Chapter 5

Image Watermarking With Non-Symmetric Rotational Attacks
CHAPTER 5

IMAGE WATERMARKING WITH NON-SYMMETRIC ROTATIONAL ATTACKS

5.1 INTRODUCTION

Robustness is a most impotent key feature of advanced watermarking. A large portion of watermarking strategies doesn't work on Geometric attacks. When we apply the Rotational attacks in unmanned that means the angle is about Non-Symmetric the data is lose because in Spatial based watermarking system will hide the data in everywhere in the image so if we embedded the data is image then it will be affected more when rotational attacks are apply. So here data protection is main problem. This chapter is about to introduce the new concept of non-symmetric rotational attacks and how it can be defense.

From the Early Chapter-4 we have studied different Geometric attacks Rotation, scale and Translation. As well as our system recover both data and cover image based on feature approach. But from analysis it will not protect the data when non-symmetric rotational attacks. So in current chapter introduce new system which defense against Non-Symmetric Rotating angle attacks.

5.2 NON-SYMMETRIC ATTACKS PREVENSION APPROACH

As shown in Figure 5.1, the flow diagram of Embedding and Extraction the system is made of Block division of DWT image and finding the SVD of the image in LL-Band. A strong Discrete Wavelet Transform with Singular Decomposition Embedding algorithm is offered based on Pseudo Zernike moment (PZM) for rotation invariance and scale invariance watermarking scheme. Following approach attach to round of the Cover image matrix is designated as the PZM control part, and the rectangle of the Cover image round is chosen to embed Information data. Initially, the Range of embed watermark is showed with DWT and the LL of DWT constant is divided into non-overlap block; then Singular Decomposition is practical to Each non-overlapping DWT blocks.

Furthermore, bits of the Numbers is imbedded through minor alterations of the singular decomposition significance (SVD) matrix in every block. Finally, to recover the attacks first apply Pseudo Zernike moment. Surf feature on watermark image so, it will extract the attacks pixel and recover the scale-angle using affine transformation. The Results has proved that the planned approach not fair has noble fight to geometric attacks, and more, all types of non-symmetric Rotation angle attacks that is not provided by other methods yet. The research work gives a better way for providing authentication to all online data geometric attacks.
5.3 EMBEDDING STEPS

Step 1: Read Watermark Image.

Step 2: Give Y a chance to signify the watermark inserting part, and utilize Haar wavelet Transform to Y; then pick up the LL band have most extreme vitality. Distribute LL into blocks Bi of size $4 \times 4$.

\[ Z_f' = [a_1, a_2, a_3, \ldots, a_S] \text{ where } Z_f' \text{ is vector, and } a_i \text{ is the SVD of all block, } S \text{ is rank of all block.} \]

Step 3: Apply the straightforward strategic monitor on encrypt the watermark.

\[ x_{n+1} = \mu x_n (1 - x_n), 0 < x_n < 1, \quad n = 0, 1, 2, \ldots \]

Step 4: Calculate the value of $Z_f^{''}$
Chapter 5  Image Watermarking With Non-Symmetric Rotational Attacks

Noms $Z_j^{p'} = \sqrt{\sum_{j=1}^{S} a_j \ast a_j}$ and then $NO^{p'} = \text{Noms} (Z_j^{p'}) \ast D$ .................................(5.2)

Step 5: Embed bit using following technique.
If $b=1$ then {if $O$ is odd then $O' = O + 1$ else $O' = O$} {Else {if $E$ is even then $E' = E$ else $E' = E + 1$}}.

Step 6: Calculate the modified value and the modified vector as follows:

$\text{Noms} (Z_j') = NO' \ast D + (D/2)$,  
$Z_j = Z_j \times \text{Noms} (Z_j') / \text{Noms} (Z_j))$ .................................(5.3)

Step 7: Apply inverse DWT to generate watermarked image.

5.4 EXTRACTION STEPS

Step 1: To gauge the utilization of ensured Pseudo Zernike moments.

$V_n (I,J) = R_n (I,J) \exp (jn \tan^{-1} (I/J))$ .......................................................(5.4)

Where $l^2 + j^2 \leq 1$, $n \geq 0$, $|m| \leq n$.

$P \ M_n = \frac{n+1}{\pi} \sum_{I} \sum_{J} f(I,J) V_n (I,J)$ .......................................................(5.5)

$A=\text{absolute} (Z)$

$\text{Angle} (Z) = \tan^{-1} (\text{imag}(Z), \text{real}(Z))$

$\text{Phi} = \text{angle} (Z) \times 180 / \pi$

Step 2: Surf Feature extract.

1. Detect “interest points, use Hessian matrix approximation. Build the integral images and the scale space of image.”

2. Notice “point report and identical, descriptor labels the delivery of the intensity content, similar to SIFT. Based on sum of Haar wavelet responses, construct a square region centered on the interest point and oriented along the orientation selected in previous section.”

Step 3: Pick “up the Recovered watermarked image, and actualize 1-level DWT disintegration to its watermark embedding part. Get the sub-band LL’ which has incomparable vitality.”

Figure 5.3: Surf Feature Extraction

- 139 | Page
Chapter 5 Image Watermarking With Non-Symmetric Rotational Attacks

Step 4: Slice the sub-band LL into blocks Bi of size 4×4.
\[ Z_j'' = [a_1, a_2, a_3, \ldots, a_s] \] ......................................................................................(5.6)
Where \( Z_j'' \) is a \( 4 \times s \) vector, and \( a_i \) is Singular decomposition of blocks and \( S \) is rampant of blocks.

Step 5: Calculate the value of \( Z_j'' \),
\[ \text{Norms} Z_j'' = \sqrt{\sum_{j=1}^{s} a_j \ast a_j} \text{ and the NO}'' = \text{Norms} (Z_j'')/D \] .............................................(5.7)

Step 6: Extract bit and extract watermark.
Step 7: Stacked extracted image with database share image with XORed operation.
Step 8: Recover Username and Password.

5.5 NON-SYMMETRIC ROTATION ATTACKS

This types of Geometric attack in the image is converted into different angle. The Rotation angle is between 0 to 180 degree angles. As from literature the angle 30, 60 and 90 its works because it is in symmetric form but for odd cased like 92, 62 etc. are non-symmetric type values this will affect the embedding data directly so here by using SURF features and affine transform will recover the attacks.

5.6 EXPERIMENTAL RESULTS
Figure 5.4: (A) Enter USR And PSW (B) QR-Code (C) Share-1 (D) Share-2 (E) Share-3 (F) Share-4 (G) Cover Image (H) DWT-SVD (I) Non-symmetric Rotation Attack (J) Rotation-Translation Attack (K) Rotation-Scale-Translation Attack (L) Recover Theta And Angle (M) Recover Image (N) Recovered Share-2 (O) QR-Code Recover

<table>
<thead>
<tr>
<th>Rotation (degree)</th>
<th>Only Rotation</th>
<th>Rotation With Scale 2</th>
<th>Rotation With Translation 10</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSNR (db)</td>
<td>MSE</td>
<td>PSNR (db)</td>
</tr>
<tr>
<td>0</td>
<td>63.083</td>
<td>0.028</td>
<td>62.051</td>
</tr>
<tr>
<td>16</td>
<td>64.043</td>
<td>0.025</td>
<td>63.072</td>
</tr>
<tr>
<td>32</td>
<td>65.063</td>
<td>0.023</td>
<td>64.022</td>
</tr>
<tr>
<td>35</td>
<td>65.053</td>
<td>0.022</td>
<td>65.064</td>
</tr>
<tr>
<td>43</td>
<td>66.021</td>
<td>0.021</td>
<td>66.014</td>
</tr>
<tr>
<td>46</td>
<td>66.081</td>
<td>0.023</td>
<td>66.032</td>
</tr>
<tr>
<td>54</td>
<td>64.093</td>
<td>0.022</td>
<td>64.086</td>
</tr>
<tr>
<td>68</td>
<td>65.023</td>
<td>0.024</td>
<td>65.068</td>
</tr>
<tr>
<td>120</td>
<td>65.033</td>
<td>0.019</td>
<td>65.029</td>
</tr>
<tr>
<td>142</td>
<td>66.071</td>
<td>0.022</td>
<td>65.032</td>
</tr>
<tr>
<td>170</td>
<td>64.081</td>
<td>0.024</td>
<td>64.055</td>
</tr>
</tbody>
</table>
**Chapter 5**  
*Image Watermarking With Non-Symmetric Rotational Attacks*

![PSNR Graph for Non-Symmetric Angle](image1)

**Figure 5.5:** PSNR Graph for Non-Symmetric Angle

![MSE Graph for Non-Symmetric Angle](image2)

**Figure 5.6:** MSE Graph for Non-Symmetric Angle

**Conclusion:** In this chapter, Embedding Process is done by DWT+SVD in Block manner. Surf and Pseudo Zemike moment feature is used to detect rotation and scaling attack. Affine transformation is used to recover watermark image attacks. The analysis of above process is verify using two parameters PSNR and MSE. The values of parameters for Non-Symmetric Rotational attack is show in Table 5.1 respectively. It concludes that the PSNR value increases above 60db and MSE value decreases below 0.20 for Color image.