Integer Wavelet Transform based Dual Watermarking Technique using Tent Map and Local Binary Pattern

By Sumaya Rahman, Chandan Saha, Md. Foisal Hossain & Tanjil Alam Tamal

Khulna University of Engineering & Technology

Abstract: Watermarking ascribes to insert pattern of bits into an image that conserves copyright information from unauthorized users. In this paper, Integer Wavelet Transform based image watermarking technique using Tent map and Local Binary Pattern has been proposed. Tent Map is used to generate chaotic key sequence to scramble two watermark images. Integer Wavelet Transform (IWT) is applied on the host image to define approximation coefficient (LL) band and to achieve higher level of robustness as perfect reconstruction is guaranteed by the composition of Lifting method. Local Binary Pattern (LBP) is used to generate binary matrix from LL band. Two watermarks are embedded simultaneously to the even and odd coefficients of 5×5 mask of host image. To check robustness, several attacks has been added to watermarked images; their normalized correlation (NC) and peak signal to noise ratio (PSNR) values are quite inspiring, that exhibits superiority of our scheme than some existing schemes.

Keywords: dual watermarking, integer wavelet transform, local binary pattern, tent map.

GJRE-F Classification: FOR Code: 090699

Strictly as per the compliance and regulations of:
Abstract - Watermarking ascribes to insert pattern of bits into an image that conserves copyright information from unauthorized users. In this paper, Integer Wavelet Transform based image watermarking technique using Tent map and Local Binary Pattern has been proposed. Tent Map is used to generate chaotic key sequence to scramble two watermark images. Integer Wavelet Transform (IWT) is applied on the host image to define approximation coefficient (LL) band and to achieve higher level of robustness as perfect reconstruction is guaranteed by the composition of Lifting method. Local Binary Pattern (LBP) is used to generate binary matrix from LL band. Two watermarks are embedded simultaneously to the even and odd coefficients of 5x5 mask of host image. To check robustness, several attacks has been added to watermarked images; their normalized correlation (NC) and peak signal to noise ratio (PSNR) values are quite inspiring, that exhibits superiority of our scheme than some existing schemes.

Keywords: dual watermarking, integer wavelet transform, local binary pattern, tent map.

1. INTRODUCTION

Watermarking is a marvelous technique in which number of bits another image or logo are inserted in another contents. Digital image watermarking supports image, audio or video file as watermark. At present data security, copyright protection, imperceptibility and authenticity have become indispensable issues in data hiding. Watermarking indemnifies all these issues in a strategic way. Watermarking technique can be implemented in two domains: spatial domain and frequency domain. In spatial domain, without using any transformation, the watermark can be embedded into host image which is of less complexity and simpler but it’s not that much robust against attacks. Frequency domain needs some transformation [1-2] before embedding the watermark image into host. Though it is complex than spatial domain, it shows more robustness against attacks. According to type of document, watermarking is of text, image, audio or video types. Based on several applications it is of three types as fragile, semi-fragile and robust. Visible and invisible watermarks are types of fragile water marking. Tamper detection is a prime theme for fragile watermarking. Robust watermarking is an algorithm that is dynamic and rigid even after adding noise.

Many embedding techniques have been proposed earlier based on Local Binary Pattern, Integer Wavelet Transform or Tent Map. Bhardwaj et al. [1] has proposed a lifting wavelet transform based robust watermarking scheme that uses singular value decomposition for obtaining singular values of watermark image. Makbol et al. [2] has discussed a robust watermarking scheme that based on IWT and SVD that performs authentication and helps security issues. Lazarov et al. [3] proposed an algorithm that uses chaotic maps for embedding; Arnold’s cat map and Tent map are applied to the host and watermark image respectively. Chang et al. [4] have proposed a LBP based recoverable fragile watermarking technique that uses 3 x 3 size blocks for LBP operator. Zhang et al. [5] proposed a blind fragile watermarking scheme based on LBP, Arnold transform and Logistic map. An sari et al. [6] proposed a water marking technique in which IWT and singular value decomposition (SVD) based scheme was discussed to ensure security and robustness. On the host image, IWT was applied first and then, on this transformed image, SVD was applied because the properties of SVD and IWT gave higher level of robustness. Wenyin et al. [7] proposed a semi-fragile multi-level image watermarking scheme based on LBP operators that was performed in spatial domain. A digital dual watermarking using SVD and redundant discrete wavelet transform (RDWT) has been proposed by Gaur et al. [8] which has a primary watermark and a scrambled watermark using Arnold cat map. Saiyyad et al. [9] proposed a dual watermarking process with hash function and the security purpose of AES ciphered watermarking and also tampers detection. It uses unique identification code as first watermark and for second water mark; hash code is generated from host image. All these papers have proposed watermarking scheme using Local Binary Pattern, Integer Wavelet Transform or Tent Map individually. But we wanted to combine these three themes into one method to provide more robustness and stiffness of technique. Morteza et al. [10-11] proposed two watermarking schemes using SVD and DWT-SVD technique.
III. Proposed Scheme

a) Embedding Procedure

A gray-scale image of size \((M \times N)\) is taken as the host image. Then IWT is applied on this image for find LL band \((CA1)\) band. After this, local binary pattern \([7]\) is applied for each \((5 \times 5)\) mask of \(CA1\) band to form binary matrix. The whole embedding procedure is shown in Fig. 1 and is illustrated in algorithm as follows:

1. A grayscale image is considered as cover image
2. Two watermark images \((w1 \& w2)\) are taken to embed in the cover image, \(w1\) is for odd pixel and \(w2\) for even pixel; perform XOR operation with Tent map to generate scrambled watermarks \((s1 \& s2)\)
3. IWT is applied on host to obtain \(CA1\) band
4. LBP is applied on \(CA1\) band if neighbor pixel > centre pixel, assign neighbor pixel = 1 and if neighbor pixel ≤ centre pixel, assign neighbor pixel = 0 Thus, binary matrix \((b)\) is generated.
5. For each \(5 \times 5\) mask, perform XOR operation on even and odd pixels of the binary matrix \((b)\).
6. Compare XOR outputs of odd \((b1)\) and even \((b2)\) pixels of the binary matrix \((b)\) with the scrambled water mark images \(s1\) & \(s2\) respectively. If \(b1\) \((i, j)\) == \(s1\) \((i, j)\) or \(b2\) \((i, j)\) == \(s2\) \((i, j)\); no change will occur to the original \(CA1\) band. If \(b1\) \((i, j)\)~ == \(s1\) \((i, j)\) or \(b2\) \((i, j)\)~ == \(s2\) \((i, j)\); any one of the 12 odd pixels or any one of the 12 even pixels of \(5 \times 5\) mask except centre pixel, will be changed in the original \(CA1\) band.
7. For odd pixels, in the original \(CA1\) band, if \(CA1\) \((i − 1, j − 1)\) > centre pixel, assign \(CA1(i − 1, j − 1)\) = centre pixel + \(k\) and if \(CA1\) \((i − 1, j − 1)\) ≤ centre pixel, assign \(CA1(i − 1, j − 1)\) = centre pixel - \(k\)
8. For even pixels, in the original \(CA1\) band, if \(CA1\) \((i − 1, j)\) > centre pixel, assign \(CA1(i − 1, j)\) = centre pixel + \(k\) and if \(CA1\) \((i − 1, j)\) ≤ centre pixel, assign \(CA1(i − 1, j)\) = centre pixel - \(k\)
9. Watermarked \(CA1\) band is obtained
10. Inverse IWT is applied to obtain watermarked image.
Algorithm for embedding $w_1$ on odd pixel position

Algorithm for embedding $w_2$ on even pixel position

$w_1$ $w_2$

$\text{Tent map}$

$\text{Xor}$

$\text{Xor}$

$\text{Scrambled watermark } s_1$

$\text{Scrambled watermark } s_2$

Scrambled watermark $s_1$

Scrambled watermark $s_2$

$\text{Watermark } w_1$

$\text{Watermark } w_2$

Figure 3: Block diagram for embedding procedure

Figure 4: Block diagram for extracting procedure
b) Extraction Procedure

In this section, we will discuss about the extraction procedure of proposed method. In the extraction part, two watermark images are extracted from the watermarked image. First two scrambled watermarks \( s_1 \) and \( s_2 \) are generated, then performing the XOR operation with tent map, the extracted watermarks \( w_1 \) & \( w_2 \) are again generated. The whole procedure is shown in Fig. 2 and also illustrated in the following algorithm:

Whole procedure is shown in Fig. 4, and also illustrated in the following algorithm:

1. IWT is applied on the watermarked image to find approximation coefficient band
2. LBP is again applied on watermarked \( CA1 \) band
3. For each \( 5 \times 5 \) mask, all even and odd pixels are found and apply XOR operation on them
4. For each \( 5 \times 5 \) mask, for both even and odd XOR outputs, if XOR output is 1, store 1; otherwise store 0
   The outputs are the extracted scrambled
5. Tent map is XORed with both \( s_1 \) & \( s_2 \) to obtain extracted watermarks \( w_1 \) & \( w_2 \) again

This procedure is repeated for different values of scaling factor.

IV. Experimental Result

In this section, the performance analysis of this proposed scheme has been discussed. We have implemented our proposed technique using MATLAB 2014 and used some test images and two watermarks for embedding. The host image is taken \( (M \times N) \) dimension. After applying IWT, dimension of LL band has become half of host image, i.e. \( (m \times n) \). So, the size of watermarks is taken as one-fifth of the LL band that means \( (m/5 \times n/5) \) as the mask size is taken \( (5 \times 5) \). Tent map is used in this technique to generate random numbers which are converted to binary numbers and then reshaped to a matrix of size \( (m/5 \times n/5) \). This output is used to scramble the two watermarks. For performing the XOR condition between tent map and sample image, it is important to take their dimension equal. If their dimensions don’t match, XOR operation will not take place. After performing XOR between the Tent map and sample image, a scrambled image is generated. For performing the XOR condition between tent map image and sample image, it is important to take their dimension equal. If their dimensions don’t match, XOR operation will not take place.

MSE means mean square error that can be defined as cumulative squared error between the watermarked image and original image. PSNR is the measure of peak to peak error of image that is measured in terms of logarithmic decibel scale. With the increase of MSE of an image, PSNR value decreases. For \( M \times N \) image, they can be calculated as following:

\[
MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [x(i, j) - y(i, j)]^2
\]  

\[
PSNR = 10 \log_{10} \left( \frac{\text{max}^2}{\text{MSE}} \right)
\]

Table 1: Performance parameters for test images

<table>
<thead>
<tr>
<th>Image</th>
<th>PSNR(dB)</th>
<th>MSE</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peppers</td>
<td>46.74</td>
<td>1.2571</td>
<td>1</td>
</tr>
<tr>
<td>Lena</td>
<td>45.43</td>
<td>1.7902</td>
<td>1</td>
</tr>
<tr>
<td>Jet plane</td>
<td>44.74</td>
<td>2.1812</td>
<td>1</td>
</tr>
<tr>
<td>Cameraman</td>
<td>44.38</td>
<td>2.3945</td>
<td>1</td>
</tr>
</tbody>
</table>
Normalized correlation describes the congruity between two images. NC for any image is always 1 when no attack is added. When any attack is added to an image, this value decreases according to amount of noise. NC is calculated by:

\[
NC = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} (W(x, y) \times W'(x, y))}{\sum_{x=1}^{M} \sum_{y=1}^{N} W(x, y)^2}
\]  

(5)

\(W\) and \(W'\) are original watermark and extracted watermark, respectively. \(M\) and \(N\) are rows and columns of the watermark image.

### Table 2: PSNR (dB) values for different scaling factor

<table>
<thead>
<tr>
<th>Scaling factor</th>
<th>Peppers</th>
<th>Lena</th>
<th>Jet plane</th>
<th>Cameraman</th>
</tr>
</thead>
<tbody>
<tr>
<td>(k = 1)</td>
<td>46.74</td>
<td>45.43</td>
<td>44.74</td>
<td>44.38</td>
</tr>
<tr>
<td>(k = 2)</td>
<td>46.31</td>
<td>45.06</td>
<td>44.42</td>
<td>44.11</td>
</tr>
<tr>
<td>(k = 3)</td>
<td>45.87</td>
<td>44.68</td>
<td>44.07</td>
<td>43.83</td>
</tr>
<tr>
<td>(k = 4)</td>
<td>45.42</td>
<td>44.29</td>
<td>43.73</td>
<td>43.54</td>
</tr>
<tr>
<td>(k = 5)</td>
<td>44.97</td>
<td>43.90</td>
<td>43.37</td>
<td>43.23</td>
</tr>
<tr>
<td>(k = 6)</td>
<td>44.52</td>
<td>43.52</td>
<td>43.02</td>
<td>42.93</td>
</tr>
<tr>
<td>(k = 7)</td>
<td>44.09</td>
<td>43.14</td>
<td>42.69</td>
<td>42.62</td>
</tr>
</tbody>
</table>

Test images, watermarks, scrambled watermarks and watermarked images with corresponding PSNR values are shown in Fig. 3. The PSNR, MSE and NC values of four test images are demonstrated in Table 1. Varying the scaling factor \(k\), different PSNR values are obtained which are listed in Table 2. From the both Table 1, it is observed that, peppers image gives the highest PSNR value for all the values of \(k\). Changing the scaling factor from 1 to 7 indicates rigidity of our proposed method because PSNR values of this scheme is fluctuating very little. With increasing this value, PSNR decreases gradually. In Peppers image, maximum PSNR is 46.74 dB, obtained for \(k = 1\). This value decreases at 45.87 dB for \(k = 3\), and finally it is 44.09 dB when \(k = 7\). same phenomena happen for all the test images.

Performance parameters as PSNR and NC are also observed after adding some noises as attack. Variation of the value of NC is noticed for different attacks because for adding noises, images become little distorted. That means, some pixel values may change in the extracted watermarks. To check the rigidity of this
technique, attacks as Salt & pepper noise, Gaussian noise, Cropping, histogram equalization, image sharpening and contrasting are added to the watermarked image and then watermarks are then extracted. Normalized correlation between the original watermark and extracted watermark for Salt & pepper noise (0.001) and Gaussian noise (0.001) are observed in Table 3. These values are fluctuating according to test images. Lena image gives the better NC values for both watermarks 0.9971 and 0.9965, for Gaussian noise.

Here, watermark 1 gives better result than watermark 2. But in peppers image, watermark 1 gives smaller value 0.9939 than watermark 2, i.e. 0.9940. Lowest value is 0.9889 for second watermark of Jet plane image. For Salt & pepper noise, NC values are decreased. In this case, watermark 2 of all the images gives better NC than watermark 1 except Peppers image. Geometric attack is also added to the watermarked image. Three types of cropping as: middle, bottom left and upper right are applied and their corresponding NC values for the both watermarks are shown in Table 4. Among these attacks, bottom left gives better NC values for both the watermarks. Overall values of bottom left are better than other two attacks. Peppers and Cameraman images gives higher NC. Image processing attacks are also added as histogram equalization, image sharpening and contrasting in Table 5. In image sharpening, the NC value is better in watermark 2 than watermark 1 for all the test images. For example, w1 gives 0.9873 NC value in Lena image and w2 gives 0.9916. But in image contrasting, watermark 1 gives better values for most of the test images such as; for Jet plane image, w1 gives 0.9681 and w2 gives 0.9669. Lena image gives lowest NC values for both watermarks among all the images; 0.9168 and 0.9256. Cameraman image gives lowest NC values for histogram equalization; w1 gives 0.9362 and w2 gives 0.9356 among these three attacks, image sharpening shows better performance for all the test images.

Figure 4: Peppers watermarked image and two extracted watermarks with various noise.
Figure 5: Lena watermarked image and two extracted watermarks with various noise

Figure 6: Jet-plane watermarked image and two extracted watermarks with various noise
Fig. 4 Shows the Peppers image with six different attacks and its corresponding extracted watermarks. For cropping (middle), extracted watermarks are very similar to the original image. For contrasting and histogram equalization, extracted watermarks are little bit distorted than other attacks. In Peppers image, watermark 2 seems to be better than watermark 1. Fig. 5 Shows the Lena image with attacks and its corresponding extracted watermarks. For contrasting and histogram equalization, both the watermarks are little distorted. In this figure, cropping (middle) gives better extracted watermarks again. Watermark 2 seems to be better than watermark 1 in this figure also. Same attacks are applied on jet-plane and cameraman images which are demonstrated in Fig. 6 and Fig. 7, respectively. Table 6 and Table 7 demonstrates the comparison of the scheme in terms of robustness test for Lena and Peppers images. NC values of watermark W2 are used for comparison with schemes [10] and [11].

V. Conclusion

In this paper, a dual level robust watermarking scheme has been introduced with the combination of integer wavelet transform, local binary pattern and tent map. IWT has made this method more robust and faster computability than any others transformation. Embedding procedure is conformed to odd and even pixel positions of host image with two watermarks. PSNR of the test images are varied according to change of scaling factor. For checking the rigidity of this method, image sharpening, histogram equalization, cropping, salt & pepper noise, gaussian noise and image contrasting are added to watermarked image. The output normalized correlation values show robustness of the method. We have also compared PSNR values with an existing method that exhibits remarkable results.

VI. References

2. M. Makbol, B. Khoo, “A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition.”


