

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. 1×1 , 2×2 , 4×4 , 8×8 , 16×16 , 32×32 and 64×64 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. Multimedia 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 $O(n^2)$ 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 pi based image watermarking method is presented for the first time in the literature.
- The proposed pi transform and modulo operator are used to watermark embedding and watermark extraction.
- The proposed method is implemented both pixel wise and

Manuscript received Feb. 26, 2018 Dr. Türker Tuncer. is now with the Firat University, Elazığ, Turkey

Phd. Yasin Sönmez. is now with the Dicle University, Diyarbakır, Turkey


```

13:     value=value+array(j)*10nod-j;
14:     endfor
15:   endif
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.

$$piV = piT(OI(i,j))(mod n), i = \{1,2,3,...,W\}, j = \{1,2,3,...,H\} \quad (1)$$

piV is coefficient of pixel, OI original image, n is modulo value, W is width of original image, H is height 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 pi 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:       new_value = piT(i + j)(mod 2)
7:       if new_value ≠ piV then

```

```

8:         similar(i,1)=i+j;
9:         break;
10:      endif
11:    endif
12:  endfor
13:  for j=1 to 255 do
14:    if i-j>-1 then
15:      new_value = piT(i - j)(mod 2)
16:      if new_value ≠ piV then
17:        similar(i,2)=i-j;
18:        break;
19:      endif
20:    endif
21:  endfor
22: endfor
23: for i=0 to 255 do
24:   if similar(i,1) ≠ -1 and similar(i,2) ≠ -1
25:     s1 = |i - similar(i,1)|;
26:     s2 = |i - similar(i,2)|;
27:     if s1 > s2 then
28:       wm_list(i)= s2;
29:     else
30:       wm_list(i)= s1;
31:     endif
32:   elseif similar(i,1)=-1
33:     wm_list(i)= similar(i,2);
34:   elseif similar(i,2)=-1
35:     wm_list(i)= similar(i,1);
36:   endif
37: 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.

$$x_{i+1} = \begin{cases} \left(rx_i(1-x_i) + \frac{(4-r)x_i}{2} \right) (mod 1), x_i < 0.5 \\ \left(rx_i(1-x_i) + \frac{(4-r)(1-x_i)}{2} \right) (mod 1), x_i \geq 0.5 \end{cases} \quad (2)$$

$x_1 \in (0,1)$ and $x_1 \neq \{0.25, 0.5, 0.75\}$
 $r \in (0, 3.99]$, if $i (mod 32) = 0$, $r = r + 10^{-10}$

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.

$$\text{if } wm_{ij} \neq (\text{piT}(OI(i,j)) \bmod 2), WI(i,j) = wm_list(OI(i,j)) \quad (3)$$

$OI(i,j)$ 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.

$$wm_{ij} = \text{piT}(WI(i,j)) \bmod 2 \quad (4)$$

Step 4: Repeat steps until size of watermark.

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

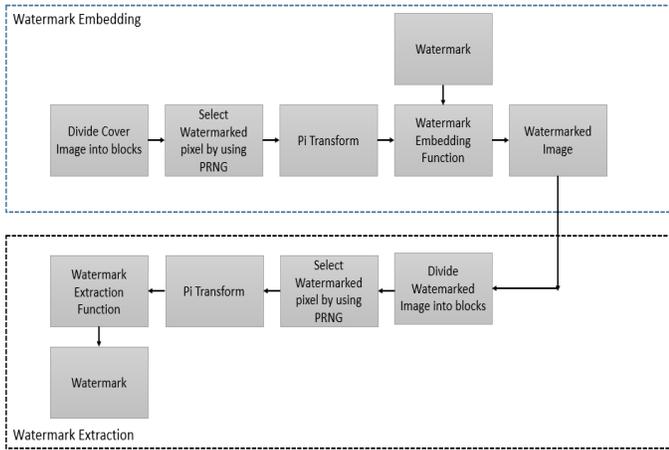


Fig 2. Block diagram of the proposed method.

V. EXPERIMENTAL RESULTS

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.

$$MSE = \frac{1}{WH} \sum_{i=1}^W \sum_{j=1}^H (OI_{ij} - WI_{ij})^2 \quad (6)$$

$$PSNR = 10 \log_{10} \frac{\text{Max}(OI_{ij}^2)}{MSE} \quad (7)$$

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 III. PSNR (dB) values of the variable size of blocks.

Image	1 x 1	2 x 2	4 x 4	8 x 8	16 x 16
Baboon	48.12	54.15	60.27	66.27	71.97
Boat	48.85	54.90	60.89	66.91	72.70

Elaine	48.73	54.75	60.80	66.74	72.36
House	48.78	54.81	60.90	67.01	72.72
Lena	47.81	53.93	60.06	66.05	71.56
Peppers	48.28	54.32	60.38	66.41	72.54
F16	48.05	54.06	60.02	66.06	71.95
Tiffany	46.71	52.71	58.74	64.64	70.66
Barbara	48.06	54.10	60.13	66.05	72.72

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

$10 \log_{10} \left(\frac{255^2}{5^2} \right) = 34.15$ 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 IV The worst PSNR values of the pi transform based watermarking method according to size of blocks.

	1 x 1	2 x 2	4 x 4	8 x 8	16 x 16
PSNR	34.15	40.17	46.19	52.21	58.23

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 V: Comparison of PSNR values of the proposed method with other methods.

Images	Patra et al.'s method [15]	Abdelhakim et al.'s method [30]	The Proposed Method
Baboon	55.89	48.09	66.27
Boat	55.98	51.13	66.91
Elaine	56.21	55.23	66.74
House	56.05	57.89	67.01
Lena	56.12	53.94	66.05
Peppers	56.22	54.60	66.41
F16	55.98	54.89	66.06
Tiffany	56.07	56.31	64.64
Barbara	55.64	52.61	66.05

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.

$$NCC = \sum_{i=1}^M \sum_{j=1}^N \frac{WM_{ij} \oplus WM'_{ij}}{MN} \quad (8)$$

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.

The obtained NCC values are given in Table 5.

TABLE VI: NCC values of the proposed method.

average filtering (3 x 3)	median filtering (3 x 3)	JPEG compression attack (QF=50)	Rescaling (512 →256 → 512)	cropping attack (%25)	speckle noise (0.0001)	sharpening attack	Salt and pepper attack (0.01)
0.5484	0.9819	0.5379	0.4618	0.8312	0.8894	0.6459	0.9949

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.

TABLE VII: Watermark Embedding time of the proposed method (milisecond)

	1 x 1	2 x 2	4 x 4	8 x 8	16 x 16
256 x 256	13.30	3.76	0.97	0.29	0.13
512 x 512	54.27	16.61	8.34	6.40	7.02
256 x 256 x 3	32.91	12.77	6.79	5.54	5.14
512 x 512 x 3	138.11	43.35	26.16	12.70	9.21

TABLE VIII: Watermark extraction time of the proposed method (milisecond)

	1 x 1	2 x 2	4 x 4	8 x 8	16 x 16
256 x 256	13.62	6.83	5.11	4.84	4.60
512 x 512	85.92	18.57	4.23	1.31	0.47
256 x 256 x 3	45.45	10.97	3.94	0.86	0.26
512 x 512 x 3	361.98	55.94	17.64	3.89	1.05

Also, secure pseudo random number generators are used to provide confidentiality of the proposed method. In this article, logistic tent map is used.

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 diciplines. Also, the proposed pi based image watermarking method clearly demonstrated that the other methods can be programmed by using dynamic programming.

REFERENCES

- [1] Y. Xiang, S. Guo, W. Zhou, S. Nahavandi, Patchwork-based audio watermarking method robust to de-synchronization attacks, *IEEE/ACM Trans. Audio Speech Lang. Process.* 22 (9) (2014) 1413–1423. <https://doi.org/10.1109/TASLP.2014.2328175>
- [2] A. Akter, N. E-Tajjina, M.A. Ullah, Digital image watermarking based on DWT-DCT: evaluate for a new embedding algorithm, in: *Third Int. Conf. On Informatics, Electronics & Vision*, May 2014, Dhaka, Bangladesh, 2014, pp. 1–6.
- [3] Q. Su, Y. Niu, Q. Wang, G. Sheng, A blind color image watermarking based on DC component in the spatial domain, *Optik* 124 (23) (2013) 6255–6260. <https://doi.org/10.1016/j.ijleo.2013.05.013>
- [4] J. Lang, Z.-G. Zhang, Blind digital watermarking method in the fractional Fourier transform domain, *Opt. Lasers Eng.* 53 (2014) 112–123. <https://doi.org/10.1016/j.optlaseng.2013.08.021>
- [5] M. Ali, C.W. Ahn, An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain, *Signal Processing*, 94, 2014, pp. 545–556. <https://doi.org/10.1016/j.sigpro.2013.07.024>
- [6] S. Dadkhah, A. A. Manaf, Y. Hori, A. E. Hassanien, S. Sadeghi, An effective SVD-based image tampering detection and self-recovery using active watermarking, *Signal Processing: Image Communication*, 29, 10, 2014, pp. 1197–1210.
- [7] L. Gao, L. Qi, Y. Wang, E. Chen, S. Yang, L. Guan, Rotation invariance in 2D-FRFT with application to digital image watermarking. *Journal of Signal Processing Systems*, 72(2), 2013, pp. 133–148. <https://doi.org/10.1007/s11265-012-0722-2>
- [8] S. Rawat, B. Raman, A blind watermarking algorithm based on fractional Fourier transform and visual cryptography, 92, 6, 2012, pp. 1480–1491.
- [9] R. Christian, D. Jean-Luc, A survey of watermarking algorithms for image authentication, *EURASIP J. Appl. Signal Process.*, 6, (2002), pp. 613–621.
- [10] E. Walia, A. Suneja, Fragile and blind watermarking technique based on Weber's law for medical image authentication, *IET Computer Vision*, Vol. 7, Iss. 1, (2013), pp. 9–19. <https://doi.org/10.1049/iet-cvi.2012.0109>
- [11] L. R. Roldan, M. C. Hernández, J. Chao, M. N. Miyatake, H. P. Meana, Watermarking-based Color Image Authentication with Detection and Recovery Capability, *IEEE LATIN AMERICA TRANSACTIONS*, VOL. 14, NO. 2, (2016).
- [12] R.O. Preda, D.N. Vizireanu, Watermarking-based image authentication robust to JPEG compression, *Electronics Letters*, Vol. 51, No. 23, (2015), pp. 1873–1875. <https://doi.org/10.1049/el.2015.2522>
- [13] M. El'arbi, C. B. Amar, Image authentication algorithm with recovery capabilities based on neural networks in the DCT domain, *IET Image Processing*, Vol. 8, Iss. 11, (2014), pp. 619–626. <https://doi.org/10.1049/iet-ipr.2013.0646>
- [14] Y.-C. Lin, D., Varadayan, B. Girod, Image Authentication Using Distributed Source Coding, *IEEE TRANSACTIONS ON IMAGE PROCESSING*, VOL. 21, NO. 1, (2012), pp. 273–283. <https://doi.org/10.1109/TIP.2011.2157515>
- [15] J. C. Patra, A. Kathik, C. Bornand, A novel CRT-based watermarking technique for authentication of multimedia contents, *Digital Signal Processing*, 20, (2010), 442–453. <https://doi.org/10.1016/j.dsp.2009.07.004>
- [16] J. C. Patra, J. E. Phua, C. Bornand, (2010). A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, *Digital Signal Processing*, 20, 1597–1611 <https://doi.org/10.1016/j.dsp.2010.03.010>
- [17] Z. Shao, Y. Shang, Y. Zhang, X. Liu, G. Guo, Robust watermarking using orthogonal Fourier–Mellin moments and chaotic map for double images, *Signal Processing*, 120, (2016), pp. 522–531. <https://doi.org/10.1016/j.sigpro.2015.10.005>
- [18] N. Wang, C. Men, Reversible fragile watermarking for 2-D vector map authentication with localization, *Computer-Aided Design* 44, (2012), pp. 320–330. <https://doi.org/10.1016/j.cad.2011.11.001>
- [19] Y. Huo, H. He, F. Chen, Alterable-capacity fragile watermarking scheme with restoration capability, *Optics Communications* 285, (2012), pp. 1759–1766. <https://doi.org/10.1016/j.optcom.2011.12.044>
- [20] W. Wójtowicz, M. R. Ogiela, Digital images authentication scheme based on bimodal biometric watermarking in an independent domain, *J. Vis. Commun. Image R.* 38, (2016), pp. 1–10. <https://doi.org/10.1016/j.jvcir.2016.02.006>
- [21] T. Tuncer, E. Avci, Block Based Fragile Watermarking Algorithm For Image Authentication and Tamper Detection, 9th International Conference on Information Security and Cryptology (ISCTURKEY 2016), pp. 5–10, 2016.
- [22] C. Qin, P. Ji, X. Zhang, J. Dong, J. Wang, Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy, *Signal Processing*, 138, (2017), 280–293. <https://doi.org/10.1016/j.sigpro.2017.03.033>
- [23] L. Berggren, J. Borwein, P. Borwein, A source book, Springer-Verlag, New York, 1997. <https://doi.org/10.1007/978-1-4757-2736-4>
- [24] R. Preston, Mountains of Pi, *New Yorker* 68, 36–67, 1992.
- [25] E. W. Weisstein, “Pi” From Mathworld – a Wolfram Web Resource, mathworld.wolfram.com/Pi.html, (Last Access Date: 18/04/2017).
- [26] A. J. Yee, A Multi-Threaded Pi-Program, www.numberworld.org/y-cruncher/, (Last Access Date: 18/04/2017).
- [27] J. M. Borwein, The Life of Pi: From Archimedes to Eniac and Beyond, www.carma.newcastle.edu.au/jon/pi-2010.pdf, 2011.
- [28] P. Trueb, Digit Statistics of the First π Trillion Decimal Digits of π , arxiv.org/ftp/arxiv/papers/1612/1612.00489.pdf, 2016.
- [29] Y. Zhou, L. Bao, C.L.P. Chen, Image encryption using a new parametric switching chaotic system, *Signal Processing*, (2014), pp. 1–21.
- [30] A. M. Abdelhakim, H. I. Saleh, A. M. Nassar, A quality guaranteed robust image watermarking optimization with Artificial Bee Colony, *Expert Systems With Applications*, 72, (2017) ,317–326. <https://doi.org/10.1016/j.eswa.2016.10.056>



Türker TUNCER was born in Elazığ, Turkey, in 1986. He received the B.S. degree from the Fırat University, Technical Education Faculty, Department of Electronics and Computer Education in 2009, M.S. degree in telecommunication science from the Fırat University in 2011 and Ph.D. degree department of software engineering at Fırat University in 2016. He works as research assistant Digital Forensic Engineering, Fırat 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 Fırat, 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