International Journal of Electronics and Communication Engineering (IJECE)
ISSN(P): 2278-9901; ISSN(E): 2278-991X
Vol. 3, Issue 4, July 2014, 55-60

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

FEATURE REGION SELECTION BASED ON SIMULATED ATTACKING FOR EFFICIENT DIGITAL IMAGE WATERMARKING

VIVEK R. NAGRE, PANKAJ P. TASGAONKAR & VYANKATESH GUTTE

Department of Electronics and Telecommunication Engineering, College of Engineering, Pune, Maharashtra, India

ABSTRACT

This paper proposed a new approach towards detecting feature region for efficient digital image watermarking. The non-overlapping feature regions which can resist most of the predefined attacks are selected. Initially, the Harris- Laplacian detector is used to extracts the features from the cover image. The primary feature region set is formed from extracted regions based on their corner response. The watermark is embedded into the extracted primary features, the simulated attacking is performed over these regions in order to checks their robustness against predefined attacks using BER. Minimal primary feature set which can resists the most predefined attacks is selected with the help of, a track-with-pruning procedure. Primary feature set is then extended by adding auxiliary feature regions in it to enhance its resistance capability against undefined attacks. A multi-criteria optimization strategy such as genetic algorithm is adopted for this purpose.

KEYWORDS: Feature, Genetic Algorithm, Multi-Criteria Optimization, BER, Simulated Attacks

INTRODUCTION

Accessing and manipulation of data has become easier due to the rapid growth of internet. Major problem with internet applications such as real-time video and audio delivery, digital libraries, and Web advertising is protection against copyright. Thus digital watermarking has been proposed as a solution for proscribing copyright violation of digital data. The effectiveness of a digital image watermark relies on its robustness against various attacks. Attacks on watermarking scheme are classified as signal processing attacks and geometric attacks [1]. first types of attacks include filtering operations and compressions whereas second type includes attacks like rotation, translation, cropping, scaling. The existing methods for watermarking do not imply higher robustness and may degrade the quality of the digital image against unknown attacks as characteristics of unknown attacks vary with known attacks.

Thus, the difficulty is to select most robust feature region set for information hiding. The robust regions are mainly used to sign copyright information of the digital work as they can resist various kinds of attacks and can preserve image quality after watermarked. The two important issues that encounters during feature region selection are: 1) repeated selection of characteristic region 2) complexity in selecting most smallest and robust region set. [2]. first issue can be addressed by choosing non overlapping feature regions because magnitude of pixel in corresponding region will change after watermarking and it may degrade image quality. The selected region has various degrees of resistance against different attack. Therefore we propose a method base on simulated attacking that considers prior knowledge of attack resistance capability of each region.

PROPOSED METHOD

Here the proposed process of detecting optimal regions is elaborated. The proposed technique extracts the features from the cover image using Harris -Laplacian detector. The regions with higher corner response

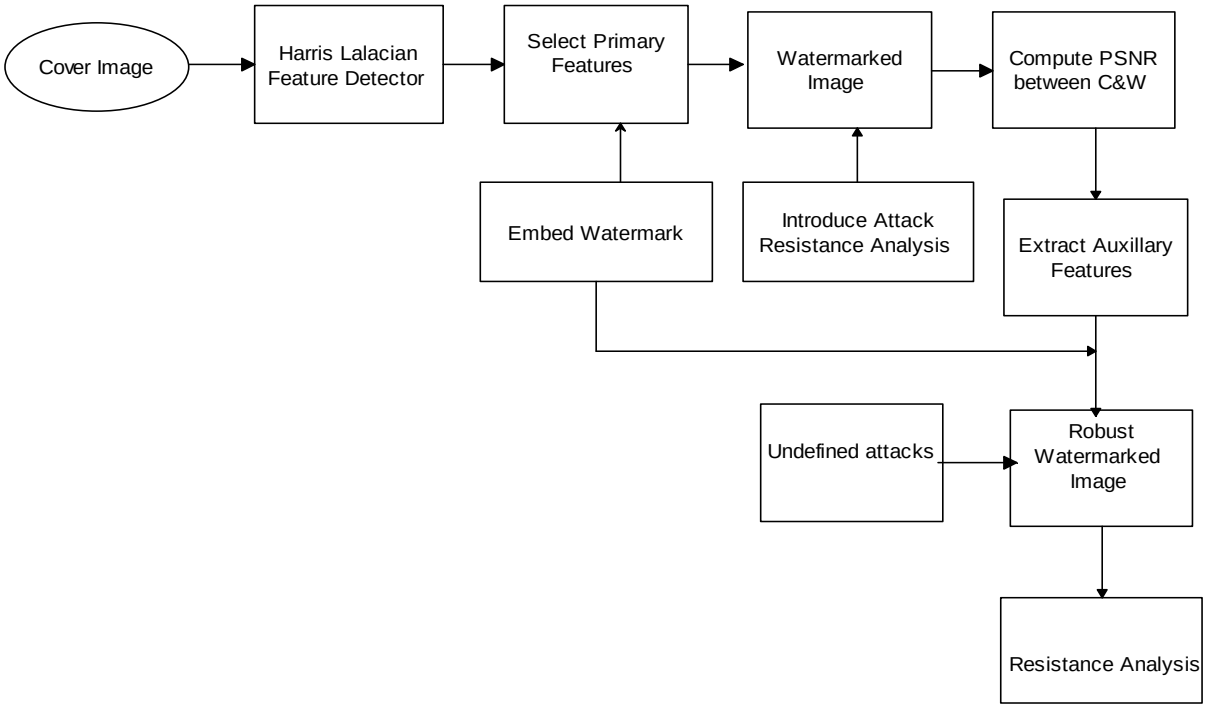

Figure 1: Block Diagram of Proposed Feature Region Selector

Are selected when the Harris–Laplacian detector is used [4]. Figure 1 shows the overall flow of the proposed method. The first stage selects primary feature region set which can resist most of predefined attacks. Resistance Analysis checks the robustness of the watermarked feature region against predefined attacks such as rotation, scaling, median filtering, JPEG compression and salt and pepper noise. Feature set obtained in first stage is extended by adding some auxiliary feature regions by genetic search approach in order to enhance its resistance against undefined attacks.

Feature Set Searching Stage

This stage aims at selecting non overlapping feature region set for watermarking based on attack simulation method.

- **Extract Primary Features**

Feature detectors are used to extract local features from image. By performing specific transformation on images feature detector extract their local features, ranging from a point to an object, and have been adopted in many applications such as object recognition, database retrieval, and motion tracking [5]. Most features such as corners in an image can be preserved after it suffers a distortion such as scaling, rotation, or illumination changes. Therefore, several feature-based methods have been developed by exploiting the robustness of feature regions against various attacks.

Figure 2: (a) Original Image (b) Selected Regions from Features Detected by the Harris–Laplacian Detector

Here we have used Harris-Laplace detector to detect regions based on corner response. Figure 2 shows the regions detected by Harris-Laplace corner detector.

- **Attack Simulation and Selection of Non-Overlapping Regions**

As the magnitude of the pixel belonging to region gets modified after being watermarked, selection of non-overlapping regions is highly preferable to avoid major degradation of image quality. The robustness of all regions by a single criterion like the corner response is difficult to identify. Therefore we adopted attack simulation method. Prior knowledge of each region's attack resistance capability will lead to find out most robust features for watermarking. Moreover, a feature region may have different degrees of robustness against different attacks [2], [8]. A few representative attacks are applied to the feature regions for evaluating their robustness in the simulated attacking phase. In the attack resistance analysis phase feature regions originally detected are first checked if they can be re-detected in the attacked image. Watermark inserted previously is extracted from these redetected regions to examine the consistency (bit error) between itself with the original watermark. Using $d_{\mathrm{r,\,a}}$ to indicate whether the region can resist the pre defined attack

$$d_{\mathrm{r,a}} = \begin{cases} 1, \mathrm{BER}(\mathrm{W}, \mathrm{W_r}) \le T \\ 0, \text{otherwise} \end{cases} \tag{1}$$

Where $\mathrm{BER}(\mathrm{W}, \mathrm{W_r})$ denotes bit error between W and $\mathrm{W_r}$. T is predefined bit error threshold. In the final phase, the most robust and smallest set of non-overlapping feature regions is selected according to the result of attack resistance analysis. This work is formulated as follows:

$$R_P^* = arg \max_{R_p} \left\{ \sum_1^{N_a} x_{a_i}^{R_P} \, min\left|R_p\right|;\ \forall r_k r_j \in R_p, k \neq j \rightarrow r_k \cap r_j = \emptyset \right\} \tag{2}$$

Where isR_p a set of selected feature regions in which two regions $r_k$and r_j are not overlapped, and the value of for a predefined attack is determined by the value of $x_{a_i}^{R_p}$ for predefined attack a_i is determined by

$$x_{a_i}^{R_p} = \begin{cases} 1, \exists \mathrm{r} \in R_p, d\mathrm{r}, a_i \neq 0 \\ 0, \text{otherwise} \end{cases} \tag{3}$$

The regions selected are complementary in attack resistance in order to improve its robustness against various attacks. Track with pruning algorithm aims to select minimal primary feature region which can resist more predefined attacks.

A Track with Pruning Algorithm

Step 1: All feature region detected by Harris Laplace detector are given as input, R0

Step 2: Initialize non overlapping primary feature region set Rp and prune set Rprune as Null. Set the size of inspected feature region sets as unity.

Step 3: Iterative search is performed.

Step 4: If number of attack resisted increases the candidate set is assigned as new primary feature set and if it cannot resist more attacks the candidate set is included in the pruned set by adding more feature regions.

Step 5: Update the primary feature region set with a candidate feature region set if the latter can resist more attacks than the former.

Step 6: Stop when all candidate set are examined.

Finally at the output stage we get minimal primary feature region set

Optimization Stage

Primary feature region set which can o resist most of the predefined attacks is obtained at previous stage. This set may fail to resist some undefined attacks, hence we need to add some auxiliary regions selected from those residual feature regions to enhance the robustness of image against undefined attacks under constraint of preserving its visual quality. Since the characteristics of undefined attacks are of wide variety and are difficult to model, we therefore adopt a multi-criteria optimization strategy [6], for the selection of auxiliary feature regions. Neither corner response nor the number of its neighboring feature points, however, can guarantee the selection of non-overlapping regions with the maximum robustness to various attacks, because higher corner response and a large number of its neighboring feature points do not always imply higher robustness of itself. Moreover, a feature region may have different degrees of robustness against different attacks [3], [5].

The symbol g_r^a is defined to indicate the overall resistance degree of the region against all predefined attacks, and it is determined by

$$g_r^a = \left(d_{r,a1} + d_{r,a2} + \cdots + d_{r,a_{N_a}}\right) = \sum_{i=1}^{N_a} d_{r,a_i} \quad (4)$$

Where,

$d_{r,ai} \in \{0,1\} \rightarrow$ indicates whether region can resist i^{th} predefined attack a_i

$N_a \rightarrow$ total number of predefined attacks

The resistance of a region against a predefined attack is one of the important characteristic of the region. The symbol g_r^a is the summary representation of attack resistance characteristics of a region. Other two characteristics of feature regions, the corner response and the integration scale are also referred. $g_{r_j}^c$ is a property related to corner response. Threshold operation is done to eliminate regions having corner response which can unstable them. In this paper threshold is set to 0.01 of maximum response [4]. For integration scale we set up parameters of initial scale, scale step factor and number of scales as 1.5, 1.2, and 13, respectively. These scales are categorized into various bands but region with scale

level in middle band are more likely to resist attacks [7]. Symbol $g_{r_j}^{\sigma}$ to indicate that scale value belongs to middle band. Therefore, the work of the extension stage can be formulated as an optimization problem which further can be converted as Multidimensional knapsack problem (MDKP) with multiple constraints as follows and a heuristic search procedure is adopted to solve this MDKP for determining the best choice of auxiliary feature regions

Maximize:

$$\sum_{j=1}^{|Rp*|} (g_{r_j}^{a} + g_{r_j}^{c} + g_{r_j}^{\sigma}) s_{r_j}$$

Subject to:

$$\sum_{j=1}^{|Rp*|} q_{r_j} s_{r_j} \leq Q_c$$

$$\sum_{j=1}^{Rp*} p_{r_i,r_j} s_i \; s_{r_j} < 1, \; i = 1, 2, 3 \ldots\ldots\ldots Rp*$$

Where

$R_{p\rightarrow}^{*}$ The number of feature regions except those in the primary feature region set as well as the regions overlapped with them and s_{r_j} is defined as

$$s_{r_j} = \begin{cases} 1 \text{ if } r_j \text{ is selected} \\ 0 \text{ otherwise} \end{cases}$$

The value of p_{r_i,r_j} indicates whether the two regions are overlapped and is defined as

$$p_{r_i,r_j} = \begin{cases} 1 \; r_i \cap r_j = \emptyset \\ 0 \text{ otherwise} \end{cases}$$

The parameter which denotes the limitation of quality degradation of an image after being attacked considered as peak signal-to-noise ratio (PSNR) value between a cover image and attacked image. A Genetic search algorithm is used to select optimal feature region set which is robust against unknown attacks.

EXPERIMENTAL RESULTS

Table 1, shows the resistance of each region against signal processing and geometric attacks along with their corner response. The systems implement Harris-Laplacian based robust region selection. The corner response values are used to remove overlapping feature regions. TABLE 1 illustrates the comparisons, based on the criterion of detection ratio, defined as the ratio of the number successfully detected regions with respect to total number of regions in an image.

- Number of Regions for optimization {7, 3, 5, 6, 8}
- Number of Regions obtained after GA {8, 3, 5}

Table 1

Regions	Corner Response	JPEG	LPF	Rotation 30	Gaussian Filter	Median 3*3	Rotation 15
3	117145	1	1	1	1	1	1
5	90636	0	1	0	1	1	1
6	97691	1	0	1	0	1	1
7	102319	1	1	1	0	0	1
8	442695	1	1	1	0	1	0

The table 2 illustrates the detection results for Lena, baboon, and pepper images against attacks. The ratio of no of successfully detected regions to total no. of watermarked regions

Table 2

Image	JPEG	LPF	Rotation 30	Gaussian Filter	Median 3*3	Rotation 15
Lena	4/5	4/5	4/5	5/5	3/5	5/5
Football	6/8	5/8	6/8	6/8	4/8	7/8
Pepper	8/12	3/12	7/12	6/12	9/12	6/12

CONCLUSIONS

In this paper a new technique has been proposed with an objective of selecting robust regions in an image which can resist most predefined attacks under the constraint of preserving image quality. Here, Harris-Laplacian feature detector is used to select the primary features from the cover image. The watermark is embedded into the extracted primary features, and its robustness against six different predefined attacks is evaluated using BER. Most of the attacks are resisted by our algorithm because of invariant property of feature regions. As our detector is based on uniform Gaussian scale the circular regions fails to resist attacks of aspect ratio, we are still making our efforts to overcome this issue. In order to enhance the resistance capacity against undefined attacks, we embed the watermark into auxiliary regions which are detected by heuristic search approach. In order to deal with security issues cryptographic authentication technique can be implemented in future.

REFERENCES

1. D. Zheng, Y. Liu, and J. Zhao, “A survey of RST invariant image water marking algorithms,” *ACM Computer Surv.* vol. 39, no.2, pp.1–91, Jun.2007
2. n-Sheng Tsai, Win-Bin Huang, and Yau-Hwang Kuo, “On the Selection Optimal Feature Region Set for Robust Digital Image Watermarking”, in *IEEE Transaction on image processing*, vol. 20, no. 3, march 2011
3. J. S. Tsai, W. B. Huang, C. L. Chen, and Y.H.Kuo, “A feature-based digital image watermarking for copyright protection and content authentication, "in *Proc. IEEE Int. Conf. Image Process*., Sep. 200, vol.5, pp. 469–472.
4. C. Schmid, R. Mohr, and C. Bauckhage, “Evaluation of interest pointdetectors,” *Int. J. Computer Vis.*, vol. 37, no. 2, pp. 151–172, Jun. 2000.
5. C. W. Tang and H. M. Hang, “A feature-based robust digital image water marking scheme,” *IEEE Trans. Signal Process.*, vol. 51, no. 4,pp. 950–959, Apr. 2003
6. H. Kellerer, U. Pferschy, and D. Pisinger, *Knapsack Problems*. Berlin: Springer, 2004.
7. J. S. Seo and C. D. Yoo, “Image watermarking based on invariant regions of scale-space representation,” *IEEE Trans. Signal Processing*, vol. 54, no. 4, pp. 1537–1549, Apr. 2006
8. A. A. Borse and S. M. Kamlapur, “Selection of feature regions set for digital image using optimization algorithm,” *International Journal of Communications Networking System* vol 01, Issue 02, December 2012
9. F. A. P. Petitcolas, “Watermarking schemes evaluation,” *IEEE Signal Process. Mag.*, vol. 17, no. 5, pp. 58–64, Sep. 2000