Chapter 5

Offline Handwritten Signature Based Watermarking Techniques

5.1 Introduction

This chapter discusses watermarking techniques which use offline handwritten signature as a watermark for indication of legitimate ownership. In fact, the employment of handwritten signature has the intrinsic advantage that it is a legal biometric attribute that has been conventionally used to certify and validate official transactions. Following two techniques are developed and presented in this chapter.

I) Offline handwritten signature based watermarking technique using correlation approach

II) Offline handwritten signature based watermarking technique using Shift Invariant Feature Transform (SIFT)

The signature data considered here for experimentation is taken from [97]. The sizes of the signature images vary from $60 \times 30$ to $120 \times 120$ and are in .png format. Samples of the few signature images are shown in Figure 5.1. The quantitative metrics used for evaluation of watermarked image and extracted watermark are PSNR and Structural Similarity Index Measure (SSIM) [98]. (Refer Appendix A)
5.2 Offline Handwritten Signature Based Watermarking Technique Using Correlation Approach

In this proposed scheme offline signature of owner is embedded as a watermark in second level detailed coefficients of discrete wavelet transform of cover object. The cover image is decomposed using biorthogonal wavelet transform. The biorthogonal wavelet transforms are invertible transforms with the properties of perfect reconstruction and symmetric wavelet functions. The biorthogonal wavelets acquire those properties as they possess two sets of low-pass filters (for reconstruction), and high-pass filters (for decomposition). Each set is the dual of the other. On the contrary, the orthogonal wavelet comprises of only one set. This subclass of wavelets permits perfect reconstruction by symmetric extension across boundaries, avoiding the coefficient expansion and border discontinuity introduced by using circular convolution together with periodic extension. Biorthogonal wavelets give higher embedding capacity compared with orthogonal wavelets [37, 38, 99]. The aforementioned characteristics make them potential candidate in the wavelet domain for watermarking.
5.2.1 Watermark Preparation

The offline handwritten signature of the owner which is used as a watermark is converted to a 1-D binary string having values 0 and 1 only. This is essential as watermarking will be done based on these two values only. It is denoted as $W_{sgn}$.

5.2.2 Watermark Embedding

A well known technique for watermark embedding is based on correlation approach [100, 101]. A pseudo-random sequence (PN) is added to the cover image $I(x, y)$ using additive multiplicative equation. To retrieve the watermark, the same pseudo-random generator algorithm is seeded with the same key, and the correlation between the PN sequence and possibly watermarked image is computed. If the correlation exceeds a certain threshold $T$, the watermark is detected. This basic approach is used simply for watermark detection only. Correlation based approach is modified for watermark extraction for multiple bits watermark. To effectively differentiate between signature watermark bit '0' and '1', whenever the signature watermark bit is zero, this pseudo-random sequence is inserted into the horizontal detailed wavelet coefficients else the wavelet coefficients are left untouched. The pseudo-random sequence thus generated during each pass is used to update the detailed coefficients. Embedding the watermark in more than one band ($HL_2$ and $LH_2$) at a time and all three detail subbands is also carried out to study effect on robustness and fidelity. Watermark embedding algorithm is as follow:

1) Apply second level wavelet decomposition on host image using biorthogonal wavelet transform.

2) Using the secret key initialize the random function generator to some fixed state.

3) For the entire length of signature watermark repeat the steps 4 to 5.

4) Generate PN sequences having values in the range of -1 to 1 and of the same dimension of the detail subband. Number of PN sequence generated will be equal to number of bands used for embedding. For embedding in $HL_2$ band only, one PN sequence is generated, for embedding in $HL_2$ and $LH_2$ bands, two PN sequences are generated while for embedding in all the three detail bands, three PN sequences are generated. Those are called as PN1, PN2 and PN3 respectively.
5) If signature watermark bit is zero update the coefficients of $LH_2$ band using Equation 5.1. When it is one, coefficients are left unaltered.

$$\hat{I}_{LH2} = I_{LH2} + \alpha PN1$$

(5.1)

If watermark has to be embedded in both horizontal and vertical bands then modify the coefficients of $HL_2$ band using Equation 5.2

$$\hat{I}_{HL2} = I_{HL2} + \alpha PN2$$

(5.2)

If watermark has to be embedded in all three detail bands then modify the coefficients of $HH_2$ band using Equation 5.3

$$\hat{I}_{HH2} = I_{HH2} + \alpha PN2$$

(5.3)

$\alpha$ is the strength of watermark and is set in the range of 0.5 to 0.7 to strike a balance between robustness and fidelity.

6) Generate the watermarked image $I^w$ by applying the inverse wavelet transform.

### 5.2.3 Watermark Extraction

For watermark extraction process only secret key and length of watermark is required. Secret key is shared between embedder and receiver and is used to regenerate pseudorandom sequence. Watermark extraction algorithm is as follow:

1) Using the secret key initialize the random function generator to some fixed state.

2) Generate another sequence $W_{\text{sgn}}^*$ consisting of only 1’s equal to the length of the original watermark. This sequence is further used to generate/reconstruct the signature watermark.

3) Apply second level wavelet decomposition on host image using biorthogonal wavelet transform.

4) For the entire length of signature watermark repeat the steps 5 to 6.
5) Generate pseudorandom sequences having values in the range of -1 to 1 and of the same dimension of the detail subband. Number of PN sequence generated will be equal to number of bands used for embedding and are denoted as PN1, PN2 and PN3 respectively.

6) For pseudorandom sequence generated during each pass, find the correlation between this sequence and the $LH_2$ subband and save it one dimensional vector which is equal to length of watermark.

$$correlation_{LH}(i) = Corr(I_{LH_2}, PN1)$$ (5.4)

If watermark is embedded in both bands then

$$correlation_{HL}(i) = Corr(I_{HL_2}, PN2)$$ (5.5)

If watermark is embedded in all three bands then

$$correlation_{HH}(i) = Corr(I_{HH_2}, PN3)$$ (5.6)

where Corr() is function to find the correlation between subbands and PN sequences. When the watermark is embedded in multiple bands, then finally find the average of correlation sequences.

7) Find the standard deviation of correlation sequence. This standard deviation is used as a as a threshold value.

8) Compare each value of correlation sequence found out in step 6 with threshold value. If it is greater than threshold value, then set corresponding bit of $W_{sgn}$ to zero, otherwise leave that particular bit unchanged.

9) The original signature image is reconstructed by reshaping the sequence $W_{sgn}^*$ thus obtained from step 8.
5.2.4 Authentication through Template Matching

This technique goes a step further wherein it extracts the features of recovered signatures and does the template matching with features of signature data base. Feature extraction process of signature database and recovered signature is carried out through Hough transform [102, 103] and Principal Component Analysis (PCA). The signature pattern thus reconstructed is authenticated using template matching. Using the Euclidean distance as a measure, the features of recovered signature are matched with the features of signature from the database. The signature with minimum Euclidean distance is the recognized signature which was embedded as a watermark. This stage can be an optional stage.

5.2.5 Experimentation and Results

5.2.5.1 Data payload

In this algorithm data payload is a pseudorandom sequence which is added to host image depending upon the bit of signature bit stream. Size of signature bit stream depends upon the size of the signature image, which varies between $60 \times 30$ to $120 \times 120$.

5.2.5.2 Strength of watermark

It is varied between 0.5 to 0.7. If it is increased beyond this range, perceptual quality of watermarked image is degraded.

5.2.5.3 Results

Figure 5.2 shows sample outputs of watermarked gray scale image and extracted watermark with various signature watermark. Extreme right bottom side signature shows the template matched signature image.

Figure 5.3 shows sample outputs of watermarked color image and extracted watermark with various signature watermark. Extreme right bottom side signature shows the template matched signature image.
Figure 5.2: continued
Figure 5.2: continued
Figure 5.2: Results of correlation based technique for different signature watermarks for Gray scale image
Figure 5.3: continued
Figure 5.3: continued
Figure 5.3: Results of correlation based technique for different signature watermarks for color images
This technique is tested with different parameters such as by varying level of decomposition for watermark, number of bands involved in watermark embedding etc.

5.2.5.4 Effect of level of decomposition

By varying the wavelet decomposition levels of host image for watermark embedding, subjective and objective analysis of watermarked image and extracted watermark is done. Table 5.1 shows PSNR and SSIM of extracted signature watermark when watermark embedding is carried out in LH band of first level and second level decomposition for a sample signature. Figure 5.4 shows the sample of output of extracted signature from first level and second level decomposition.

Table 5.1: Effect of decomposition level

<table>
<thead>
<tr>
<th>Images</th>
<th>level1</th>
<th></th>
<th>level2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSNR in dB</td>
<td>SSIM</td>
<td>PSNR in dB</td>
<td>SSIM</td>
</tr>
<tr>
<td>Lena</td>
<td>33.24</td>
<td>88.14</td>
<td>37.04</td>
<td>60.18</td>
</tr>
<tr>
<td>pepper</td>
<td>33.21</td>
<td>88.13</td>
<td>39.22</td>
<td>61.45</td>
</tr>
<tr>
<td>Boat</td>
<td>33.21</td>
<td>88.46</td>
<td>39.22</td>
<td>57.23</td>
</tr>
<tr>
<td>Goldhill</td>
<td>33.21</td>
<td>87.96</td>
<td>39.22</td>
<td>63.29</td>
</tr>
<tr>
<td>Hat</td>
<td>33.2</td>
<td>81.22</td>
<td>39.02</td>
<td>38.61</td>
</tr>
<tr>
<td>Matherann</td>
<td>33.21</td>
<td>85.65</td>
<td>39.22</td>
<td>46.56</td>
</tr>
</tbody>
</table>

(a) Original and watermarked image with original and extracted watermark from second level of decomposition

Figure 5.4: continued
5.2.5.5 Effect of multiple frequency bands for watermark embedding

Experimentation is done to embed the watermark redundantly in more than one band in order to study the robustness against attacks. PSNR of watermarked image and SSIM of extracted watermark after embedding in multiple frequency band are shown Figure 5.5 for different test images. Figure 5.6 shows the output of extracted watermark for one test image when watermark is extracted from (i) horizontal band alone (ii) horizontal and vertical band and (iii) from all three detail subbands.

Figure 5.5: PSNR of watermarked image and SSIM of extracted watermark when watermark is embedded in multiple frequency band
Figure 5.6: Figures showing quality of extracted watermark when it is embedded into multiple frequency bands
5.2.5.6 Effect of varying the strength

Table 5.2 shows the effect of changing the strength of watermark on both the PSNR of the watermarked image, and SSIM between the original and extracted watermark.

Table 5.2: Effect of varying watermark strength

<table>
<thead>
<tr>
<th>Embedding band</th>
<th>Watermark Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.3</td>
</tr>
<tr>
<td>HL band</td>
<td>PSNR</td>
</tr>
<tr>
<td></td>
<td>SSIM</td>
</tr>
<tr>
<td>HL and LH band</td>
<td>PSNR</td>
</tr>
<tr>
<td></td>
<td>SSIM</td>
</tr>
<tr>
<td>All three detail bands</td>
<td>PSNR</td>
</tr>
<tr>
<td></td>
<td>SSIM</td>
</tr>
</tbody>
</table>

5.2.5.7 Robustness against attacks

Watermarking algorithm is tested against different attacks for robustness for all three bands. The sample of output results are shown Figure 5.7. Table 5.3 shows the average SSIM of extracted watermark under different attacks.

(a) Histogram attack

Figure 5.7: continued
Figure 5.7: continued

(b) Salt and Pepper noise

(c) Gaussian noise

(d) Median filtering
(e) Wiener filtering

(f) Unsharpening

(g) Row Column Copy

Figure 5.7: continued
(h) Row Column Blanking

(i) Cropping

(j) scale down

Figure 5.7: continued
Figure 5.7: Results of correlation based technique under different attacks

Table 5.3: Average SSIM of extracted watermark under different attacks for correlation based technique

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Parameters</th>
<th>SSIM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>HL band</td>
</tr>
<tr>
<td>Histogram Equalization</td>
<td></td>
<td>63.18</td>
</tr>
<tr>
<td>Salt and pepper noise</td>
<td>0.02 to 0.2</td>
<td>47.76</td>
</tr>
<tr>
<td>Gaussian noise</td>
<td>1%</td>
<td>43.95</td>
</tr>
<tr>
<td>Wiener filtering</td>
<td>3x3 window</td>
<td>33.23</td>
</tr>
<tr>
<td>Median filtering</td>
<td>3x3 window</td>
<td>37.44</td>
</tr>
<tr>
<td>Unsharpening</td>
<td></td>
<td>83.75</td>
</tr>
<tr>
<td>JPEG Compression</td>
<td>Q=50</td>
<td>61.33</td>
</tr>
<tr>
<td>Row column blank</td>
<td>Cols=50,99,192,300</td>
<td>58.3</td>
</tr>
<tr>
<td></td>
<td>Rows = 14, 169, 119, 320</td>
<td></td>
</tr>
<tr>
<td>Row column copy</td>
<td>Cols = 211-123, 256-11, 455-169,</td>
<td>59.49</td>
</tr>
<tr>
<td></td>
<td>359-50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rows = 123-211, 11-256, 169-455,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>359-50</td>
<td></td>
</tr>
<tr>
<td>Scaling</td>
<td>2</td>
<td>33.2</td>
</tr>
<tr>
<td>Cropping</td>
<td>10%</td>
<td>55.28</td>
</tr>
</tbody>
</table>
5.2.6 Observations

The technique employed has many factors that affect perceptual quality of watermarked image and the extracted watermark.

- When watermark is embedded in first level decomposition, the coefficients are significant. Therefore, image gets more distorted and PSNR value of watermarked image is smaller compared to the case when watermark is embedded in second level of decomposition. The average PSNR of watermarked image when signature is embedded in first and second level of LH band is 33 dB and 38 dB respectively.

- The level of decomposition not only affects the quality of the watermarked image, but also affects the extracted watermark. SSIM factor is on higher side when watermark is embedded in the first level of wavelet decomposition. The average SSIM of extracted watermark for first and second level is 86.59 and 54.55 respectively.

- There is significant improvement in SSIM, when signature is embedded only in second level decomposition of LH band and in multiple frequency bands LH and HL or all three detail bands. When recovering the signature from multiple bands, average of correlation sequences is taken for decision. It gives appreciable improvement in performance parameters and also shows strong robustness against different attacks. The average SSIM of extracted watermark corresponding to embedding in only LH band, LH and HL and all three detail band is 54.53, 68.16 and 77.29 respectively. However PSNR drops down when signature is embedded in more than one band.

- The watermark strength has an important influence on both the marked image and the extracted watermark. As the strength increases, the PSNR decreases. This is because the payload is multiplied by the strength before embedding. Due to this, cover image is more distorted. On the other hand, increasing the strength increases the robustness of the method, meaning that the correlation between the extracted and the original watermark is almost near or equals to 1. Tradeoff has to be achieved among these two factors.

- Robustness against signal processing attacks
  - The proposed algorithm is fragile to intensity adjustment attack.
Watermark is not robust against Wiener and Median filtering when it is embedded in only HL band

The technique survives JPEG compression attack for Q.F up to 50, when watermark is embedded in all three bands.

• Robustness against geometric attacks
  – Algorithm is fragile to rotation attack.
  – It survives scaling attack for scale of 0.5 to 2 only when watermark is inserted into two (HL and LH) or three bands (HL, LH and HH)

• This method moves a step ahead, it extracts the feature of recovered signature and does the template matching with the signature database. This feature can be used for the authentication. Template matching fails when SSIM of extracted signature falls below 35%.

• For color image watermarking, RGB planes are preferred rather than luminance chrominance scheme. Watermark is embedded into the Blue channel as changes in Blue channel are less visible. PSNR of color image is more compared to that of the gray scale image.
5.3 Offline Handwritten Signature Based Watermarking Technique Using Shift Invariant Feature Transform

The development of this algorithm aims at designing a watermarking scheme which is robust against geometric attacks. Robustness to geometric distortion remains one of the most difficult areas of watermarking research. Geometric variation of watermarked media can induce synchronization errors between the extracted watermark and the original watermark during the detection process. It is very difficult to cope up with geometric distortions especially for robust watermarking systems since these attacks break the synchronization between the watermark and detector [104]. Several approaches have been developed for survival against geometric attacks, which can be divided into following categories.

- Use of periodic sequence to embed the watermark in a repetitive pattern, allowing the detector to estimate the performed attack due to altered periodicities.

- Use of invariant-transform to maintain synchronization under rotation, scaling, and translation is the second approach. Examples of these transforms are log-polar mapping of DFT [105] and Fractal transform coefficients [106], Fourier-Mellin transform, Radon transform, Mexican Hat wavelet transform etc. Though these schemes are theoretically effective, they are difficult to implement due to poor interpolation accuracy during log-polar and inverse log-polar mapping.

- Template based approach embeds reference template to assist watermark synchronization during the detection process [107]. The template should be invisible and have low interference with the previously embedded watermarks.

- Moments based watermarking schemes make use of magnitudes of Zernike moments as they are rotation invariant. Magnitudes of moments can be used as a watermark signal or be further modified to carry embedded data [108].

- Content based scheme is another solution for watermark synchronization. Media contents represent an invariant reference for geometric distortions so that referring to content can solve the problem of watermark synchronization, i.e., the location of the watermark is not related to image coordinates, but to image semantics [109].
Content based approach for synchronization is the most challenging approach among all. In this algorithm an attempt has been made to make the algorithm robust against geometric distortions like spatial scaling and rotation using content based approach for synchronization. This type of synchronization is called implicit synchronization because the synchronization pattern is implied by the underlying media itself. In the proposed method Shift Invariant Feature Transform (SIFT) is used for synchronization purpose. SIFT is used to extract the feature points by considering local image properties and it is invariant to rotation, scaling, translation and partial illumination changes [110]. Feature points, which are also called as keypoints are localized elements of a cover image that are inherently linked to that image and usually contain semantic information. They have the property of being reasonably stable and are more difficult to remove by a malicious attacker. Feature points can be used either for watermark embedding/detection or for synchronization. Our approach uses SIFT feature points for synchronization. Before watermark detection, feature points of watermarked image are calculated and compared with the feature points of original image to estimate the geometric distortion. This distortion is inverted and then watermark detection process is carried out.

5.3.1 Watermark Preparation

The offline handwritten signature of the owner which is used for authentication purpose is converted to a 1-D binary string having values 0 and 1 only. This is essential as watermarking will be done based on these two values only. It is denoted as $W_{sgn}$.

5.3.2 Watermark Embedding

In the proposed scheme, the color image is separated into Red, Blue and Green channels. Red channel is used to extract feature points using SIFT and these feature points are saved as synchronous registration information which is required for watermark detection.(Refer Appendix B for SIFT feature points extraction.) As human eye is less sensitive to changes in Blue color, it is preferred to embed watermark in Blue channel. Watermark embedding process is as follow:

1. Separate the color carrier image into three color channels.
2. Calculate feature points of Red channel by using SIFT and save as synchronous registration information.

3. Perform 2-level DWT using bi-orthogonal wavelet transform on the Blue and green components of carrier image.

4. Select the LH subband of Blue and Green channel of decomposed image. Select the first \( L_w \) number of wavelet coefficients from these bands, where \( L_w \) is equal to the length of signature watermark.

5. Embed the watermark in selected coefficients of Blue component of the host image based on following logic.
   
i) For entire length of watermark
   
ii) Compare Blue channel coefficients with Green channel coefficients
   
iii) If \( W_{sgn}(i) == '1' \)
   
iv) Set Blue channel coefficient to a value higher than corresponding Green channel coefficient
   
v) Else if \( W_{sgn}(i) == '0' \)
   
vi) Set Blue channel coefficient to a value smaller than corresponding Green channel coefficient

vii) End if

viii) End for

6. Reconstruct the watermarked image \( I_w \) using inverse discrete wavelet transform.

The offset value (OV) that is to be added or subtracted from Green channel coefficients to make corresponding Blue channel coefficients smaller or larger based on watermarking bits is given by

\[
OV = \frac{\text{Avg}_\text{lum}(I_b)}{\sqrt{m \times n}} \times 4
\]  

(5.7)

Where \( \text{Avg}_\text{lum} \) is the intensity of Blue component of image, \( m \) and \( n \) are the dimensions of image. Traditionally, offset value is fixed. In proposed scheme the offset is adapted depending upon the image. This results in better PSNR than fixed offset value.
5.3.3 Watermark Extraction

Watermark extraction process is carried out in two steps. First step is the estimation of geometric attacks by comparing the feature points of original image and watermarked image and correction of such geometric distortion for synchronization. Second step is actual extraction of watermark from the distortion inverted image.

5.3.3.1 Geometric attack estimation

Feature points are suitable for watermarking with implicit synchronization as they have covariance with geometric transformations [111]. Scale and orientation are used as feature points which are invariant to geometric transformations.

- Scale estimation: SIFT feature points are achieved under different scales. Therefore, the scale characteristics of feature points have a proportional relationship with image scaling. Scaling factor can be estimated as SIFT feature points are achieved under different scales. Therefore, the scale characteristics of feature points have a proportional relationship with image scaling. Scaling factor can be estimated as

\[ S_{est} = \frac{\sum_{i=1}^{m} q_i}{\sum_{i=1}^{m} p_i} \]  

(5.8)

Where 'm' is the total number of matched feature points of original image and watermarked image, 'S' is the scaling factor of attacked watermark image, \( p_i \) and \( q_i \) are the scales of matched feature points of original and watermarked image. Scaling correction is done by resizing the attacked watermarked image by scale correction factor given by Equation 5.9.

\[ scale\_correction = S_{est}^{-1} \]  

(5.9)

- Rotation estimation: Angle of rotation of attacked image can be calculated based on difference in orientation of matched feature points of original and attacked image. Assuming watermarked image is rotated by an angle \( \theta \), total number of matched feature points is 'm', the center angle of original image feature points is \( \phi_o \) and that of corresponding matched feature point of rotated image is \( \phi_r \), the estimation of
angle by which watermarked image is rotated can be computed as follow:

\[
\theta_{est} = \frac{\sum_{i=1}^{m} (\phi_r - \phi_0)}{m}
\]  

(5.10)

The image is restored to its original shape by rotating it by *anti_rotation* factor given by Equation 5.11

\[
anti_{rotation} = -\theta_{est}
\]  

(5.11)

5.3.3.2 Watermark extraction from distortion inverted image

In this stage, watermarked image is checked for any geometric distortions such as scaling, rotation as discussed above. Watermark detection steps are as follow:

1. Segregate the three channels of watermarked color image and extract the feature points of Red channel using SIFT.

2. Synchronization step: Compare these feature points with feature points of original image to estimate geometric distortion.

3. Correct these geometric distortions.

4. Apply 2 level wavelet transform using bi-orthogonal wavelet on Blue and Green channel.

5. Generate the sequence of only ’1’ which is equal to length of watermark. This sequence is used for reconstruction signature.

6. Select the LH subband of Blue and Green channel of decomposed image. Select the first ’\(L_w\)’ number of wavelet coefficients from these bands, where ’\(L_w\)’ is equal to the length of signature watermark.

7. Watermark detection is based on following logic:
   
   i) While length of watermark
   
   ii) Compare Blue channel coefficients with corresponding Green channel coefficients
   
   iii) If Blue channel coefficient is higher than corresponding Green channel coefficient
   
   iv) Set watermark bit equal to ’1’ of the sequence generated in step 5
v) Else if Blue channel coefficient is smaller than corresponding Green channel coefficient
vi) Set watermark bit equal to ‘0’
vii) End if
viii) End while

8. Reshape it to form two dimensional signature image.

5.3.4 Experimentation and Results

5.3.4.1 Data payload

Number of coefficients of Blue channel and green channel are changed depending upon the signature bit. Therefore number of coefficients changed depends upon the length of signature which in turn depends upon the size of signature image which varies between 60 × 30 to 120 × 120.

5.3.4.2 Estimation of geometric attacks

Watermarked image is subjected to different scaling and rotation transformations. Through SIFT synchronization, transformations are estimated and inverted as discussed earlier. Table 5.4 shows the actual scaling factor, estimated scaling factor and percentage of accuracy. Table 5.5 shows the angle by which image is rotated, estimated rotation angle and percentage of accuracy.

Table 5.4: Estimated scaling factor and percentage of accuracy

<table>
<thead>
<tr>
<th>Scaling factor</th>
<th>Estimated scaling factor</th>
<th>Percentage of accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5</td>
<td>0.5601</td>
<td>87.96</td>
</tr>
<tr>
<td>0.6</td>
<td>0.6526</td>
<td>91.22</td>
</tr>
<tr>
<td>2</td>
<td>2.0372</td>
<td>98.13</td>
</tr>
<tr>
<td>3</td>
<td>3.0351</td>
<td>98.82</td>
</tr>
<tr>
<td>4</td>
<td>4.0750</td>
<td>98.12</td>
</tr>
<tr>
<td>5</td>
<td>5.0804</td>
<td>98.39</td>
</tr>
<tr>
<td>6</td>
<td>6.1199</td>
<td>98.00</td>
</tr>
</tbody>
</table>
Table 5.5: Estimated rotation angle and percentage of accuracy

<table>
<thead>
<tr>
<th>Rotation angle</th>
<th>Estimated rotation angle</th>
<th>Percentage of accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>9.94132</td>
<td>99.41</td>
</tr>
<tr>
<td>20</td>
<td>20.0890</td>
<td>99.55</td>
</tr>
<tr>
<td>30</td>
<td>29.8258</td>
<td>99.42</td>
</tr>
<tr>
<td>40</td>
<td>40.3002</td>
<td>99.25</td>
</tr>
<tr>
<td>60</td>
<td>59.3999</td>
<td>99</td>
</tr>
<tr>
<td>90</td>
<td>89.97069</td>
<td>99.97</td>
</tr>
<tr>
<td>100</td>
<td>100.1319</td>
<td>99.87</td>
</tr>
<tr>
<td>110</td>
<td>109.9108</td>
<td>99.92</td>
</tr>
<tr>
<td>120</td>
<td>119.4345</td>
<td>99.53</td>
</tr>
<tr>
<td>150</td>
<td>148.9016</td>
<td>99.27</td>
</tr>
<tr>
<td>170</td>
<td>169.5421</td>
<td>99.73</td>
</tr>
<tr>
<td>300</td>
<td>298.3983</td>
<td>99.47</td>
</tr>
<tr>
<td>330</td>
<td>330.9143</td>
<td>99.72</td>
</tr>
</tbody>
</table>

5.3.4.3 Results

Figure 5.8 shows various signature watermarks embedded in the image Baboon, watermarked image and the corresponding extracted signature watermarks.

![Figure 5.8: continued](image-url)
Figure 5.8: Results of SIFT based technique for different signature watermarks
Figure 5.9: Average PSNR and SSIM for different images for SIFT based technique for signature watermark

Figure 5.9 shows average PSNR and percentage of SSIM for different host images.

5.3.4.4 Robustness against geometric attacks

Sample watermarks extracted from watermarked images under geometric transformation are shown in Figure 5.10.

(a) 30 degree rotation

(b) 60 degree rotation

Figure 5.10: continued
Figure 5.10: Results of SIFT based technique under different geometric attacks
5.3.4.5 Robustness against signal processing attacks

Some of the extracted signatures under different signal processing attacks are shown in Figure 5.11.

(a) Brightness attack
(b) Unsharpen
(c) Gaussian noise
(d) Salt and pepper noise
(e) JPEG compression

Figure 5.11: Results of SIFT based technique under different signal processing attacks
Table 5.6 shows the percentage of SSIM and perceptual quality of extracted watermark on a scale of three as good, recognizable and not recognizable under different types of attacks.

Table 5.6: Average percentage of SSIM and perceptual quality of extracted watermark

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Attacks</th>
<th>parameter</th>
<th>% of SSIM</th>
<th>Perceptual quality of extracted watermark</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Brightness</td>
<td>0.8</td>
<td>99.24</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2</td>
<td>98.27</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Histogram Equalization</td>
<td></td>
<td>94.3</td>
<td>Not recognizable</td>
</tr>
<tr>
<td>3</td>
<td>Salt and Pepper</td>
<td>0.1</td>
<td>99.21</td>
<td>Recognizable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.2</td>
<td>98.65</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Gaussian Noise</td>
<td>1%</td>
<td>98.55</td>
<td>Recognizable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3%</td>
<td>98.35</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Unsharpen</td>
<td></td>
<td>100</td>
<td>Good</td>
</tr>
<tr>
<td>6</td>
<td>JPEG Compression</td>
<td>80</td>
<td>99.323</td>
<td>Recognizable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>85</td>
<td>99.37</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>90</td>
<td>99.43</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>95</td>
<td>99.61</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Row-Column Blanking</td>
<td>Cols = 50, 99, 192, 300</td>
<td>100</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rows = 14, 169, 119, 320</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Row-Column Copying</td>
<td>Cols = 211-123, 256-11, 455-169, 359-50</td>
<td>100</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rows = 123-211, 11-256, 169-455, 359-50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Cropping</td>
<td>10%</td>
<td>99.59</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30%</td>
<td>99.13</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Scaling</td>
<td>0.5</td>
<td>99.68</td>
<td>Good</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>99.99</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>99.99</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>99.99</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Rotation</td>
<td>30 to 180</td>
<td>98.43</td>
<td>Good</td>
</tr>
</tbody>
</table>

5.3.5 Observations

- After geometric transformation, percentage of accuracy of estimated scaling factor is 95% and for rotation it is 99%.

- Average PSNR of watermarked image without any attack is 39dB.

- Average SSIM of extracted signature without any attack is 100% .

- Robustness against geometric transformation
– Method shows strong robustness against rotation attack for wide range of angles.

– Method shows strong robustness against scaling attacks for a scaling factor within range of 0.4 to 3.

– Extracted signature is recognizable up to 30% cropping.

• Robustness against signal processing attacks

    – Method is fragile for histogram equalization, and JPEG compression below Q.F = 40.

5.4 Summary

This chapter discussed the techniques for watermark embedding with handwritten signature. Correlation based approach for watermark extraction is a blind technique and is applicable for color as well as gray scale images. On the other hand, SIFT based scheme is a semiblind technique for watermark extraction and can be used only for color images. These methods can be used for ownership assertion.