“ROBUST DIGITAL IMAGE WATERMARKING WITH SELECTION OF FEATURE REGION SET”

S. R. GUNGRAD, K.D.KHARAT

Govt Engg College, Aurangabad

Abstract- A feature based region selection method and feature selection method for robust digital image watermarking is proposed in this paper. This method aims to select a non overlapping feature region set, which has the greatest robustness against various attacks and can preserve image quality as much as possible after watermarked. The goal of robust digital image watermarking preserve geometric distortion and signal processing attacks. The watermark detection task can be much simplified when it is applied to the normalized image. However, because image normalization is sensitive to image local variation, we apply image normalization to non overlapped image disks separately. The disks are centered at the extracted feature points. Several copies of a 16-bit watermark sequence are embedded in the original image to improve the robustness of watermarks. Simulation results show that our scheme can survive low-quality JPEG compression, color reduction, sharpening, Gaussian filtering, median filtering, row or column removal, shearing, rotation, local warping, cropping, and linear geometric transformations.

Index Terms - Feature extraction, Image transformation, geometric distortion, image normalization robust watermark. Feature detector, genetic algorithm, multidimensional knapsack problem (MDKP).

I. INTRODUCTION

A digital watermarking algorithm is indicated by the robustness of embedded watermarks against various attacks. Attacks which attempt to destroy or invalidate watermarks can be classified into two types, noise-like signal processing and geometric distortions. Attacks of the first type intend to remove embedded watermarks from the cover image by a signal processing approach. [2]

The second type of attack, which results in synchronization errors by geometric distortions, makes a detector fail to detect the existence of watermarks even if they are still on the image. The methods proposed to resist geometric distortions can be classified into the transform-based Feature-based DCT Based schemes.[1]-[3]

We investigate two issues of existing feature-based schemes in this paper: 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.

For the first issue, since the magnitude of pixels in a region will be modified when a watermark is inserted into this region, it is preferred to select non overlapping regions for watermarking to avoid a major degradation of image quality.[1]-[14]. In order to select a non overlapping region watermarks embedded in invariant-transform domains generally maintain synchronization under rotation, scaling, and translation [2]-[15]. Examples of these transforms are log-polar mapping of DFT (Discrete Fourier transformation).

Several applications of watermarking have been considered by researchers [2]:

Copyright: The Watermark is associated with a unique identity number. The watermark identifies the owner of the content and can be used for copyright purposes. The embedding and the detection of the watermark depend on a feature based method. The watermark has been robust and detectable after numerous processing attacks that preserve the original data in image [5]-[10].

Database Retrieval and Data Hiding: In this case, the mark permits the identification of the content. The mark contains a description of the content or a pointer to this description and can be used for database “classification.” In this application, the robustness of the mark is not decisive but the mark has to be detected after basic format conversion.

Authentication: The mark can be a fragile mark that will disappear after image manipulation. It can be used to authenticate the content and to prove that its integrity has been preserved. The function of the mark is to prove that the content has not been manipulated and consequently the robustness of the marking algorithm is not a prior achievement.

Fig.1 Block diagram for watermarking
II. EXISTING WORK

The extracted feature of image content can be used as reference points for both watermark embedding and detection. In the Harris detector and the Achard-Rouquet detector are used for feature extraction [7]-[16]. Simulation results show that this scheme is less effective for images with mainly textures.

The authors suggest retrieving feature points by the Mexican Hat wavelet scale interaction method. We propose a feature region selection method based on the idea of simulated attacking and multidimensional knapsack problem (MDKP) optimization techniques in this paper. This method can be integrated into the feature-based watermarking schemes to enhance their robustness against various types of attacks [16].

Watermark can be inserted into the image using various techniques like spread spectrum and feature based techniques. Insertion and detection of watermark using the above techniques consumes too much computation time[9]-[15].

As a result, we propose a method of inserting watermark into image using MDKP in DCT domain to reduce the computation time. The cover image is divided into blocks and an MDKP is formulated to optimize the selection of most robust blocks in the image. Watermark is inserted into the blocks by transforming them to DCT domain.

In this paper, we develop a robust watermarking scheme. This scheme combines the advantages of feature extraction and image normalization to resist image geometric distortion and to reduce watermark synchronization problem at the same time. An experiment is conducted to preliminary test the performance of the different watermarking techniques when deliberate attacks were done as an attempt to remove the watermark. The three watermarking techniques used are Least Significant Bit, DCT and DWT. The techniques were applied to embed the Hat image into the Lena image.

III. DIFFERENT TYPES OF WATERMARKS

Some of the different types of watermarks that have been developed in the past few years are listed below[7]-[16]:

2.1 Visible Watermarks
Visible watermarks are designed to be easily perceived by the viewer, and clearly identify the owner; the watermark must not detract from the image content itself, however.

Most research currently focuses on invisible watermarks, which are imperceptible under normal viewing conditions.

2.2 A Watermark May be Fragile, Semi-Fragile or Robust.
A watermark may be fragile, semi-fragile or robust fragile watermarks are designed to be distorted or "broken" under the slightest changes to the image. Semi-fragile watermarks are designed to break under all changes that exceed a user-specified threshold. [A threshold of zero would form a fragile watermark.] Robust watermarks withstand moderate to severe signal processing attacks (compression, rescaling, etc.) on an image.

2.3 Spatial watermarks
Spatial watermarks are constructed in the image spatial domain, and embedded directly into an image's pixel data. Spectral (or transform-based) watermarks are incorporated into an image's transform coefficients (DCT, Wavelet).

2.4 Images-Adaptive Watermarks
Image-adaptive watermarks are usually transform-based, and very robust. They locally adapt the strength of the watermark to the image content through perceptual models for human vision. These models originally developed for image compression.

2.5 Blind Watermarking Techniques
Blind watermarking techniques can perform verification of the mark without use of the original image. Other techniques rely on the original to detect the watermark.

IV. PROPOSED WORK

Watermark can be inserted into the image using various techniques like spread spectrum and feature based techniques. Insertion and detection of watermark using the above techniques consumes too much computation time. As a result, we propose a method of inserting watermark into image using MDKP in DCT domain to reduce the computation time. The cover image is divided into blocks and an MDKP is formulated to optimize the selection of most robust blocks in the image. Watermark is inserted into the blocks by transforming them to DCT domain. After insertion of watermark they transformed back to spatial domain. The experimental results is applied to some images the proposed method will have better robustness than existing methods.

We propose an algorithm which works in DCT domain using MDKP. The algorithm uses the DCT block. The original size of the image considered in the experiment. The image is processed into blocks; the blocks are transformed using DCT.

The existing methodology has lot of disadvantages and that are all difficult to handle. All methodology use to watermark digital images was intended to
attack easily. So the attackers can easily identify the watermark in an image after watermarked. Also there 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 was selected and perform some predefined attacks to evaluate the robustness of every candidate feature region. Based on the evaluation results the track-with-pruning procedure used to search a minimal primary feature set which can resist the most predefined attacks.

**Implementation of Work**

This work is formulated as a multidimensional knapsack problem and by using DCT.

We propose an algorithm which works in DCT domain using MDKP. The algorithm uses the DCT block size as 8×8. The original size of the image considered in the experiment is 512×512. The image is processed into blocks; the blocks are transformed using DCT.

The symbol $g_b^a$ is defined to indicate the overall resistance degree of the block $b$ against attack $a$. It is determined by

$$g_b^a = (d_{b,a1} + d_{b,a2} + \ldots \ldots + d_{b,aNa}) = \sum_{i=1}^{Na} d_{b,ai}$$

Where $d_{b,ai} \in \{0,1\}$ indicates if block $b$ can resist the $i^{th}$ predefined attack $a_i$ and $N_a$ is the total number of predefined attacks. The symbol indicates the property related to corner response of the block $b$. It is zero, if it is less than threshold is set to 1% of the maximum response value. We use binary symbol to indicate whether region belongs to the middle scale band or not. This can be formulated into an MDKP.

![Flow chart](image)

**Fig.- Flow chart**
The symbol $g_b^a$ is defined to indicate the overall resistance degree of the block $b$ against attack $a$. It is determined by

$$g_b^a = (d_{b,a1} + d_{b,a2} + \ldots + d_{b,an})$$

Insert watermark into the block, transform block back into spatial domain and move on to the next block, and write the watermarked image out to a file. Finally separate the watermark from the image using DCT block size. Compare the watermark extracted image to the file compare it with the original image.

Where $\text{block}_b \in \{0,1\}$ indicates if block $b$ can resist the $i^{th}$ predefined attack $a$, and $N_b$ is the total number of predefined attacks. The symbol indicates the property related to corner response of the block $b$. It is zero, if it is less than threshold is set to 1% of the maximum response value. We use binary symbol to indicate whether region belongs to the middle scale band or not. This can be formulated into an MDKP.

maximize

$$\sum_{p=1}^{n_s} (g_{b_1}^{p} + g_{b_2}^{p} + g_{b_3}^{p}) S_{b_1}$$

subjected to

$$\sum_{q=1}^{n} w_{k} S_{b_1} < c_k \quad k = 1, \ldots, n$$

Is defined as

$$S_{b_1} = \begin{cases} 1, & \text{if block is selected} \\ 0, & \text{otherwise} \end{cases}$$

Insert watermark into the block, transform block back into spatial domain and move on to the next block, and write the watermarked image out to a file. Finally separate the watermark from the image using DCT block size. Compare the watermark extracted image to the file compare it with the original image.

V. RESULTS

The watermark is inserted in image. After inserting watermark following attacks are applied on different image. When we see the image cannot duplicated, we can extract the watermark from the original image. The time required is less. In minimum time we can extract the watermark.

Different attack applied on images it resist these attack

<table>
<thead>
<tr>
<th>Image / Attack</th>
<th>Cameraman</th>
<th>Moon</th>
<th>Tire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salt &amp; paper</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Passion</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Rotation</td>
<td>15</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>90</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Gaussian</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

CONCLUSION

In this paper, a method based on DCT domain using MDKP solving procedure is developed to select image blocks for robust digital image watermarking under the constraint of preserving image quality. The robustness of the watermark is significantly improved and image quality after watermarking is still preserved. The development of a MDKP techniques leads to numerous perspectives.

REFERENCES


