LBP based Watermarking Scheme for Image Tamper Detection and Recovery

Priyanka B. Patil
P.G.Student
Department of Computer Engineering
Late G.N.Sapkal College of Engineering,
Anjaneri, Nasik

J.V. Shinde
Assistant Professor
Department of Computer Engineering
Late G.N.Sapkal College of Engineering,
Anjaneri, Nasik

ABSTRACT
In recent years, digital images are in use in a wide range of applications and for multiple purposes. They also play an important role in the storage and transfer of visual information, especially the secret ones. With this widespread usage of digital images, in addition to the increasing number of tools and software of digital images editing, it has become easy to manipulate and change the actual information of the image. Therefore, it has become necessary to check the authenticity and the integrity of the image by using modern and digital techniques, which contribute to analysis and understanding of the images’ content, and then make sure of their integrity.

Digital image fragile watermarking is an information hiding technique which adds the watermark into the host image for authentication. While achieving the high integrity one should not compromise with quality distortion of images. Numbers of watermarking schemes exist today for balancing between the tamper detection rate and quality of reconstructed images. In the propose scheme we aim at maintaining high tamper detection rate as well as high Peak to Signal Noise Ratio (PSNR) of reconstructed images for their quality. For that we utilize Local Binary Pattern (LBP) for this purpose to obtain the optimum solution.

In the propose scheme we used a fragile image watermarking scheme with recovery ability based on local binary pattern (LBP). The local binary pattern operator used to extract localized spatial features. A local binary pattern is used to represent the localized relations of a pixel with its neighborhood pixels. Every pixel measured by the LBP operator and obtained its own local binary pattern as representation of local spatial relations. We utilize the LBP operator to generate authentication data which are embedded into each image block with 3 × 3 pixels size for tamper detection and recovery. The recovery information is obtained by calculating the mean value of each image block, and then the mean value is converted into a binary string which is embedded into eight neighboring pixels’ LSBs of each image block for image recovering.

In the propose scheme we can take the input as 256 × 256 as well as 512×512 dimension image, one of the advantage compared to other existing system is that it can also processed the color image. The quality is calculated by the PSNR but in the proposed scheme PSNR at peak point is also calculated to get better result.

General Terms
Digital image watermarking, fragile image watermarking, local binary pattern (LBP), PSNR (peak signal to noise ratio)

Keywords
Authentication, signal, noise, information hiding, integrity

1. INTRODUCTION
The success of Internet and digital consumer devices such as mobile, laptop, tablet etc. which are used by individuals profoundly changes our daily lives and society by making the transmission, capture and storage of digital data easily and conveniently. However, this raises a big issue is how to protect these data and prevent them from unauthorized use. These concerns have become issues in many regions such as video and music industry etc. So as a solution digital watermarking is mainly used. Hence digital watermarking becomes very stunning research topic. Digital watermarking technology that detect and create invisible markings, which can be used to track down the origin, accuracy, and authorized usage of digital data. In future the major development of digital watermarking is like as: pirate tracking, image authentication, copyright protection, and hide communication. [1][3]

The meaning of robustness is in which watermark is capable to resist some changes in the watermark embedded signal. So a good algorithm should be robust. In terms of embedding field digital watermarking are classified into two category spatial domain and frequency domain watermarking. In spatial domain method watermark is embed by modifying the pixel values of novel image and transform domain process which embed the data by modulating the transform area coefficients. Semi fragile spatial domain technique is more robust than frequency domain technique.

2. RELATED WORK
Debotosh Bhattacharjee, Ayan Seal, Suranjan Ganguly, Mita Nasipuri, and Dipak Kumar Basu[1] proposed the study two local-matching techniques, one of it is wavelet and the other based on Local Binary Pattern, are analyzed. Human face images are process first and cropped the face region only, from the entire face images. After the LBP features for dimensionality reduction, are used separately for recognition of the face.

Yaoran Huo, Hongjie He and Fan Chen[3] proposed proposes a semi-fragile watermarking scheme with discriminating general tampering from collage attack, which presents a new tamper proofing providing more information on who modified the image. For each 8×8 image block, the proposed scheme has a superior performance of tamper detection and an ability of discriminating general tampering from collage attack, but not able to recover the tampered region.

Chun-Shien [6] proposed a multipurpose watermarking scheme which can be applied to achieve both authentication.
and protection of multimedia data the proposed scheme has three special features:

1) The approximation information of a host image is kept in the hiding process by utilizing masking thresholds

2) Oblivious and robust watermarking is achieved for copyright protection.

3) Fragile watermarking is achieved for detection of malicious modifications and tolerance of incidental manipulations.

Ismail Avcıbas [7] proposed the problem of steganalysis of images, and we have developed a technique for discriminating between cover-images and stego-images. This approach is based on the hypothesis that message-embedding schemes leave statistical evidence or structure in images that can be exploited for detection. Image quality metrics as the feature set. To identify good features (quality measures)

Chih-Wei Tang and Hsueh-Ming Hang [8] proposed a digital image watermarking scheme was designed to survive both geometric distortion and signal processing attacks. There are three key elements in our scheme:

1) Reliable image feature points;
2) Image normalization;
3) DFT domain bits embedding

No reference images are needed at the detector.

Darko Kirovski and Henrique S. Malvar [13] proposed present several novel mechanisms for effective encoding and detection of direct-sequence spread-spectrum watermarks in audio signals. The developed techniques aim at

I) improving detection convergence and robustness

ii) improving watermark imperceptiveness, iii) preventing desynchronization attacks, iv) alleviating estimation/removal attacks, and finally, v) establishing covert communication over a public audio channel.

Chao-Ming Wu, Yan-Shuo Shih [15] proposed A simple self-recovery fragile watermarking scheme is proposed paper. To localize tampering, the original image is partitioned into blocks of size 3*3. In this scheme, the watermark payload is composed of parity watermark section and two copies of restoration watermark section. All of the watermark sections are used for tamper detection.

3. PROPOSE SCHEME

Local Binary Pattern (LBP) is a feature which is used for classification in digital images. LBP was first elaborated in 1994. Since then it is used as a powerful feature for texture classification. Earlier LBP operator is widely used in texture classification and face recognition to measure the local contrast between pixels. Now a days it is also used to ensure the authenticity of digital image as it provide a comparatively robust watermark embedding technique for digital images. The main concept of LBP can be explained as:

3.1.1 Concept

In LBP technique, LBP operator is defined as, a local neighborhood surrounding a center pixel which is used as the threshold to define the local contrast of the surrounding pixels with respect to the center pixel. The surrounding pixels are labeled as 1 when the value of that pixel is greater than the center, or labeled as 0 when the value is smaller than the center. To obtain LBP code of the center pixel threshold values of neighboring pixels are multiplied with their corresponding weights and summing up them and watermark value is generated.

3.1.2 Watermark Embedding

In this method, three vectors are created namely gp, mp and sp. The first vector gp is used to hold the grey level values of pixels, second vector mp is used to hold the values of difference between each surrounding pixel and the center pixel, third vector sp is used to hold the binary information about each pixel based on the obtained difference between center pixel and the each surrounding pixel as 1 or 0 by comparing it with the value of center pixel.

In order to embed watermark, the XOR function is used to calculate the XOR value of the whole sp vector because has associative and commutative properties that is any circular shift of bits does not change the value of the function.

One bit of the watermark is embedded in a local region. In order to embed the watermark bit in the local region, the watermark bit and the XOR value of the region is compared if they are not same then only that bit is embedded in that local region. In this method author uses a 3*3 window to define local region. After successfully selecting the local region, the pixel whose value in the mp vector is minimum is choose to embed the watermark bit. If all the values of a local region are 0 or 1 then the value of the center pixel is modified in order to embed the watermark bit.

![Fig 1: the process of watermark pixel value generation](image-url)
3.1.3 Watermark Extraction
To extract the watermark from the image simply the XOR value of each local region is judged if the value is 0 the corresponding watermark bit is 0 or if the value is 1 the corresponding watermark bit is 1.

So the watermark embedding and the extraction phases are very simple but are robust against the post processing attacks like noise addition.

Fig 2: watermark embedding and extraction process

4. RESULT AND ANALYSIS
gray-level images with 256x256 and 512 x 512 pixels are used in experiments, which are “Airplane”, “Lena”, “Sailboat” and “Peppers” Experimental results are compared with proposed system.

1. The comparison result of PSNR of the watermarked image is shown in Table 1, between the LBP and proposed scheme that embeds the information into 2-LSBs of each pixel value. The PSNR of proposed scheme can give the better performance as compare to LBP, the test is perform on the sample image as LENA, AIRPLANE & PEPPERS

Table 1: Comparison of PSNR of LBP based system and proposes system

<table>
<thead>
<tr>
<th>Image</th>
<th>LBP used system</th>
<th>Proposed system</th>
</tr>
</thead>
<tbody>
<tr>
<td>LENA</td>
<td>42.6453</td>
<td>44.09695</td>
</tr>
<tr>
<td>AIRPLANE</td>
<td>41.2847</td>
<td>43.2156</td>
</tr>
<tr>
<td>PEPPERS</td>
<td>42.5264</td>
<td>45.4627</td>
</tr>
</tbody>
</table>

2. The comparison of tamper detection rates between the proposed scheme and LBP. The tamper detection rate of LBP scheme is over 40% .The tamper detection rate of the proposed scheme is over 90%, which means the proposed scheme can easily detect the tampering on digital images. The tamper detection rate is calculated in terms of no of detected block from the total tamper blocks

Table 2: Comparison of Tamper Detection Ratio of LBP based system and proposes system

<table>
<thead>
<tr>
<th>Image</th>
<th>LBP used system (no of tamper block/detected block)</th>
<th>Proposed system (no of tamper block/detected block)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LENA</td>
<td>3688/3872</td>
<td>3260/3218</td>
</tr>
</tbody>
</table>

3. The quality of the image is calculated on the basis of the watermark and the reconstructed image as follows:

quality of watermark image and reconstructed image in terms of MSE (mean square error), SNR (signal to noise näl to noise ratio), also one advantage that we can calculate the peak signal to noise ratio at peak point , on the basis of these parameter we can calculate the quality of image.

Table 3: calculated quality of GRAY SCALE reconstructed and Watermark image

<table>
<thead>
<tr>
<th>Image</th>
<th>Watermark image</th>
<th>Reconstructed image</th>
</tr>
</thead>
<tbody>
<tr>
<td>LENA</td>
<td>25.19</td>
<td>26.46</td>
</tr>
<tr>
<td>SNR</td>
<td>38.99</td>
<td>33.12</td>
</tr>
<tr>
<td>PSNR</td>
<td>44.11</td>
<td>34.24</td>
</tr>
<tr>
<td>PSNR at peak point</td>
<td>44.11</td>
<td>34.24</td>
</tr>
</tbody>
</table>

Table 4: calculated quality of COLOUR reconstructed and Watermark image

<table>
<thead>
<tr>
<th>Image</th>
<th>Watermark image</th>
<th>Reconstructed image</th>
</tr>
</thead>
<tbody>
<tr>
<td>LENA</td>
<td>2.53</td>
<td>2.43</td>
</tr>
<tr>
<td>SNR</td>
<td>36.96</td>
<td>37.15</td>
</tr>
<tr>
<td>PSNR</td>
<td>44.09</td>
<td>44.26</td>
</tr>
<tr>
<td>PSNR at peak point</td>
<td>44.02</td>
<td>44.19</td>
</tr>
</tbody>
</table>
In this section the "LENA" , "AIRPLANE", "SAIBOAT" are used for experiments images of (Table 2) as explain The tamper detection rate of LBP scheme is over 40% and proposed scheme is over 90%, which means the proposed scheme is better and easily detect the tampering on digital images. In (Table 3 & 4) describes the quality of reconstructed image is better as compare to watermark image so the result of all image is as shown.

5. CONCLUSION
In this result paper of watermarking techniques is describe as a new development in the digital image watermarking for 256×256 extends to 512×512 in which the watermarking techniques is analyzed with the help algorithm LBP(local binary operate) and it will be better than existing system also in the propose scheme we can apply the watermarking on color image for tamper detection and recovery the quality of the image is calculated in terms of MSE,SNR,PSNR,PSNR at peak point also the tamper detection ratio is also calculated.

6. REFERENCES
[6]. Chun-Shien Lu, Hong-Yuan Mark Liao, “Multipurpose Watermarking for Image Authentication”


