Pi Transform based Blind and Dynamic Digital Image Watermarking Method

Türker TUNCER and Yasin SÖNMEZ

Abstract—To provide copyright protection and image authentication, digital watermarking techniques have been widely used and these techniques have been generally used images as medias. Quantitated index modulation (QIM), Least significant bits (LSB), Chinese remainder theorem (CRT) etc. based methods are used in watermark embedding and watermark extraction sections in the watermarking techniques which are presented in the literature. In this paper, a novel pi transform based watermarking method is presented. The main goal of the pi transform is to find unique indices of the pixel values by the help of the pi and these values are called pi values. In this article, pi values of an image are modified for watermark embedding and watermark extraction. This method consists of pi transform, watermarking list generation, block division, pixel selection by using random number generator, watermark embedding and watermark extraction. Firstly, pi values of the pixels are obtained by using pi transform and the watermarking list is generated by using these pi values of pixels. This list is used for watermark embedding and watermark extraction. Then, the cover image is divided into non-overlapping blocks. 1 x 1, 2 x 2, 4 x 4, 8 x 8, 16 x 16, 32 x 32 and 64 x 64 size of non-overlapping blocks are used in this article. Pseudo Random Number Generator (PRNG) is used to select the pixel which is going to be used for watermark embedding. Logistic-tent system is used as PRNG in this article. The help of watermarking list dynamically programs watermark embedding and watermark extraction steps. Capacity, visual quality, robustness and execution time are used for evaluation of the proposed pi based image watermarking method. The experimental results clearly demonstrated that, the proposed pi based image watermarking method resulted successfully.

Keywords—About four key words or phrases in alphabetical order, separated by commas.

I. INTRODUCTION

Usage of multimedia has been rapidly increased with the introducing cloud technology and social media. Multimediare are widely used not only in cloud technology or social networking, but also distance education, health services, e-government applications, military applications, etc. are used multimedia processing and multimedia transmission. However, due to easy access to multimedia, it can also have disadvantages such as security for multimedia transmission. Especially, there are many advanced software which can be easily manipulated on the images. This may indicate problems such as image authentication and copyright protection. One of the methods used to solve this problem is image watermarking. The main aim of the image watermarking methods is proving originality of the images. The image watermarking methods are classified in active image authentication methods. Image watermarking methods classify as blind, semi-blind and non-blind according to watermark extraction. They classify as spatial, frequency, compression and encrypted according to domain and they classify as fragile, semi-fragile and robust according to robustness. The components of digital watermarking methods are given as follows. The watermark is embedded into cover image. Watermark is used for proving originality of the cover image. Watermark embedding process is used to embed watermark into cover image. The watermark embedding process should be provided high visual quality in a cover image. Some of the watermarking methods use image or watermark encryption but use of the encryption algorithms are optional. These algorithms can be symmetric or asymmetric and these algorithms are used for providing privacy of the watermark. Watermarked image consists of cover image and watermark. Watermark extraction function is used to extract watermark from watermarked image. Briefly, an image watermarking method consists of cover image, watermark, watermark embedding function, watermarked image and watermark extraction function. In the literature, QIM, LSB, CRT, modulo based watermarking etc. methods are generally used in watermarking. Additionally, PRNG, encryption methods, key, etc. are used to provide confidentiality of watermarking method [1-9].

In this article, a novel pi based image watermarking method is proposed. To obtain pi values from pixel values, pi transform is proposed and watermark embedding and watermark extraction processes are applied by using these values. In this study, dynamic programming is used for reducing time complexity of the proposed method. Time complexity of the proposed pi based image watermarking method is O(n2) by the help of dynamic programming. The characteristics of the proposed method are given below:

- The proposed pi transform finds unique value for each of natural numbers in the pi. This is a conjecture but we use only 8 bit numbers and we obtain pi values of the 8 bit numbers by using the proposed transform.
- The proposed pi transform and modulo operator are used to watermark embedding and watermark extraction.
- The proposed method is implemented both pixel wise and
block wise. In the block wise watermarking method, PRNG (Pseudo random number generator) is used to select embedding pixel. Logistic-tent system is used as PRNG in this method.

- The seed values of the logistic-tent system are updated periodically to provide privacy of this PRNG.
- The proposed method can be implemented on both gray scale images and color images.
- Dynamic programming based a new blind watermarking method is proposed in this article.

The rest of the proposed method organized as follows. Related works are mentioned in section 2, the proposed pi transform is described in section 3, in section 4, the proposed pi based image watermarking method is introduced, the experimental results are demonstrated in section 5, finally, conclusions and recommendations are presented in section 6.

II. RELATED WORKS

One of the widely used methods for image authentication, tamper detection and copyright protection is the digital image watermarking. Some watermarking methods that are previously proposed in the literature are cited in this section. These methods are as follows. Walia and Suneja [10] suggested weber law based blind and fragile image watermarking algorithm for medical images. In their study, pixels are classified according to density and watermark was embedded into cover medical image according to determined conditions. Roldan et al. [11] presented an image authentication method by using QIM, DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform). Their method used frequency domain for watermark embedding and watermark extraction and this method has image recovery ability. Multilayer perceptron neural network was used to image recovery. Preda and Vizireanu [12] proposed DCT based watermarking method for image authentication. The main goal of usage DCT was robustness against JPEG compression in their method. El’arbi and Amar [13] offered a watermarking method by using DCT and back propagation neural network. They used DCT for watermark embedding and watermark extraction and 3 layered back propagation neural network is used for tampered areas recovery. Lin et al. [14] proposed an image authentication and verification method by using distributed source code. Patra et al. [15] suggested a block based image authentication method. They used CRT for watermark embedding and extraction in spatial domain. The most important feature of this method is a new watermark embedding function based on CRT. Their method was compared with SVD (Singular Value Decomposition) based watermarking methods and they obtained superior results. Patra et al. [16] presented a digital watermarking method that is robust against JPEG compression attack by applying CRT based watermark embedding method to the DCT coefficients. Shao et al. [17] offered a robust double image watermarking method based on chaotic map and orthogonal Fourier-Mellin moments. Their method consists of image content authentication and image verification stages. In their method, Fourier-Mellin moments were used to feature extraction and chaos is used for scrambling the watermark. Wang and Men [18] proposed a reversible watermarking method. Image watermarking and public key cryptography are used for image authentication and this method uses the active authentication methods in a hybrid way. Huo et al. [19] offered a block based image watermarking method. They used two keys and these keys were used for watermark generation and to select pixel respectively. Wójtowicz and Ogiela [20] proposed a watermarking method to provide privacy of biometrics images and authenticate them. They used multi-modal biometrics system because of they used iris and fingerprint together and they embedded features of these into a face image. Tuncer and Avcı [21] presented a chaotic and block based image watermarking method for image content authentication. They extracted features from images and they used these features as seed values of logistic map. Logistic map was used as PRNG in their method. The generated random numbers were used as watermark and they used ±1 operator to watermark embedding. Qin et al. [22] proposed a fragile watermarking scheme. In their method they used overlapping blocks to tamper detection and image recovery. They presented an embedding strategy to recover tampered areas with high quality. Block wise tampering detection and pixel-wise content restoration were used in their method.

III. THE PROPOSED PI TRANSFORM

The pi number is expression as ratio of a circle’s circumference to circle’s diameter and pi is the most famous mathematically constant throughout history. Many mathematicians such as Archimedes, Zu Chongzhi, Viete, Newton, Euler, Ramanujan etc. worked on pi. The computation of the pi together with the use of the computers has been accelerated and by the help of the computers 13.3 trillion digits of pi were calculated in 2016. All of the natural numbers are existed in the pi according to some mathematicians, but this theorem has not been proven yet [23-28].

The main purpose of the proposed pi transform is to be able to calculate a unique starting index for each number in the pi. To obtain this transform, a new algorithm is developed and pseudo code of the proposed pi transform is demonstrated in Algorithm 1.

### TABLE I. Pi Transform Algorithm

<table>
<thead>
<tr>
<th>Algorithm 1. The proposed pi transform.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong> Pi Digits</td>
</tr>
<tr>
<td><strong>Output:</strong> Obtained pi transform values</td>
</tr>
<tr>
<td>1: <strong>pi_digits</strong> = {3, 1, 4, 1, 5, 9, 2, 6, 5, 3, 5, 8, 9, 7, 9, 3, 2, 3, 8, 4, 6, 2, 6, 4, 3, \ldots};</td>
</tr>
<tr>
<td>2: <strong>counter</strong> = {-1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, \ldots};</td>
</tr>
<tr>
<td>3: cnt=0; i=0;</td>
</tr>
<tr>
<td>4: while(i&lt;length(pi_digits));</td>
</tr>
<tr>
<td>5: value=pi_digits(i);</td>
</tr>
<tr>
<td>6: nod=0; // Number of digits</td>
</tr>
<tr>
<td>7: while(counter(digit)==-1);</td>
</tr>
<tr>
<td>8: array(nod)= pi_digits(i+nod);</td>
</tr>
<tr>
<td>9: nod=nod+1;</td>
</tr>
<tr>
<td>10: if nod&gt;0 then</td>
</tr>
<tr>
<td>11: value=0;</td>
</tr>
<tr>
<td>12: for j=1 to nod do</td>
</tr>
</tbody>
</table>


13: value=value+array(j)*10^nod-j;
14: endif
15: endfor
16: endwhile
17: counter(value)=0;
18: pi_transform(value)=i;
19: if nod=0 then
20:     i=i+1;
21: else
22:     i=i+nod-1;
23: endif
24: endwhile

IV. THE PROPOSED WATERMARKING METHOD

In this paper, a novel image watermarking method based on pi transform is proposed. The proposed pi based image watermarking method consists of 4 sections and these are pi transform, generating watermarking list, watermark embedding and watermark extraction. Firstly, pi transform is implemented which explained in Section 3 for image watermarking. To implement the proposed image watermarking method, dynamic programming is used. This method uses pi coefficients and modulo operator to watermark embedding and watermark extraction. A watermark list is created so that digital watermarking can be applied quickly. By the help of this list, dynamic programming is applied on this method successfully. The biggest advantage of creating the watermarking list is to avoid from performing the cyclic operation for watermark embedding and watermark extraction. The proposed method is provided both block wise image watermarking and pixel wise image watermarking. In the block-based digital watermarking method, a pseudo random number generator (PRNG) is used to select the pixel to be embedded in the watermark. Logistic-tent system is used as PRNG in this method. Eq. 1. describes pi values for creating watermarking list.

\[
\text{piV} = \text{piV}(O(i,j))(\text{mod n}), i = \{1,2,3,\ldots,W\}, j = \{1,2,3,\ldots,H\}
\]  

(1)

\(\text{piV}\) is coefficient of pixel, \(O\) original image, \(n\) is modulo value, \(W\) is width of original image, \(H\) heigh of original image, \(i\) and \(j\) are indices of image. In this method \(n\) is selected 2.

The list contains the nearest pixel values with different piV values. The algorithm of the generating watermarking list is given in Algorithm 2.

**TABLE II. Pseudo code of watermarking list generation Algorithm.**

Input: Coefficients of all pixels, pi_values with size of 1 x 256
Output: Watermark embedding list, wm_list with size of 1 x 256
1: similar=ones(256,2)’-1; // This list stores similar values
2: for i=0 to 255 do
3:     Calculate piV by using Eq.1.
4:     for j=1 to 255 do
5:         if i+j<256 then
6:             if similar(i,1)=i+j then
7:                 similar(i,1)=i+j;
8:             else
9:                 if similar(i,2)=i+j then
10:                   similar(i,2)=i+j;
11:             endif
12:         endif
13:     endif
14: endfor
15: for i=0 to 255 do
16:     if similar(i,1) ≠1 and similar(i,2) ≠1 then
17:         if similar(i,1)=i then
18:             similar(i,1)=closest(i,2);
19:         else if similar(i,2)=i then
20:             similar(i,2)=closest(i,1);
21:         endif
22:     endfor
23: endfor
24: for i=0 to 255 do
25:     if similar(i,1) and similar(i,2) ≠1 then
26:         s1 = |i - similar(i, 1)|;
27:         s2 = |i - similar(i, 2)|;
28:         if s1>s2 then
29:             wm_list(i)= s2;
30:         else
31:             wm_list(i) = s1;
32:         endif
33:     endif
34: endfor
Watermarking list is obtained by using Algorithm 2 and by the help of this algorithm, variable watermarking lists can be generated. Owing to generated list, the proposed watermarking has low time complexity. Steps of the proposed watermarking embedding algorithm are given below.

**Step 1:** Load Cover image and watermark.

**Step 2:** Divide Cover image into non overlapping blocks.

**Step 3:** Select watermark embedding pixel, P, by using PRNG. In this paper Logistic-Tent system is used to generate random number [29]. Equation of Logistic-Tent system is shown in Eq. 2. In this paper, seed values of the Logistic-tent system are updated periodically to provide confidentiality of the PRNG.

\[
x_{i+1} = \begin{cases} 
  \left( \frac{rx_i(1-x_i) + (4-r)x_i}{2} \right) \pmod{1}, & x_i < 0.5 \\
  \left( \frac{rx_i(1-x_i) + (4-r)(1-x_i)}{2} \right) \pmod{1}, & x_i \geq 0.5
\end{cases}
\]

(2)

For \(x_i \in [0,1] \) and \(x_1 \notin [0.25,0.5,0.75] \), \(r \in [0,3.99], \text{if } i \pmod{32} = 0, \text{ if } r + 10^{-10}\)

\(r\) is chaos multiplier, \(x\) is random generated array and \(x_1\) is initial value of this array.

**Step 4:** Modify selected pixel by using Eq. 3.
is selected pixel by using the proposed logistic-tent system. \( WI(i,j) \) is watermarked pixel.

**Step 5:** Repeat steps until size of watermark. The Watermark extraction steps are given below.

**Step 1:** Load watermarked image.

**Step 2:** Generate random number by using seed values.

**Step 3:** Use Eq. 4. to extract watermark.

\[
wm_i j = piT(WI(i,j)) \mod 2
\]  

(4)

**Step 4:** Repeat steps until size of watermark.

Block diagram of the proposed watermarking method is shown in Fig. 2.

The watermarking list is created to provide high visual quality. According to the watermarking list, maximum difference is 5. In this case, the worst PSNR is obtained for 1 x 1 size of blocks. The worst PSNRs of the presented pi transform based watermarking method according to block size are shown in Table 4.

<table>
<thead>
<tr>
<th>Image</th>
<th>1 x 1</th>
<th>2 x 2</th>
<th>4 x 4</th>
<th>8 x 8</th>
<th>16 x 16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>48.12</td>
<td>54.15</td>
<td>60.27</td>
<td>66.27</td>
<td>71.97</td>
</tr>
<tr>
<td>Boat</td>
<td>48.85</td>
<td>54.90</td>
<td>60.89</td>
<td>66.91</td>
<td>72.70</td>
</tr>
</tbody>
</table>

Visual Quality: One of the widely used performance metrics in the image watermarking methods is visual quality. To obtain experiments of the visual quality, MSE (mean square error) (20) and PSNR (peak signal to-noise ratio) (28) are generally used. Mathematical definition of the MSE and PSNR are given Eq. 6 and 7.

\[
MSE = \frac{1}{WH} \sum_{i=1}^{W} \sum_{j=1}^{H} (OI_{ij} - WI_{ij})^2
\]  

(6)

\[
PSNR = 10 \log_{10} \frac{Max(OI^2_{ij})}{MSE}
\]  

(7)

\( OI \) is original image and \( WI \) is watermarked image, \( W \) is width of image and \( H \) is height of image. The obtained PSNR values for variable size of blocks are shown in Table 3.

<table>
<thead>
<tr>
<th>Image</th>
<th>1 x 1</th>
<th>2 x 2</th>
<th>4 x 4</th>
<th>8 x 8</th>
<th>16 x 16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>48.73</td>
<td>54.75</td>
<td>60.80</td>
<td>66.74</td>
<td>72.36</td>
</tr>
<tr>
<td>House</td>
<td>48.78</td>
<td>54.81</td>
<td>60.90</td>
<td>67.01</td>
<td>72.72</td>
</tr>
<tr>
<td>Peppers</td>
<td>48.28</td>
<td>54.32</td>
<td>60.38</td>
<td>66.41</td>
<td>72.54</td>
</tr>
<tr>
<td>F16</td>
<td>48.05</td>
<td>54.06</td>
<td>60.02</td>
<td>66.06</td>
<td>71.95</td>
</tr>
<tr>
<td>Tiffany</td>
<td>46.71</td>
<td>52.71</td>
<td>58.74</td>
<td>64.64</td>
<td>70.66</td>
</tr>
<tr>
<td>Barbara</td>
<td>48.06</td>
<td>54.10</td>
<td>60.13</td>
<td>66.05</td>
<td>72.72</td>
</tr>
</tbody>
</table>

To test performance of the pi based image watermarking method, PSNR values of the proposed method are compared with PSNR values of the previously presented method in the literature. We compared with 8 x 8 size of blocks because of 8 x 8 size of blocks are generally used in literature. Comparison results are shown in Table 5.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>55.89</td>
<td>48.09</td>
<td>66.27</td>
</tr>
<tr>
<td>Boat</td>
<td>55.98</td>
<td>51.13</td>
<td>66.91</td>
</tr>
<tr>
<td>Elaine</td>
<td>56.21</td>
<td>55.23</td>
<td>66.74</td>
</tr>
<tr>
<td>House</td>
<td>56.05</td>
<td>57.89</td>
<td>67.01</td>
</tr>
<tr>
<td>Lena</td>
<td>56.12</td>
<td>53.94</td>
<td>66.05</td>
</tr>
<tr>
<td>Peppers</td>
<td>56.22</td>
<td>54.60</td>
<td>66.41</td>
</tr>
<tr>
<td>F16</td>
<td>55.98</td>
<td>54.89</td>
<td>66.06</td>
</tr>
<tr>
<td>Tiffany</td>
<td>56.07</td>
<td>56.31</td>
<td>64.64</td>
</tr>
<tr>
<td>Barbara</td>
<td>55.64</td>
<td>52.61</td>
<td>66.05</td>
</tr>
</tbody>
</table>

Robustness: To measure robustness of the pi based image watermarking algorithm, various attacks are applied on the watermarked image in this section. These are average filtering attack, median filtering attack, JPEG compression attack, rescaling attack, cropping attack, speckle noise attack, sharpening attack and salt and pepper noise attack. These attacks are applied on pixel wise watermarked images. In this article, normalized cross correlation (NCC) is used for measuring robustness. Eq. 8. describes mathematical model of NCC.

\[
NCC = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{WM_{i,j} \oplus WM'_{i,j}}{MN}
\]  

(8)

\( WM \) is watermark, \( WM' \) is attacked watermarked, \( M \) is width of watermark and \( N \) is height of watermark.
The watermark is used for measuring robustness is shown in Fig. 4.

![Fig. 4. Watermark logo.](image)

The obtained NCC values are given in Table 5.

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>NCC Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG compression (QF=50)</td>
<td>0.8312</td>
</tr>
<tr>
<td>Rescaling (512 → 256 → 512)</td>
<td>0.4618</td>
</tr>
<tr>
<td>Cropping (%25)</td>
<td>0.8984</td>
</tr>
<tr>
<td>Speckle noise (0.0001)</td>
<td>0.6459</td>
</tr>
<tr>
<td>Sharpening attack</td>
<td>0.9949</td>
</tr>
</tbody>
</table>

**Execution Time:** The pi based image watermarking method is dynamically programmed. To coding dynamically of the proposed pi based image watermarking method, a watermarking list has to be obtained. To obtain watermarking list, it is sufficient to run the Pi Transform given in Algorithm 1 and the generating watermarking list given in Algorithm 2. After obtaining the watermarking list, watermark embedding and watermark extraction processes can be performed quickly. 256 x 256, 512 x 512, 256 x 256 x 3 and 512 x 512 x 3 size of images are used for obtaining experiments of the execution time. The recommended method is using MATLAB 2013a program on a laptop computer with 4 GB RAM and i7 4370 processor with Windows 10 operating system. The watermark embedding times and watermark extraction times are shown in Table 7 and Table 8.

**VI. CONCLUSIONS**

In this study, a novel image watermarking method based on pi transform is proposed. This method consists of Pi transform, generating watermarking list, block division, pixel selection by using secure PRNG (this is for block based method), watermark embedding and watermark extraction phases. The basic philosophy of this study is the theory that pi is the host all of the natural numbers. We cannot prove this theory in infinite space but the proposed method uses pixel values of images are in the finite field. Therefore, the proposed pi transform obtains unique values for each of the pixel values and the pi coefficients of the pixel values are obtained by using the proposed pi transform. To provide uniform distribution, modulo operators are used. Watermarking list is generated by using this transform. Watermark embedding and watermark extraction processes use the watermarking list. The help of the watermarking list applies dynamic programming applied on the proposed pi based image watermarking method. In addition, pi transform based image watermarking method can be applied on block wise and pixel wise. In the block wise method, logistic-tent system that is a chaotic map select watermarked pixel. Capacity, visual quality, robustness and execution time are used for evaluated performance of the suggested method. The experimental results have demonstrated that the presented image watermarking method has high capacity, high visual quality and lower time complexity. In robustness test, the pi based image watermarking is not robust. Therefore, the proposed pi based image watermarking method can be used as image authentication method.

In the future studies, SVD, DCT, DWT etc. methods will be used with the proposed method for developing more robust image watermarking methods. In addition, the proposed pi transform will be used in other disciplines. Also, the proposed pi based image watermarking method clearly demonstrated that the other methods can be programmed by using dynamic programming.
REFERENCES


Türker TUNCER was born in Elazığ, Turkey, in 1986. He received the B.S. degree from the Firat University, Technical Education Faculty, Department of Electronics and Computer Education in 2009, M.S. degree in telecommunication science from the Firat University in 2011 and Ph.D. degree department of software engineering at Firat University in 2016. He works as research assistant Digital Forensic Engineering, Firat University. His research interests include data hiding, image authentication, cryptanalysis, cryptography, image processing. turkertuncer@firat.edu.tr

Yasin Sönmez received the master graduated in computer science from University Firat, Turkey in 2012. He is currently Phd student in software engineering, end working for the computer technology at the University of Dicle. His research interests include Computer vision and video analysis. yasin.sonmez@dicle.edu.tr