the several strategies to resist against geometric distortions. In feature based detection, the selected area for watermark embedding and extraction will be determined. Afterwards, this area will be transformed to the regions which have known size, orientation and shape for the purpose of embedding and extraction. Interest points will be chosen based on the content of image. In general feature based watermarking follows from this process: first, selecting the maximum feature points of the picture so that the other districts do not effect and suppressed the quality of the whole image. Then the ultimate set of selected points is finalized by the threshold analysis.

1. Advanced Informatics School Universiti Teknologi Malaysia, 54100, Malaysia
2. Multimedia University

SEEK DIGITAL LIBRARY

Proc. of The Third Intl. Conf. on Advances in Computing, Control and Networking - ACCN 2015.
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-082-8 doi: 10.15224/ 978-1-63248-082-8-80

Finally, extracted feature points are applied as areas for watermark insertion while these feature points should be detectable without synchronization error at the receiver [18, 19].

2.1 Related Works of Feature Based Extraction using Harris Laplacian Transform

In [17], instead of selecting feature points based on some of the criteria like number of neighboring feature points or corner response which cannot guarantee the maximum robustness, they select a number of non-overlapped feature regions aiming to keep the high quality of the watermarked image as well as maximum robustness. For this purpose, the candidate feature regions are exposed under various types of attacks and the most robust feature regions are chosen. In order to search a minimal primary feature set, a track-with-pruning procedure is adopted and for attaining robustness against undefined attacks auxiliary feature regions will be added formulating as multi-dimensional knapsack problem (MDKP) with the aid of genetic algorithm.

The point of this technique is to find small robust regions resisting against removal and geometric attacks. These regions are not repeated in selection. However, measuring the robustness of the selected features against simulated attacks seems to be very time consuming and reduce the speed of the technique. Unfortunately the authors did not mention the value of PSNR and NCC after attacks.

In [19] an image watermarking approach proposed in which the emphasize is on prevention of the leakage of information and proposing a secure technique by incorporating randomization to select the feature points for watermark embedding and elimination of simulated attack procedure by scattering the selected features over the cover image resulting the robustness of the technique in better coverage against cropping, random cropping and centered cropping and signal processing attacks in addition to the other attacks prevented to their mentioned previous work.

For this purpose, firstly, the Harris Laplacian is exerted to the cover image to localize the feature points in the scale space. Then the Laplacian of Gaussian operation is applied in order to choose the points having maximum over scales. The circular feature regions are chosen among all of the candidate feature points based on their scale specifications and a secret key. In order to avoid degradation of the watermarked image quality, and increasing the stability of the feature points, it is necessary to find non overlapped feature points. So the optimal non overlapping regions will be selected randomly based on Genetic Algorithm and Multi-Dimensional Knapsack Problem. Finally normalization is done on the feature points to resist against geometric attacks and avoiding redundant signals to be hidden in each region.

Experimental results represent the robustness of this method against geometric and common signal processing attacks. False positive has a low rate and there is not a great degradation in watermarked quality. However, using noise visibility function (NVF) to make a balance between imperceptibility and robustness leading to pre calculation in feature detection, feature region selection, and watermark insertion. On the other hand, since selecting the large values for the secret key causes exceeding the most feature regions from the image size and small values results to smaller feature points capacity than the watermark size, there is a dependency between the secret key and radius of the features. If the number of feature points and their size is high, the leakage of information is probable [17] proposed a feature based extraction method using Harris Laplacian, Laplacian-of-Gaussian, and Susan detectors to extract the feature points. For region selection process they selected non overlapped regions based on the specifications that each detector has offered. For example Harris Laplacian and Laplacian-of-Gaussian offer RST invariant specifications. In order to find minimal primary areas, selected regions are pollarded by the use of pruning algorithm. After choosing suitable regions, the watermark is embedded to the areas using Discrete Cosine Transform (DCT).

Since in this method the watermark is not embedded in spatial manner, it is believed that it would be better than other spatial domain embedding algorithms in terms of robustness and imperceptibility. However experimental results show the robustness of the technique against just several attacks represented in Figure 1. On the other hand, load of computation is increased because of repeating the DCT calculation for each selected regions.

In [20], a watermarking scheme proposed according to image normalization and rotation invariant features. In this scheme, at first, the cover image is segmented into homogeneous areas using Bayesian image segmentation. Afterwards, for each chosen area, one feature point is selected by the use of Gaussian Scale model. Then the orientation of feature points for every circular region centering at the feature points is calculated. In order to make each selected regions to their compact size image normalization is employed to make the regions scale invariant. To enhance embedding watermark strength based on the specifications of each region, the Noise Visibility Function is performed. In comparison to the other mentioned methods and considering Figure 1 this method can cope with fewer attacks in addition to the other limitations like lack of speed and imposing pre calculations.

.

2.2 Related Works of Feature Based Extraction using Affine Covariant Regions (ACR)

In [21], the feature points are considered as Affine Covariant Regions (ACR) and for selecting these regions, affine invariant point detector is employed. Since these regions are including some common areas, the graph theatrical algorithm is used to find non overlapped ACRs to prevent the low quality of the watermarked image. Then, selected areas are normalized locally in which each ellipse area is transformed to a circle align with its dominant gradient orientation. The circular watermark will be hidden in these normalized regions and to make a tradeoff between imperceptibility and robustness an indirect inverse normalization will be adopted after watermark embedding to

SEEK DIGITAL LIBRARY

Proc. of The Third Intl. Conf. on Advances in Computing, Control and Networking - ACCN 2015.
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-082-8 doi: 10.15224/ 978-1-63248-082-8-80

optimize the strength of it. The watermark is embedded in a spatial manner.

Finding affine invariant points of the cover image, this scheme copes with synchronization error in geometric attacks. However, identifying the solidity of the selected feature points, pre calculation is required to specify a threshold value. On the other hand, in this scheme the watermarking embedding operations applied in a spatial domain. So, all of the flaws of spatial domain watermarking mentioned in introduction is inherited by this scheme.

2.3 Related Works of Feature Based Extraction using Binary Patch and Zernike Transform)

In the work proposed by [22] a Robust Feature Point Detector (RFPD) is introduced . In order to find invariant feature areas, Scale Invariant Feature Transform (SIFT) algorithm is used. SIFT refers to an algorithm in which an image is transformed to a big set of vectors of local features. The selected circular regions are candidate for watermark embedding and extraction. After choosing the circular feature points, they are transformed into a set of binary images by applying Zernike transform. The reason is to avoid cumulative computation errors stemming from inverse Zernike transform which causes degradation of image quality. Finally, the size of local Zernike moments will be computed and changed for watermark embedding and extraction.

This scheme can resist against common signal processing and geometric attacks. However, it suffers from high computational load as well as the main computation of watermark embedding and extraction. Additionally, the value of PSNR is not mentioned after attacks.

3 Comparison and Discussion

Although feature based extraction techniques find their popularity among different methods against geometric attacks, utilizing these techniques need to consider the following issues. At first deviation of scale occurs in these techniques when the watermark is exposed on attacks or even without attacks causes some distortions on selected features in comparison to non-featuring areas leading to false positive problem.

On the other hand, in the algorithms used DWT, DCT or DFT transforms, for each detection process these transforms should be done for the selected feature points imposing a high computational load on the system practical [15] and finally, in order to increase the performance of the algorithm. Feature points in both detection and extraction parts should be the same which makes constraints on the system.

Capacity is also depends on the radius of the selected features which means that the limitation of capacity is exist in feature based extraction techniques. Comparisons among each of the mentioned works are performed in Table 1. All done in gray scale. In this table the influential factors affected on robustness, capacity and imperceptibility of the watermarking methods are shown and each technique is investigated based on these factors. The attacks that can be detected and prevented by each technique are shown in Figure1. The colored squares show the name of each attack.

TABLE 1. Investigation and comparison of the techniques based on important influential factors.

Author/Year / **Influential factors**	Yuan 2014	Tsai 2012	Malsh 2012	Tsai 2011	Gao 2010	Priya 2010
Sufficient robustness (signal processing & geometric attacks)	no	yes	no	yes	yes	no
False positive affect	yes	yes	yes	yes	yes	yes
Degradation of the watermark quality	no	no	yes	no	no	yes
Repeated feature regions	yes	no	no	no	no	no
Sufficient security	no	yes	no	no	no	no
robust small regions	yes	yes	yes	yes	yes	yes
pre calculation	yes	yes	yes	yes	yes	yes
Dependency of capacity to the secret key	yes	yes	-	yes	-	-
Time consuming	yes	no	no	yes	yes	yes
High speed	no	yes	yes	no	no	no
Watermark inserted in spatial domain	yes	yes	no	yes	yes	yes

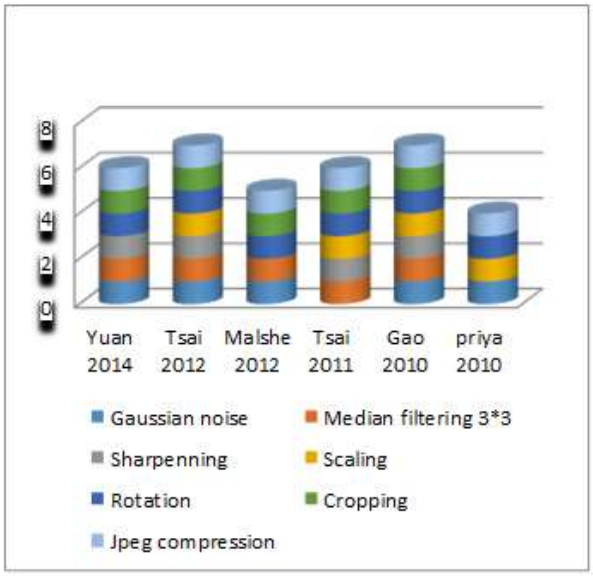

Fig. 1. The number of attacks each technique Resist against.

4. Conclusion and Future Work

In this paper, we presented an overview of digital image watermarking and existing references on feature based extraction techniques. Different algorithms proposed based on these techniques were explored and the most vital factors affected on robustness, imperceptibility, capacity, security and speed of the algorithms investigated and the strength and flaws of each technique is discussed. Future work is to design and implement a new algorithm in feature based extraction techniques considering the advantages and avoiding the disadvantages of the current works by incorporating the influential factors introduced in this paper.

SEEK DIGITAL LIBRARY

Proc. of The Third Intl. Conf. on Advances in Computing, Control and Networking - ACCN 2015.
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-082-8 doi: 10.15224/ 978-1-63248-082-8-80

Acknowledgement

This work is a part of research supported by Ministry of Education (MOE), Malaysia, with the grant No.R.K130000.7838.4F643.

References

[1] Li, L., et al., *AN H.264/AVC HDTV watermarking algorithm robust to camcorder recording.* Journal of Visual Communication and Image Representation, 2015. **26**(0): p. 1-8.

[2] Dadkhah, S., et al., *An effective SVD-based image tampering detection and self-recovery using active watermarking.* Signal Processing: Image Communication, 2014. **29**(10): p. 1197-1210.

[3] Amirmazlaghani, M., M. Rezghi, and H. Amindavar, *A novel robust scaling image watermarking scheme based on Gaussian Mixture Model.* Expert Systems with Applications, 2015. **42**(4): p. 1960-1971.

[4] Dolatabadi, Z.S.S., A.B.A. Manaf, and M. Zamani, *Using Three Levels DWT to Increase Robustness against Geometrical Attacks.* International Journal of Advancements in Computing Technology, 2013. **5**(14): p. 86.

[5] Sahraeian, S.M.E., et al., *Information hiding with maximum likelihood detector for correlated signals.* Digital Signal Processing, 2015. **36**(0): p. 144-155.

[6] Tsai, H.-H., Y.-J. Jhuang, and Y.-S. Lai, *An SVD-based image watermarking in wavelet domain using SVR and PSO.* Applied Soft Computing, 2012. **12**(8): p. 2442-2453.

[7] Abbasi, A. and C. Woo, *Robust Image Watermarking Using Genetic Programming.* Journal of Software & Systems Development, 2012.

[8] Wang, Z., N. Wang, and B. Shi. *A novel blind watermarking scheme based on neural network in wavelet domain*. in *Intelligent Control and Automation, 2006. WCICA 2006. The Sixth World Congress on*. 2006: IEEE.

[9] Muselet, D. and A. Trémeau, *Recent trends in color image watermarking.* Journal of Imaging Science and Technology, 2009. **53**(1): p. 10201-1.

[10] Lin, S.D., S.-C. Shie, and J.Y. Guo, *Improving the robustness of DCT-based image watermarking against JPEG compression.* Computer Standards & Interfaces, 2010. **32**(1): p. 54-60.

[11] Singh, A.K., et al. *A novel technique for digital image watermarking in spatial domain*. in *Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on*. 2012.

[12] Hong-Ying, Y., et al., *Geometrically resilient digital watermarking scheme based on radial harmonic Fourier moments magnitude.* AEU-International Journal of Electronics and Communications, 2015. **69**(1): p. 389-399.

[13] Moghaddasi, Z. and A.B.A. Manaf, *Secure Genetic Based Image Steganography System in Frequency Domain.*

[14] Wu, H.-T., J.-L. Dugelay, and Y.-Q. Shi, *Reversible Image Data Hiding with Contrast Enhancement.* Ieee Signal Processing Letters, 2015. **22**(1): p. 81-85.

[15] Su, P., Y. Chang, and C. Wu, *Geometrically Resilient Digital Image Watermarking by Using Interest Point Extraction and Extended Pilot Signals.* 2013.

[16] Wu, P., *Research on digital image watermark encryption based on hyperchaos.* 2013.

[17] Tsai, J.-S., 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, 2011. **20**(3): p. 735-743.

[18] Tao, H., et al., *Robust Image Watermarking Theories and Techniques: A Review.* Journal of Applied Research and Technology, 2014. **12**(1): p. 122-138.

[19] Tsai, J.-S., et al., *Joint robustness and security enhancement for feature-based image watermarking using invariant feature regions.* Signal Processing, 2012. **92**(6): p. 1431-1445.

[20] Priya, N.N. and S.L. Stuwart, *Robust feature based image watermarking process.* International Journal of Computer Applications, 2010. **4**(5): p. 13-16.

[21] Gao, X., et al., *Geometric distortion insensitive image watermarking in affine covariant regions.* Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, 2010. **40**(3): p. 278-286.

[22] Yuan, X.-C. and C.-M. Pun, *Feature extraction and local Zernike moments based geometric invariant watermarking.* Multimedia Tools and Applications, 2014. **72**(1): p. 777-799.

SEEK DIGITAL LIBRARY