Hierarchical-Edge based Torus Automorphism for Digital Watermarking

G.Rosline Nesa Kumari, Dr.S.Maruthuperumal, Dr.V.Vijayakumar

Abstract—The present paper proposes a Hierarchical-Edge based Torus Automorphism (HETA) to build an efficient Digital Watermarking (DWM) system. To increase the robustness of the embedded watermark against intentional attacks, Torus automorphism is used. TA disarranges the original image equally and randomly. The TA image is divided into blocks with hierarchical nature. The hierarchical blocks, minimizes changes in cover image when they are converted into corresponding in watermarked image. And they maintain high security over other methods. The watermark is embedded into the subblocks by exploring the edge concept. The edges are found by using Diagonal 45° Edge Pair Difference (DEPD) method. This makes the proposed HETA-DW system difficult to break and it is more robust even in the presence of attacks. The experimental result on various standard images indicates to break and it is more robust even in the presence of attacks.

Index Terms—Hierarchical, edge, Torus Automorphism, block, intentional attacks.

I. INTRODUCTION

Advanced digital technologies have made multimedia data broadly available. Recently, multimedia applications become universal in practice and thus security of multimedia information has become most important concern. The rapid growth of the multimedia services has created a potential demand for the fortification of ownership since digital media is easily reproduced and manipulated. In [16] Digital watermarking has been introduced for solving such problems. One of the largest outstanding applications of watermarking is using robust and practical watermarking to protect image and video data [17, 5].

The majority watermarking methods have been proposed to reach the goal of copyright protection [18]. All these watermarking methods embed the watermark in the cover image. Normally, these watermarking techniques can be divided into two categories. The primary category embeds the watermark into the spatial domain [2, 3, 6, 11 and 7]. The embedding method is carried out by modifying the Least Significant Bits (LSB) directly and watermark is embedded in the LSB of preferred pixels. The embedding system is carried out by transforming the original image into the frequency domain by DCT and DWT [4, 5, 8, and 9]. Normally, embedding data into the frequency domain is more robust than into the spatial domain; however, the spatial domain can carry more embedded information than the frequency domain. Regrettably, most watermark embedding schemes, spatial and frequency domains alike, have the identical drawbacks. Primarily, the watermark image is a binary image, which excludes it from the general situation. The watermark image must be meaningful and representative. Thus, the less constraint of the watermark image is, the better scheme will be. Secondly, the watermark scheme reduces the image quality and the degraded quality of the image makes it suspicious to pirates.

It is instigate in the journalism that the robust watermarking systems proposed so far can only stay alive some of the possible external attacks but not everyone. While spatial domain watermarking, in nearly all cases, is easy to apply on computational point of view but too fragile to resist vast varieties of external attacks. In frequency or transformed domain approaches offers robust watermarking but in the popular cases, executions need higher computational complexity. In accumulation, the transform domain technique is global in environment (global means inside the block in block based approach) and cannot restrict visual degradation of the original image. The image quality is degraded in the spatial domain methods due to watermarking could be banned in the neighborhoods leaving the section of interest unchanged.

In this paper, Hierarchical-Edge based Torus Automorphism for watermarking is presented. The proposed approach accomplishes the aim of copyright protection without degrading the image quality. In the proposed HETA-DW algorithm, the cover image is transformed by using two-dimensional Torus Automorphism and it is divided into blocks. To insert binary watermark DEPD method is used in the proposed HETA-DW system.

The rest of this paper is organized as follows. The related theories are discussed in Section 2. In Section 3, proposed approach is discussed. The experimental results are analysed in Section 4. Finally, conclusions are discussed in Section 5.

I. RELATED WORKS

A. Generation of mixed image

To increase secure and robustness of the embedded watermark against several attacks, Torus automorphism is used in the proposed system [10,12,13]. The TA disarranges the watermark bits equally and randomly before embedding and reconstructing it after extraction. Torus automorphism [11] is one of the kinds of a dynamic system. A dynamic system, changes the state’s when time’t’ changes and the dynamic system is defined in Equation (1).

$$S_{t+1} = f(S_t), t \in \mathbb{Z}$$  \hspace{1cm} (1)

where $t$ is discrete time. Apply the current state $S_t$ to the function $f$ in order to generate the next state $S_{t+1}$. On the other...
hand, TA can be seen as a permutation function in the two dimensional space. Its transform function is a 2×2 matrix A, where |A| = 1 is an eigen value. The state $S_{i+1}$ is having a coordinate $(x_{i+1}, y_{i+1})$, which is generated by the transform function from the last state $S_i$.

$$
\begin{bmatrix}
X_{i+1} \\
Y_{i+1}
\end{bmatrix} =
\begin{bmatrix}
\alpha_{11} & \alpha_{12} \\
\alpha_{21} & \alpha_{22}
\end{bmatrix}
\begin{bmatrix}
X_i \\
Y_i
\end{bmatrix} \mod N
$$

(2)

where $\alpha_{11}, \alpha_{12}, \alpha_{21}$ and $\alpha_{22} \in Z$. If the coordinate $x_0$ or $y_0$ is an irrational number in the initial state $s_0$, all the states in the dynamic system will not be shown repeatedly. However, if they are all rational numbers, there is a state $S_R = S_0$, where $R$ is the recurrence number. In Voyatzis and Pitas [1] proposed a torus automorphism with a single coefficient. The definition of their transform function is

$$
\begin{bmatrix}
X_{i+1} \\
Y_{i+1}
\end{bmatrix} =
\begin{bmatrix}
1 & 1 \\
k & k + 1
\end{bmatrix}
\begin{bmatrix}
X_i \\
Y_i
\end{bmatrix} \mod N
$$

(3)

where the recurrence number $R$ is related to the coefficient $k$, parameters $N$ and $k$ are secret keys needed for the scrambling and reconstruction of the watermark. Generally, $R$ will be $N-1$ or $N+1$, when $N$ is a prime number.

II. PROPOSED HETA-DW ALGORITHM

Copyright protection concerns the positive identification of ownership in order to protect the right of the owner. To provide an integrated solution in copyright protection and authentication, the proposed method integrates two methods namely TA and hierarchical DEPD. This integrated scheme provides robust watermarks suitable for copyright protection because they can resist common image processing operations. The proposed authentication systems is not going to embed the data into the watermarked image hence the image quality of the watermarked image will not be debilitated.

A. Embedding Algorithm

The block diagram of the proposed HETA-DW method is shown in Figure 1. The proposed method consists of six steps, as explained below.

**Step 1:** To increase the robustness and to maintain disarrangement of the image equally and randomly TA is applied on the original image. TA offers cryptographic protection of the image. TA is a two dimensional permutations. The matrix $\begin{bmatrix}
1 & 1 \\
k & k + 1
\end{bmatrix}$ is called as Torus automorphism. Transform the original image $(x,y)$ into $(x_o,y_o)$ by using Torus automorphism, also called mixed image.

**Step 2:** The disarranged image is divided into Hierarchical manner with a block size of two. The advantages of these Hierarchical blocks are:

- It minimizes changes in cover image when they are converted to corresponding watermark carrying regions in the watermarked image.
- It maintains high security over other methods.
- It increases the payload of the watermarking system.
- It withstands robustness for common attacks.

**Step 3:** Choose a block for inserting the watermark, based on global and local thresholds as explained below. The TA image is is partitioned into $(p \times p)$ non-overlapping block where $p = 2^n$, and $n = 1, 2, 3, ...,$. Let the size of the mixed image is $(N \times N)$. Then a total of $N/p^2$ blocks are obtained from the TA image. Calculate average for each block $B_i$ and calculate average of blocks $\mu$. Consider the block for inserting the watermark if $\mu \geq B_i$, and identify the diagonal edge pair pixels.

**Step 4:** Choose edge pixels of the selected block of step 3. Edge pixels are chosen for inserting the watermark for the following reasons.

- Image edges give good information about the image content because they allow the identification of the object structures.
- Edge detection is a fundamental tool used in most of the image processing applications to obtain information from the images as a precursor step to feature extraction.
- Edge aims at identifying points in a digital image at which the image brightness changes sharply or more formally and has discontinuities.
- Edge detection process detects and outlines the boundaries between objects and the background in the image.
- Edge features are useful to overcome the attacks generated by noise, edge strips and acuity.
- Edges form boundaries between the different textures.
- Edge reveals the discontinuities in image intensity from one pixel to another.

That’s why the present study found that edges are relatively a good choice for image authentication. The proposed method evaluates edge features on the entire TA image. For evaluating the edges “Diagonal 45° Edge Pair Difference” (DEPD) method is used. The DEPD detector provides better edge information with an advantage of being less sensitive to noise and finds the edges by looking for local maximum of the gradient of unprocessed input image. The DEPD method is explained below.
Diagonal 45° Edge pair Difference (DEPD) Method:

Consider diagonal 45° edge pair pixels to embed a watermark bit \( b \in \{0, 1\} \) into a pixel pair \((s, t)\). The difference \( d \) between \( s \) and \( t \) is calculated \( d = |s - t| \). The new difference \( d' \) is calculated by \( d' = 2 \times \lfloor \frac{d}{2} \rfloor + b \). The diagonal pair after embedding the watermark bit is calculated by the following:

\[
(s', t') = \begin{cases} 
  (s, s + d) & \text{if } s \leq t \\
  (t + d, t) & \text{otherwise}
\end{cases}
\]

For example \((s, t) = (100, 102)\) and \( b = 1 \), the difference \( d \) is equal to 2. The modified difference \( d' = 2 \times \lfloor \frac{d}{2} \rfloor + b = 2 \times \lfloor \frac{2}{2} \rfloor + 1 = 3 \). Since \( s \leq t \), the embedded pixel pair becomes \((s', t') = (100, 103)\). If \((s, t) = (103, 100)\) and \( b = 0 \), the difference is \( d' = 2 \times \lfloor \frac{d}{2} \rfloor + b = 2 \times \lfloor \frac{3}{2} \rfloor + 0 = 2 \). Since \( s > t \), the embedded pixel pair becomes \((s', t') = (102, 100)\).

Step 5: On the edge pixels the watermark bits are inserted using DEPD method as explained above.

Step 6: Apply inverse TA to produce watermarked image.

B. Extracting Algorithm

To identify the watermark bit and to maintain disarrangement of the image equally and randomly TA is applied on the watermarked image. The disarranged image is divided into Hierarchical manner with a block size of two. Calculate average for each block \( B_i \), and calculate average of blocks \( \mu \). Consider the block for extracting the watermark if \( \mu \geq B_i \), and identify the diagonal edge pair pixels from extract the binary watermark.

III. EXPERIMENTAL RESULTS

The proposed HETA-DW method is experimented on the cover images of Baboon, Boat, MRI brain, Flower, Lena and Pepper of size 512x512, as shown in Figure 2. The watermark considered for the experiments are logo MGR of size 64x64 as shown in Figure 3. The proposed HETA-DW chosen the parameters \( K, n \) and \( N \) of TA are 11, 256 and 449 respectively.

Table 1 indicates the PSNR and NCC values for the proposed HETA-DW. PSNR values of Table 1 ranges from 48 dB to 49 dB for the considered 6 images for HETA-DW, which means the watermark is almost imperceptible. The NCC value of Table 1 indicates the proposed method shows high imperceptibility. The Figure 4 shows the watermarked images for the proposed scheme.
The proposed HETA-DW method is also tested with various attacks such as Median filter, Cropping, Rotation, Salt and pepper noise, Gaussian noise, JPEG compression, Gaussian blurring, Motion blurring and Sharpening. The watermarked images are cropped with percentage (10%, 15%, 25%), Rotated with (2°, 4°, 6°), adding Gaussian and salt and Pepper noise (10%, 15%, 20%), filtered with a window size of (3x3, 5x5,7x7) median filter, Gaussian Blurring with (1px 2px 3px) and Motion blurring with (10px, 15px, 20px), JPEG compression with (90, 80, 70) and Sharpening (5%, 10%, 15%). The Figure 5 gives the watermarked image under various attacks for the baboon image. Table 2 and Table 3 show the PSNR and NCC values with various attacks on the considered images. From the Table 2, it is clearly evident that the proposed scheme is having an average of PSNR value 43, for all the images even after attacks. This factor indicates the robustness is not degraded for the proposed HETA-DW scheme with attacks. The experimental results of table 3 demonstrate that the average correlation coefficient’s value is 0.7 for all images. This clearly indicates the quality of the watermark image is not at all degraded for any attacks. Figure 6 shows the extracted binary watermark logo image from the different attacks on watermarked images.

## Table 2

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Baboon PSNR(dB)</th>
<th>Boat PSNR(dB)</th>
<th>MRI brain PSNR(dB)</th>
<th>Flower PSNR(dB)</th>
<th>Lena PSNR(dB)</th>
<th>Pepper PSNR(dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Median filter (3x3)</td>
<td>46.35</td>
<td>46.48</td>
<td>46.32</td>
<td>46.27</td>
<td>46.67</td>
<td>46.54</td>
</tr>
<tr>
<td>Median filter (5x5)</td>
<td>45.23</td>
<td>44.76</td>
<td>45.74</td>
<td>44.48</td>
<td>45.38</td>
<td>44.23</td>
</tr>
<tr>
<td>Median filter (7x7)</td>
<td>42.47</td>
<td>42.57</td>
<td>42.27</td>
<td>42.38</td>
<td>42.67</td>
<td>42.43</td>
</tr>
<tr>
<td>Cropping 5%</td>
<td>45.36</td>
<td>45.58</td>
<td>45.85</td>
<td>45.28</td>
<td>45.39</td>
<td>45.63</td>
</tr>
<tr>
<td>Cropping 15%</td>
<td>43.24</td>
<td>43.68</td>
<td>43.28</td>
<td>43.65</td>
<td>43.12</td>
<td>43.76</td>
</tr>
<tr>
<td>Cropping 25%</td>
<td>41.09</td>
<td>40.37</td>
<td>41.74</td>
<td>40.27</td>
<td>41.49</td>
<td>40.24</td>
</tr>
<tr>
<td>Rotate 2°</td>
<td>44.56</td>
<td>44.58</td>
<td>44.27</td>
<td>44.42</td>
<td>44.62</td>
<td>44.73</td>
</tr>
<tr>
<td>Rotate 4°</td>
<td>42.87</td>
<td>43.29</td>
<td>42.34</td>
<td>43.73</td>
<td>42.21</td>
<td>43.13</td>
</tr>
<tr>
<td>Rotate 6°</td>
<td>40.98</td>
<td>40.17</td>
<td>40.85</td>
<td>40.83</td>
<td>40.65</td>
<td>40.67</td>
</tr>
<tr>
<td>Salt and Pepper Noise 10%</td>
<td>45.39</td>
<td>45.39</td>
<td>45.27</td>
<td>45.92</td>
<td>45.49</td>
<td>45.94</td>
</tr>
<tr>
<td>Salt and Pepper Noise 15%</td>
<td>43.56</td>
<td>43.69</td>
<td>43.16</td>
<td>43.11</td>
<td>43.37</td>
<td>43.32</td>
</tr>
<tr>
<td>Salt and Pepper Noise 20%</td>
<td>41.37</td>
<td>41.56</td>
<td>41.48</td>
<td>41.09</td>
<td>41.32</td>
<td>41.84</td>
</tr>
<tr>
<td>Gaussian noise 10%</td>
<td>45.34</td>
<td>44.67</td>
<td>45.93</td>
<td>44.34</td>
<td>45.69</td>
<td>44.84</td>
</tr>
<tr>
<td>Gaussian noise 15%</td>
<td>43.16</td>
<td>42.67</td>
<td>43.37</td>
<td>42.26</td>
<td>43.43</td>
<td>42.25</td>
</tr>
<tr>
<td>Gaussian noise 20%</td>
<td>41.49</td>
<td>40.28</td>
<td>41.28</td>
<td>40.72</td>
<td>41.72</td>
<td>40.84</td>
</tr>
</tbody>
</table>

## Table 3

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Baboon NCC</th>
<th>Boat NCC</th>
<th>MRI brain NCC</th>
<th>Flower NCC</th>
<th>Lena NCC</th>
<th>Pepper NCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Median filter (3x3)</td>
<td>0.90</td>
<td>0.89</td>
<td>0.86</td>
<td>0.87</td>
<td>0.84</td>
<td>0.86</td>
</tr>
<tr>
<td>Median filter (5x5)</td>
<td>0.82</td>
<td>0.84</td>
<td>0.78</td>
<td>0.80</td>
<td>0.81</td>
<td>0.81</td>
</tr>
<tr>
<td>Median filter (7x7)</td>
<td>0.76</td>
<td>0.74</td>
<td>0.72</td>
<td>0.76</td>
<td>0.76</td>
<td>0.75</td>
</tr>
<tr>
<td>Cropping 5%</td>
<td>0.88</td>
<td>0.87</td>
<td>0.83</td>
<td>0.82</td>
<td>0.85</td>
<td>0.87</td>
</tr>
<tr>
<td>Cropping 15%</td>
<td>0.81</td>
<td>0.82</td>
<td>0.78</td>
<td>0.78</td>
<td>0.80</td>
<td>0.82</td>
</tr>
<tr>
<td>Cropping 25%</td>
<td>0.75</td>
<td>0.73</td>
<td>0.69</td>
<td>0.69</td>
<td>0.75</td>
<td>0.74</td>
</tr>
<tr>
<td>Rotate 2°</td>
<td>0.83</td>
<td>0.84</td>
<td>0.82</td>
<td>0.84</td>
<td>0.82</td>
<td>0.82</td>
</tr>
<tr>
<td>Rotate 4°</td>
<td>0.74</td>
<td>0.73</td>
<td>0.73</td>
<td>0.76</td>
<td>0.73</td>
<td>0.75</td>
</tr>
<tr>
<td>Rotate 6°</td>
<td>0.69</td>
<td>0.70</td>
<td>0.71</td>
<td>0.71</td>
<td>0.69</td>
<td>0.69</td>
</tr>
<tr>
<td>Salt and Pepper Noise 10%</td>
<td>0.88</td>
<td>0.84</td>
<td>0.88</td>
<td>0.87</td>
<td>0.87</td>
<td>0.86</td>
</tr>
<tr>
<td>Salt and Pepper Noise 15%</td>
<td>0.78</td>
<td>0.79</td>
<td>0.79</td>
<td>0.79</td>
<td>0.79</td>
<td>0.79</td>
</tr>
</tbody>
</table>
the proposed HETA-DW method with various other methods.

<table>
<thead>
<tr>
<th>Test Images</th>
<th>Bijan G. Mobasseri, et.al</th>
<th>G. Boato, et.al</th>
<th>Proposed HETA-DW scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>25.36</td>
<td>40.1</td>
<td>49.34</td>
</tr>
<tr>
<td>Boat</td>
<td>26.45</td>
<td>40.94</td>
<td>48.76</td>
</tr>
<tr>
<td>MRI brain</td>
<td>25.39</td>
<td>40.23</td>
<td>48.30</td>
</tr>
<tr>
<td>Flower</td>
<td>25.84</td>
<td>39.91</td>
<td>48.30</td>
</tr>
<tr>
<td>Lena</td>
<td>25.87</td>
<td>40.65</td>
<td>49.48</td>
</tr>
<tr>
<td>Pepper</td>
<td>25.34</td>
<td>39.87</td>
<td>46.71</td>
</tr>
</tbody>
</table>

IV. CONCLUSION

The present paper proposed a Hierarchical-Edge based Torus Automorphism (HETA) to build an efficient Digital Watermarking (DWM) system. The TA disarranges the watermark bits equally and randomly before embedding and reconstructing it after extraction. This made the proposed system as more secure and robust to the embedded watermark against several attacks. The propose HETA-DDW method used the hierarchical approach to gain high security over other methods, to increases the payload of the watermarking system and to withstands robustness for common attacks. The proposed HETA-DW used the edge pixels for inserting the watermark because image edges give good information about the image content and edge features are useful to overcome the attacks generated by noise, edge strips and acuity. The edges are evaluated by using DEPD detector. The DEPD edge detector provides better edge information with an advantage of being less sensitive to noise and it is easy to implement. Experimental results show that the proposed HETA-DW scheme is robust to reasonable compression rate while preserving good image quality. The PSNR tables indicated the efficiency and resiliency of the proposed system against various attack like image Cropping, Rotation, Adding Gaussian noise, Median Filtering, Blurring and Motion blurring and image Resizing. From the Table 2, it is clearly evident that the proposed scheme is having an average of PSNR value 43, for all the images even after attacks. This factor indicates the robustness is not degraded for the proposed HETA-DW scheme with attacks. The experimental

A. Comparison of the proposed method with various other methods

Table 4 compares the PSNR values after inserting the watermark without attacks by the proposed HETA-DW method with Bijan G. Mobasseri, et.al method [14] and G. Boato et.al method [15]. Table 4 clearly indicates the HETA-DW outperform the other existing methods. A graph is also plotted in Figure 7 which indicates the comparison of

![Figure 6 Retrieved binary logo images](image-url)

![Figure 7 Comparison graph of the proposed HETA-DW method with various other methods](image-url)
results of Table 3 demonstrate that the average correlation coefficient’s value is 0.7 for all images. This clearly indicates the quality of the watermark image is not at all degraded for any attacks. The proposed watermarking technique preserves robustness to all geometrical transformations. The result indicates the efficacy of the proposed system over the various other existing methods.

ACKNOWLEDGMENT
The authors would like to express their gratitude to Sri K.V.V. Satyanarayana Raju, Founder & Chairman, and Sri K. Sasi Ki-ran Varma, Managing Director, Chaitanya group of Institu-tions for providing necessary Infrastructure. Authors would like to thank the anonymous reviewers for their valuable comments.

REFERENCES