Subjective and Objective Watermark Detection using a Novel Approach – Bar-code Watermarking

Vidyasagar Potdar, Song Han, Elizabeth Chang, Chen Wu
Digital Ecosystems and Business Intelligence Institute, Curtin University of Technology, Perth, Western Australia
Vidyasagar.Potdar@cbs.curtin.edu.au, Song.Han@cbs.curtin.edu.au

Abstract

Many digital watermarking algorithms are proposed in the literature. Broadly these watermarking algorithms can be classified into two main categories. The first category of algorithms uses a pseudo random Gaussian sequence (PRGS) watermark whereas the second category of algorithms uses a binary logo as a watermark. The main advantage of PRGS based watermarking scheme is its ability to detect the presence of watermark without manual intervention. However the main drawback is calculating reliable threshold value. In the similar manner the main advantage of binary logo watermark is that there is no need to calculate threshold value but requires manual intervention to detect the presence of watermark. The advantage and disadvantage of either approach is quite clear hence it would be a good idea to design a watermarking scheme which inherits the advantages from both these approaches. In this paper we present one such approach which is termed as bar-code watermarking. The proposed scheme offers objective as well as subjective detection. A PRGS sequence watermark is represented as a bar-code on a binary logo and embedded in the host image. Watermark detection can be either done subjectively or objectively.

1. Introduction

The adoption of Internet in day to day has resulted in exchange of copyrighted material over peer-to-peer (P2P) networks which results in copyright infringements. Digital watermarking schemes are developed to detect copyright infringements.

Broadly these watermarking algorithms can be classified into two main categories. The first category of algorithms uses a pseudo random gaussian sequence (PRGS) watermark where the presence of the embedded watermark is detected by using statistical correlation whereas the second category of algorithms use a binary logo as a watermark and this logo is extracted to detect the presence of watermark.

The former approach is more objective because it relies on a statistical correlation value to ascertain the presence of watermark however the latter approach is more subjective because the presence of watermark is detected by visual inspection by a third entity. In the former approach the original watermark is required to detect the presence of the extracted watermark because correlation is calculated by comparing the original watermark with the extracted watermark. However with the latter approach the original watermark is not required because the extracted watermark which is normally a logo is visually recognizable. There is no need to compare it with the original embedded logo. The mere fact that the logo is visible is enough to prove the presence of watermark.

Table 1. PRGS vs. Binary Logo Watermarks

<table>
<thead>
<tr>
<th>PRGS</th>
<th>Binary Logo Watermark</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advantages</strong></td>
<td><strong>Disadvantages</strong></td>
</tr>
<tr>
<td>Automatic Watermark Detection</td>
<td>Threshold Calculation</td>
</tr>
<tr>
<td>Use of original watermark for detection</td>
<td>No need of using original watermark for detection</td>
</tr>
</tbody>
</table>

The advantages and drawbacks of either approaches is described in Table 1. The paper is organized as follows. In Section 2, we discuss some existing watermarking schemes (based on wavelet) which embed binary watermarks. We specifically discuss some quantization based algorithms. A detailed discussion and critical analysis is provided for the
existing schemes. In Section 3, we describe the proposed watermarking scheme. We first outline the procedure of watermark generation followed by watermark embedding and extraction algorithm. In Section 4, we discuss the experimental setting where we specify the attacks and its intensity which would be used to test the robustness of the proposed watermarking scheme. In Section 5, results obtained after each attack are described in detail and a conclusion is drawn as to how our algorithm resists these attacks. Section 6 concludes the paper.

2. Existing Work

In this section we discuss some wavelet based watermarking algorithms. We classify these algorithms based on their decoder requirements as blind detection or non-blind detection. Most of the watermarking schemes surveyed in this section use a binary logo as a watermark. The size of the watermark is smaller compared to the host image.

In [3], Hsu and Wu present a wavelet based watermarking scheme which embeds a binary logo as a watermark. The watermark is embedded in the mid frequency components of the wavelet sub-bands. This scheme is resistant to common image processing attacks only. Its robustness against geometric distortions is not discussed. The main drawback of this algorithm is its non-blind nature i.e. the original image is required for detecting the presence of watermark.

Lu et al. [4] present a robust watermarking scheme based on image fusion. The algorithm is a non-blind watermarking algorithm which embeds grey-scale image and binary image as watermarks. The watermark strength is modulated based on Just Noticeable Distortion (JND) threshold. All the coefficients in the LL, HL, LH, and HH sub-band at all the four levels are used to embed the watermark. The algorithm is shown to be robust against the following attacks: Blurring, Median Filtering, Re-scaling, JPEG compression, EZW compression, Jitter Attacks, Collusion Attacks, Rotation, Stimark Attacks, unZign Attack, a combination of above attacks were tested. However the main issue with this algorithm is its non-blind nature which limits its application.

Raval and Rege [5] present a non-blind watermarking scheme where two binary watermarks are embedded in LL2 and HH2 sub-band. All the coefficients in the LL2 and HH2 subband are used. After performing a two level decomposition of the host image (I), the binary watermark is embedded in the LL2 and HH2 subband by additive embedding. It has been shown that watermarks embedded in LL2 subbands are robust to one set of attacks (filtering, lossy compression, geometric distortions) while those embedded in HH2 subbands are robust to another set of attacks (histogram equalization, gamma correction, contrast and brightness adjustment and cropping). However the use of uniform scaling parameter results in some visible artifacts. It should have been a good idea to consider variable scaling factors for different sub-bands.

Tao and Eskicioglu [6] conduct a comparative study to find out the effects of embedding watermarks in the first and second level decomposition. The authors suggest that embedding in the first level is advantageous because it offers more coefficients for modification and the extracted watermarks are more textured and have better subjective visual quality. The technique uses variable scaling parameters for different subbands at different decomposition levels. Their main observations are LL1 and LL2 bands are robust against JPEG compression, Blurring, Gaussian Noise, Scaling, Cropping, Pixilation and Sharpening. HH1 and HH2 bands are robust against Histogram Equalization, Intensity Adjustment, and Gamma Correction. HL1, HL2 and LH1, LH2 also show similar robustness. As with the other techniques the main issue with this algorithm is the non-blind nature, original image is required for extracting the watermarks.

Ganic and Eskicioglu [7] inspired by Raval and Rege [5] propose another watermarking scheme based on DWT and Singular Value Decomposition (SVD). They argue that the watermark embedded by using [5] scheme is visible in some parts of the image especially in the low frequency areas, which reduces the commercial value of the image. Hence they generalize their technique by using all the four sub-bands and embedding the watermark in SVD domain.

All the algorithms discussed so far require the original image for detecting the presence of watermark which is a major drawback and is not feasible in all scenarios. Hence we now discuss some blind watermarking algorithms which embed an image logo as a watermark.

In [1] Tsai et al. improve the scheme proposed in [3] by presenting a scalar quantization based blind watermarking scheme which embeds a binary logo as a watermark and the offer blind detection. They embed the watermark in the middle and low frequency components of the wavelet sub-bands i.e. all sub-bands except LL subband. All the selected coefficients are quantized by a constant factor which is a main issue with this algorithm because certain high texture rich regions within an image can tolerate large modifications (quantization step sizes) because of their inherent high texture masking capacity and hence can be strongly watermarked. At the same time smooth regions have a comparatively lower masking capacity.
and hence should be quantized using smaller step sizes. This algorithm shows robustness against JPEG compression only. Its robustness against geometric attacks and other image processing attacks is not discussed.

In [8] Barni et al. present wavelet based watermarking scheme which incorporates HVS to modulate the strength of the watermark according to the local characteristics. The watermark is not a binary logo but it is a binary PRGS. The watermark is embedded in HHl, HLl and LHl subbands. This scheme is robust against JPEG compression, cropping and morphing.

In [9] Meerwald present a quantization based watermarking scheme in the JPEG2000 coding pipeline. The watermarks are embedded in all the subbands prior to the entropy coding stage. The scheme is only robust against a small set of attacks like JPEG, JPEG2000, Blur and Sharpening.

In [2] Chen et al. present another quantization based watermarking scheme which improves on the algorithm proposed in [1] by incorporating variable quantization based on HVS similar to [8]. They embed the watermark in the approximate subband of the fourth level wavelet decomposition i.e. the LL4.

Based on the survey we identified the following issues with the existing watermarking schemes are:
1. Do not offer subjective and objective detection simultaneously in one watermarking scheme.
2. Binary logo watermarking schemes do not offer objective detection.
3. Existing solutions do not provide an alternative detection mechanism in case the objective detection fails or is considered incorrect.

In order to address these issues we proposed a new watermarking scheme termed as bar-code watermarking. The basic idea behind bar-code watermarking is to represent the PRGS watermark in a binary logo and make it machine readable. The machine readability is achieved by representing the PRGS watermark as a bar-code. For example 1010101010101010 can be represented as

<table>
<thead>
<tr>
<th>PRGS watermark (W)</th>
<th>Bar-coded representation of PRGS watermark</th>
<th>Complete Bar-coded Binary Logo Watermark (Wb)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1010101010101010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1010101010101010</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1010101010101010</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.2 Watermark Embedding

Inputs: Original Image (I), BBLW (Wb), Secret Keys (K)
Output: Watermarked Image (Iw)

The detail approach is described as follows:

Step 1. Generate the BBLW using steps described in section 3.

Step 2. Permute the BBLW using the permutation function f(.) and permutation key (P) to increase the security of the watermark - WbP.

Step 3. The BBLW can be embedded in an image by using any binary logo embedding algorithm. In this paper we used the robust logo embedding algorithm presented by the authors in [10] to embed the binary
The detailed algorithm is discussed in the Appendix A. The basic sub steps are:

1. Decompose the original image $I$ by one level wavelet transform to obtain LL$_1$, LH$_1$, HL$_1$ and HH$_1$ subbands using Haar Wavelet Filter.

2. For each sub-band except the LH$_1$ sub-band, starting at the top left corner divide the wavelet coefficients into non-overlapping blocks of 8x8 and calculate the mean intensity values of each block.

3. Construct the quantization table $T$.

4. Quantifying all the blocks in LH$_1$, HL$_1$ and HH$_1$ using HVS threshold to represent the BBLW $W_b$.

5. Apply inverse wavelet transform to embed the watermark logo.

**Step 4.** The output is the watermarked image $I_w$.

### 3.3 Watermark Extraction and Detection

**Inputs:** Watermarked Image ($I_w$), Secret Keys ($K$)

**Output:** BBLW ($W_b$)

The detail approach is described as follows:

**Step 1.** Load the watermarked image $I_w$.

**Step 2.** Using the extraction algorithm proposed in [10] extract the BBLW. The sub steps are:

1. The watermarked image $I_w$ is decomposed by one level wavelet transform to obtain LL$_1$, LH$_1$, HL$_1$ and HH$_1$.

2. For each sub-band except the LL sub-band, starting at the top left corner we divide the sub-band into non-overlapping blocks of 8x8 and calculate the mean intensity values of the wavelet coefficients.

3. Compare these values with the quantization table $T$ to generate the BBLW.

4. Inverse permute the BBLW ($W_b^p$) to recover the original BBLW ($W_b$).

**Step 3.** The BBLW is now parsed to recover the PRGS. The sub steps are:

1. Consider the first block of pixel (8x4) beginning from 1st row and 1st column.

2. Calculate the number of black pixels and white pixels with in that block.

3. If the black pixels are more than a specific threshold ($T_b$)
   
   The block under consideration represents 1
   
   Proceed to the next block

4. Else if the white pixels are more than a specific threshold ($T_b$)
   
   The block under consideration represents 0
   
   Proceed to the next block

**Step 4.** Compare it with the original PRGS and calculate correlation coefficient to detect the presence of the watermark.

*If the correlation is weak or the watermark cannot be detected then*

The extracted logo can be visually inspected.

### 4. Experimental Setting

In the experiments that we conducted we used the four original images as shown in Table 3. The size of the original image is 1024x1024 pixel grey scale image whereas the size of the watermark logo is 64x64 pixels. We used Haar Wavelet filter to decompose the image in the wavelet domain.

**Table 3. Original Images used for watermarking**

<table>
<thead>
<tr>
<th>Lena</th>
<th>Baboon</th>
<th>F-16</th>
<th>Pepper</th>
</tr>
</thead>
</table>

The watermark logo $W_b$ and the permuted watermark $W_b^p$ that is used in the experiments is shown in Table 4. The watermarked image is as shown in Table 5. There are no visible artifacts because the wavelet coefficients are quantized under the HVS constraints; secondly the wavelet coefficients belong to the detailed subbands (LH$_1$, HL$_1$ and HH$_1$) and quantizing those results in the implicit perceptual masking.

**Table 4. Watermarks used in Experiments**

<table>
<thead>
<tr>
<th>Bar-Code Watermark</th>
<th>Permuted Watermark</th>
</tr>
</thead>
</table>

The entire watermark information is hidden along the edges and corners. The proposed algorithm is shown to be robust against fifteen major attacks including watermark removal and synchronization removal attacks. Although distortions exist the watermark is still visually recognizable (subjective detection) and statistically detected (PSNR values).

**Table 5. Watermarked Images**

<table>
<thead>
<tr>
<th>Lena</th>
<th>Baboon</th>
<th>F-16</th>
<th>Pepper</th>
</tr>
</thead>
</table>
We attacked the watermarked image with the following attacks; the details of the attacks are listed in Table 6.

Table 6. List of Attack applied on watermarked images

<table>
<thead>
<tr>
<th>Attack Name</th>
<th>Attack Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gamma Correction</td>
<td>Increase gamma level of image by 110, 120, 130, 140, 150%</td>
</tr>
<tr>
<td>JPEG</td>
<td>Perform JPEG compression on image QF 90, 80, 70, 60, and 50</td>
</tr>
<tr>
<td>JPEG 2000</td>
<td>Perform JPEG 2000 compression QF 90, 80, 70, 60, and 50</td>
</tr>
<tr>
<td>Contrast</td>
<td>Increase contrast of image by 15, 32, 52, 74, 100%</td>
</tr>
<tr>
<td>Salt &amp; Pepper</td>
<td>Apply a salt &amp; pepper filter to image. Noise density 0.001, 0.002, 0.003, 0.004 and 0.005</td>
</tr>
<tr>
<td>Row Column Blanking</td>
<td>Blank rows and columns in image. Blank 5, 10, 20, 30 and 40 rows and columns</td>
</tr>
<tr>
<td>Row-Column Copying</td>
<td>Copy rows and columns in image to the adjacent row or column. Blank 5, 10, 20, 30 and 40 rows and columns</td>
</tr>
<tr>
<td>Cropping</td>
<td>Crop image smaller by four block sizes, five times successively.</td>
</tr>
<tr>
<td>Rotate 90, 180</td>
<td>Rotate the image by 90 or 180 degrees clockwise.</td>
</tr>
</tbody>
</table>

5. Experimental Results

In this section we discuss the experimental results that we gathered by running our prototype. We used watermark shown in Table 4 to embed in four images. The extracted watermarks are shown in the following Table 7

Table 7. Watermarks extracted after attacks

<table>
<thead>
<tr>
<th>Lena</th>
<th>Baboon</th>
<th>F-16</th>
<th>Pepper</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Lena watermarked image" /></td>
<td><img src="image2.png" alt="Baboon watermarked image" /></td>
<td><img src="image3.png" alt="F-16 watermarked image" /></td>
<td><img src="image4.png" alt="Pepper watermarked image" /></td>
</tr>
<tr>
<td><img src="image5.png" alt="Gamma Correction" /></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6. Conclusion

In this paper, we present a bar-code watermarking approach which can offer objective as well as subjective detection. The PRGS sequence watermark is represented as a bar-code on a binary logo. This bar-code binary logo is then embedded in the host image which is to be watermarked. The proposed approach serves two main purposes firstly it could be used for objective watermark detection using correlation and
secondly it could also be used for subjective detection (visual inspection) in case the objective detection fails.

6. References


Appendix A

IMPORT: Image: image of attacked barcode
reference: image of unattacked barcode

EXPORT: Readable: boolean indicating whether barcode is readable

METHOD: Boolean checkBarcode( image, reference)

Variables in terms of average white pixels in each bar of a perfect barcode

maxBlack = 0 % (will hold the highest average of all the bars that are supposed to be black)
minWhite = 1 % (will hold the lowest average of all the bars that are supposed to be white)
maxX = 0.5 % (will hold the highest average of all the bars that are supposed to be X)
minX = 0.5 % (will hold the lowest average of all the bars that are supposed to be X)

for each row in image
for each bar in row
average = average of current bar in image
if reference bar is:
: black
  if average > maxBlack
    then maxBlack = average
  end if
 : white
  if average < minWhite
    then minWhite = average
  end if
 : X
  if average > maxX
    then maxX = average
  end if
  if average < minX
    then minX = average
  end if
end if
end for
end for

if maxBlack >= minX OR minWhite <= maxX
then readable = false
else readable = true
return readable

% (if the barcode is readable, the appropriate threshold values for black bars and white bars can be found in between maxBlack and minX, and maxX and minWhite respectively)