Enhanced Robustness for Digital Images Using Geometric Attack simulation

Ferdin Joe J\textsuperscript{a}, Vaikunda Raja T\textsuperscript{b}

\textit{Department of Computer Science & Engineering, Prathyasha Institute of Technology & Management, Anna University, Chennai.}

Abstract

The effectiveness of a digital watermarking algorithm is indicated by the robustness of embedded watermarks against various attacks. Attacks which attempt to destroy watermarks have two types, noise-like signal processing and geometric distortions. To select a non-overlapping region, some reference parameters have been used, the regions with higher feature corner response are selected when the Harris–Laplacian or Harris–affine detector is used. The number of neighboring feature points inside a region is a major reference for obtaining a non-overlapping set in the watermarking method based on Mexican Hat wavelet scale interaction. A watermarked feature region may have different degrees of robustness against different techniques if there is prior knowledge of each region's attack resistance capability. We proposed a feature region selection method based on the idea of simulated attacking and finding the Optimal feature region set.

© 2012 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of Noorul Islam Centre for Higher Education. Open access under CC BY-NC-ND license.

Keywords: Feature detector; robust digital watermarking; Optimal Feature region.

Introduction

A feature region selection method for robust digital image watermarking is proposed here. The existing methodology discussed in [2], [3], [4], [5] and [6] have various difficulties and drawbacks. The tamper-resistant algorithm used in [2] can be extracted by using the spread spectrum type of attack. The watermark will be constructed as an independent and identically distributed Gaussian random vector that

\textsuperscript{a} Email: ferdinjoe@gmail.com,
\textsuperscript{b} Email: tvaikundaraja@gmail.com
is invisibly inserted in a spread-spectrum into the perception of most significant spectral components of the data. The robust digital watermark used in [3] detects by the cryptographic attack and the image quality after inserting the watermark got degraded than the original one. It makes use of terms agreed for information hiding. The term cover image is used to describe the unmarked original image and stegoimage for an image with one or more hidden embedded marks. One significant deviation from the recommended steganographic nomenclature is that the frequent use of the term watermark is to describe the embedded mark.

The cocktail watermark encoding algorithm was developed based on the assumption that the original image is gray-scale [3]. The wavelet transform adopted is constrained such that the size of the lowest band is 16*16. The hidden watermark is either a noise-style watermark or a bipolar watermark. Gray-scale watermark hiding is found in another work. A noise-style watermark is Gaussian distributed with zero mean and unit variance. A bipolar watermark value is defined as the sign of a noise-style watermark value, and the magnitudes of the Gaussian sequence are used as the weights for modulation. The watermarking scheme is used as normalized image for both watermark embedding and detection in [4]. The normalized image is obtained from a geometric transformation procedure that is invariant to any affine distortions of the image. This ensured the integrity of the watermark in the normalized image even when the image underwent affine geometric attacks. Image Normalization Based Watermarking System is noted that the cover image is not needed for the watermark extraction. This scheme is suitable for public watermarking applications. Watermarked image undergoes a geometric attack that cannot be simply described by RST or more general affine transforms. It is not feasible, to describe the actual image distortion by a global geometric transformation model. Such geometric attacks may cause hardly noticeable perceptual distortion, but have catastrophic effects to many existing watermarking algorithms.

A digital image watermarking scheme must be robust against a variety of possible attacks. Geometric distortions are more difficult to handle than other types of attacks in [5]. Some number of rotation and scaling invariant watermarking algorithms were used in the conventional method. The Fourier Mellin transform (FMT) has the property of rotation and scaling invariance. Once the Discrete Fourier Transform (DFT) and the FMT are applied to an image, the image will be transformed to the rotation, scaling, and translation (RST) invariant domain. The watermark embedded into this domain is found to be RST invariant. The implementation difficulties hinder the research of watermarking schemes based on this principle.

Tsai et al in [15] has proposed a method for no overlapping region selection. This work has the implementation using the attack simulation and thereby increasing the robustness of the images. During the extraction of data, there is some degradation in the quality of images. This quality factor is taken as the key problem to solve.

To reduce the probability of error and make the feature points still detectable after distortions, the feature points that are very robust to the concerned distortions are selected for watermarking process. The segmented image is used to detect the feature points, because it is low-pass filtered and all the high-frequency components that are sensitive to many distortions have been removed. Due to the small size of the watermark embedding area in the given algorithm, the experimental results show that the linear correlation is sensitive to the image contents and the watermark patterns, which makes it difficult to analyze the watermarking processes using linear correlation as the watermark detector. The fluctuation of the linear correlation values is caused by the correlation between the natural image content and the watermark pattern. To improve the performance of the watermark detector, preprocessing is applied before calculating linear correlation. We has two issues of existing feature-based schemes; one is avoiding repeated selection of robust regions for watermarking to resist similar attacks, and the other is the difficulty of selecting the most robust and smallest feature region set to be watermarked.
2. Related Works

The background work for the proposed methodology is discussed in detail in this section. Many techniques are discussed in digital watermarking over time. The track-with-pruning algorithm is developed to search for the optimal solution. The first operational stage is responsible to find out a minimal feature region set under the objective of resisting as many predefined attacks as possible. The algorithm aims to select the fewest regions from those obtained by a feature detector to achieve the greater robustness. The primary feature region set and the pruned feature region set are initialized as null, and the number of inspected feature regions is set as one. An iterative search is performed for determining the primary feature set. The candidate feature region sets with the cardinality equal to current values are selected from the power set with the set of detected feature regions. Each of them is satisfied with two conditions: 1) all feature regions are non-overlapped and 2) all elements of its power set are not in the pruned set. A candidate set is assigned as the new primary feature set if it increases the number of resisted attacks. A candidate set is included in the pruned feature region set while there is no more attack resisted after adding new feature regions to the set.

2.1. Pruning Algorithm

The early pruning mechanism is in preprocessing and the constraint of non-overlapping between feature regions reduce the computation time significantly because of diminishing impossible sets quickly. The procedure is stopped when all possible candidate sets are executed, or when the execution result reaches the desired number of resisted attacks. The track with pruning algorithm used in this methodology is to obtain better pruning of features from image.

2.2 Region Detection

The Harris–Laplacian Detector is used to detect the optimal feature region in an image. The selected region is not overlapped. Figure 3 shows the non overlap of feature regions selected. We have a comparison between the color image to feature region detected image. The selected regions will not get overlap and those regions are optimal regions in the given image. To extract feature regions by setting the parameters of initial scale, scale step factor between two successive levels, and the number of scale levels are used. For each test image, the detector extracts 100 feature regions according to their corner response. The watermark used is a sequence which repeats 16 times from a pseudo randomly generated 100-bit sequence. The Harris detector used the same operator for scale selection.
The functional block diagram of Harris–Laplacian Detector is illustrated in Figure 1. The original image is selected to obtain the optimal feature region. Pixels from the original image are extracted initially. Then the threshold value for the rectangle coordinates is calculated. This value used to convert the RGB to gray scale and then median filtering is done for 2D transformation. The 2D transformation is done to reduce the feature set and to get the easier segmentation of the images and to reduce the complexity of RGB image in 3D. The alpha value from the rectangle region selection is calculated. Now the non-overlapping region is selected using the laplacian algorithm. These steps give the optimal feature region in the selected image.

We took lena image an example of optimal feature region selection. Figure 2 shows the original lena
This original image is fed as sample input to get the optimal feature region selection. The output of the region selection was shown in Figure 3. The non-overlapping region was marked as round shape. The Harris affine detector relies heavily on both the Harris measure and a Gaussian scale-space representation. The Harris corner detector algorithm relies on a central principle, the image intensity will change largely in multiple directions at a corner. This can alternatively be formulated by examining the changes of intensity due to shifts in a local window. Around a corner point, the image intensity will change greatly when the window is shifted in an arbitrary direction. The Harris-Laplace detector combines the traditional 2D Harris corner detector with the idea of a Gaussian scale-space representation in order to create a scale-invariant detector. Harris-corner points are good starting points because they have been shown to have good rotational and illumination invariance in addition to identifying the interesting points of the image.

3. Existing Methodologies

The existing methodologies discussed so far have more difficulties and drawbacks. There are wide ranges of techniques described over time. The secure tamper-resistant algorithm for watermarking images and a methodology for digital watermarking that may be generalized to audio, video, and multimedia data in [2]. The watermark will be constructed as an independent and identically distributed Gaussian random vector that is invisibly inserted in a spread-spectrum into the perception of most significant spectral components of the data. The inverse mapping is computed as an inverse FFT (IFFT) in [3] followed by an inverse Fourier-Mellin transform. The resilience of watermarking to geometric attacks are easy to implement, but can make many of the existing watermarking algorithms ineffective in [4].

3.1 Tamper-resistant algorithm

This algorithm was used in [2] makes an independent and identically distributed Gaussian random vector to construct the watermark that is invisibly inserted in a spread-spectrum into the perception of most significant spectral components of the data. The watermark should not be placed in perceptually insignificant regions of the image because many common signal and geometric processes affect these components.

3.2 Inverse Fourier-Mellin transform (IFMT)

The inverse transformation in [3] from RST invariant domain to the image domain uses the phase computed during the forward transformations from image domain to the RST invariant domain. A watermark extracted with or without a cover image. The image is transformed to the RST invariant domain and the watermark is decoded.

3.3 Geometric Attacks

The watermarking scheme is to use a normalized image for both watermark embedding and detection. The normalized image is obtained from a geometric transformation procedure that is invariant to any affine distortions of the image. This will ensure the integrity of the watermark in the normalized image even when the image undergoes affine geometric attacks.
3.4 Fourier Mellin transforms (FMT)

The property of rotation and scaling invariance discussed in Fourier Mellin Transform [5] reduce the probability of error and make the feature points still detectable after distortions. The feature points that are very robust to the concerned distortions should be selected for watermarking process. The segmented image is used to detect the feature points. As it is low-pass filtered and all the high-frequency components are sensitive to many distortions, FMT has a set back in performance.

4. Proposed Methodology

The existing methodologies in [2], [3], [4], [5] and [6] have lot of disadvantages and that are all difficult to handle. In the methodologies, watermarking of digital images was intended to be attacked easily, so the attackers can easily identify the watermark in an image after decryption. Also it has lot of changes in the image quality after watermarking in previous methodologies. The image quality should be preserved to make good watermarking and that make the persistent of the image after watermarked. In the proposed methodology at the initial stage the optimal feature regions were selected and some predefined attacks were performed to evaluate the robustness of every candidate feature region.

Based on the evaluation results, the track-with-pruning procedure was used to search a minimal primary feature set which can resist the most predefined attacks. In order to enhance the resistance to undefined attacks under the constraint of preserving image quality, the primary feature set is then extended by adding into some auxiliary feature regions. This work is formulated as a multidimensional knapsack problem and solved by a genetic algorithm based approach. The experimental results for StirMark attacks [15] on some benchmark images support our expectation that the primary feature set can resist all the predefined attacks and its extension can enhance the robustness against undefined attacks like fragile attack, ambiguity attack, etc. Based on analytical comparison with some well-known feature based methods, the proposed method exhibits better performance in robust digital watermarking.

5. Conclusion

A novel method based on the simulated attacking approach and the GA-based MDKP solving procedure is proposed to select the most adequate feature regions for robust digital image watermarking under the constraint of preserving image quality. Compared with other feature-based watermarking methods, the robustness against various attacks, the proposed method is designed to perform better and the image quality after watermarking is set to be still preserved. It may be considered that our method consumes too much computation time in measuring the robustness of feature regions due to the simulated attacking. But in practice, according to the study of performances in existing methodologies, small number of candidate feature regions will be sufficient to reach full robustness.

References