A Novel Data Hiding Method based on Edge Detection and 2^k Correction with High Payload and High Visual Quality

T. TUNCER, Y.SÖNMEZ

Abstract— In this paper a novel edge adaptive data hiding method is proposed. The proposed edge adaptive steganography method is improved version of the Bai et al.'s [31] (A high payload steganographic algorithm based on edge detection) method. The main aim of the proposed method is to achieve high payload with high visual quality. This method consists of preprocessing, edge detection, classification of the secret data, data embedding and data extraction phases. In the preprocessing phase 6 and 7 least significant bits (LSB) elimination are applied on the cover image to get a better edge detection in the next phase. As edge detection methods Sobel, Canny, Laplacian Of Gaussian (LOG), block-based edge detection and hybrid edge detectors are used. After the edge detection, secret data is divided into 2 classes and then these are embedded into edge pixels and texture pixels of the image. In order to increase the visual quality 2k correction is applied on the stego images. Modulus operator is utilized in the data extraction phase. In the experimental results, payload and visual quality measurements demonstrated the success of the proposed method.

Index Terms— Least Significant Bit (LSB) substitution; 2^k correction; Edge Detection; Data hiding

I. INTRODUCTION

THE ERA we live in is called information era. The vast majority of information is stored as digital media. As a results the information security has become a very important research topic in order to provide security of digital media, thus information security has become a hot-topic research area [1]. In the information security, cryptography and data hiding are widely used. While cryptography provides the confidentiality of digital data, aim of the data hiding is to provide security of the communication. Recently, data hiding has gained popularity over cryptography and started to appear more often in the literature [2-4]. Data hiding methods generally use spatial domain and frequency domain for data embedding.

TÜRKER TUNCER, is with Department of Digital Forensic Engineering of Firat University, Elazig, Turkey, (e-mail: turkertuncer@firat.edu.tr).

https:// orcid.org/0000-0002-1425-4664

YASIN SÖNMEZ, is with technical sciences vocational high school of Dicle University, Diyarbakir, Turkey, (e-mail: yasin.sonmez@dicle.edu.tr).

D https://orcid.org/0000-0001-9303-1735

Manuscript received June 2, 2019; accepted July 11, 2019. DOI: 10.17694/bajece.573514 Spatial domain based data hiding methods have shorter execution time, higher embedding Capacity and higher visual quality but these methods are not robust. In order to increase the robustness of the data hiding method, frequency domain is used [5-8]. In frequency domain, Discrete Wavelet Transform (DWT) [9], Integer Wavelet Transform (IWT) [10], Discrete Cosine Transform (DCT) [11,12], Discrete Fourier Transform (DFT) [13], etc. are used as transformation functions. Data hiding algorithms generally consist of host image, secret data, data hiding, stego image and data extraction. In addition to these basic components, cryptography, frequency transforms, heuristic optimization techniques, edge detectors, segmentation algorithms, secret sharing, visual cryptography, game rules, etc. are widely used in data hiding [14-20]. The most popular data hiding method is Least Significant Bit (LSB) substitution [21]. LSB is a practical method because LSB provides higher visual quality, higher payload Capacity and shorter execution times. Thus, LSB is the widely used method in the data hiding. Some of the previously presented data hiding methods are given as follows. Mahato et al. [22] presented a data hiding method based on the popular minesweeper game for secure communication. The authors generated a scenario for secure communication where the sender plays minesweeper game to embed the secret data and then he/she sends the game to the receiver. The secret message can be extracted from the received game-play. Liao et al. [23] suggested a data hiding method for medical images. To increase robustness against JPEG compression of this method DCT was used. Shiu et al. [24] proposed a reversible signal data hiding for physiological signals. They analyzed this method theoretically and they showed that this algorithms computational complexity is O(n) and this method can be used for ECG and EMG signals. Yuan [25] suggested a secret sharing based image data hiding method with high visual quality. In this method, firstly secret sharing was used to generate minimal distorted secret shares and these secret shares were embedded into multi cover images by using LSB. Wu and Tsai [26] described a data hiding concept based on pixel value difference (PVD). In this method, cover image was divided into non-overlapping blocks and 2 connected pixels differences was modified for data hiding. Subhedar and Mankar [27] proposed a robust QR factorization based data hiding. To evaluate of this method, they used robustness and visual quality performance metrics. Maheswari and Hemanth [28] proposed a Fresnelet Trasform (FT) and QR code based

data hiding method. They utilized LSB as data hiding function. FT and QR coding provided robustness. Chen et al. [29] suggested a hybrid edge detector based data hiding method. Hybrid edge detector utilized Gaussian filter and sobel matrix. Capacity and visual quality was used to evaluate performance of this method. Tseng and Leng [30] proposed an extended edge based data hiding method to achieve minimal distortion. This method was a block based method and they calculate Mean Square Error (MSE) for each 4 x 4 blocks. Bai et al. [31] suggested an edge detection based image data hiding algorithm with high payload Capacity. This method consisted of 5LSBs elimination, edge detection by using Canny [32], Sobel [33] and Fuzzy Logic Edge Detector (FLED) [34], secret message classification in two sub-class, data hiding and data extraction phases. Capacity and visual quality were used to evaluate performance of this method. Sun [35] presented a edge based image data hiding method. In this method, Canny Edge Detector (CED) was used for edge detection, Huffman was used for secret data compression and 2k correction was used for data hiding and data extraction.

In this method, we proposed a novel edge adaptive data hiding method. This method consists of mLBSs elimination, edge detection, secret data classify, data hiding and data extraction phases. In this method, LSB is used for data hiding and data extraction. Briefly, the proposed method is an improved version of Bai et al.'s [31] method. The main aim of the proposed method is to provide higher payload with higher visual quality than Bai et al.'s [31] method. Technical contributions of the proposed method are given below.

mLSBs elimination is used for achieving high payload Capacity. Bai et al.'s [31] used 5LSBs elimination in order to increase Capacity. In this method, we used mLSBs elimination $(m \in \{6,7\})$ to find more edge pixel. A block based edge detector is presented in this paper. In this edge detector, OTSU [36] method and 2 x 2 non-overlapping blocks are used. This method detects edge pixel in the binary form.

A hybrid edge detector is proposed in this paper to achieve high payload Capacity. This detector uses Canny, Sobel, Laplacian of Gaussian and the proposed block based edge detectors. The main aim of the HED is to detect all of the edge pixels in an image. In this method, edge detectors are used for creating data hiding map. By using this map, secret data is divided into x and y classes. xLSBs and yLSBs data embedding method are used as data embedding function. To achieve high visual quality, 2^k correction is applied on the stego image. By using 2^k correction, higher visual quality is achieved than Bai et al.'s method.

II. PROPOSED EDGE DETECTOR

Canny, Sobel and LOG methods are used in this paper for known edge detection methods. In addition to these methods, a block based edge detection method which is a modified version of the FLED method and a hybrid edge detection method are used.

Block based Edge Detection (BED): This method is a modified version of the Fuzzy Logic Edge Detector (FLED) method. In this method, OTSU thresholding method, 2 x 2 size of non-overlapping blocks and a rule table are used. This

method detects edges of binary form of the images. The steps of the proposed edge extraction algorithm are as follows.

- **Step 1:** Convert binary image to original image by using OTSU threshold method.
- Step 2: Divide binary image into 2 x 2 size of nonoverlapping blocks. A sample 2 x 2 size of block is shown in Fig. 1.





• Step 3: Detect edges by using Eq. 1.

$$Edge = \begin{cases} 0, \sum_{i=1}^{4} p_i = 4 \text{ or } \sum_{i=1}^{4} p_i = 0\\ 1, Otherwise \end{cases}$$
(1)

Hybrid Edge Detection (HED): Many edge detection methods are proposed in the literature. These methods yield different edge properties of images and edge detectors used in the literature have weak and superior features against each other. This has led to the development of an edge detection method that can obtain all edge data in the image. In this article, a hybrid edge detector which uses the widely used edge detection methods is proposed and this edge detector can obtain more edge information from the image. The main purpose of this method is to increase the Capacity of the edge based data hiding method by obtaining more edge information. BED, Canny, Sobel and LOG edge removal operators are used in this method. The steps of the HED is given in Eq. 2-6.

- C = Edge (I, 'Canny')(2)
- S = Edge (I, 'Sobel')(3)
- L = Edge (I, 'LOG')(4)
- B = Edge (I, 'BED')(5)
- $H = C \oplus S \oplus L \oplus B \tag{6}$

Where C is edge image using canny edge detector, S is edge image using sobel edge detector, L is edge image using LoG edge detector, B is edge image using binary edge detector, \oplus is OR operator and H is edge image using hybrid edge detector.

III. THE PROPOSED EDGE ADAPTIVE DATA HIDING METHOD

Capacity and visual quality are the most important evaluation criteria in edge detection based data hiding methods [29-32]. In this study, a novel edge detection based data hiding method is proposed to improve Bai et al.'s [31] method. In this article, edge detection is used as data hiding map. To increase capacity, mLSBs elimination and a new hybrid edge detector are used together and the proposed hybrid edge extractor uses Sobel, Canny, LOG and the block-based edge extraction algorithm. To provide high visual quality, 2^{k} correction [35] method is used. The proposed method generally consists of preprocessing, edge detection, secret data classification, data hiding and data extraction phases. Flowchart of the proposed method is shown in Fig. 2.



Fig. 2. Flow diagram of the proposed method.

Pre-processing, secret data classification and data embedding steps of the proposed edge based data hiding method are given below.

- Step 1: Load image
- Step 2: Set 0 to mLSBs by using Eq. 7. This step • describes pre-processing phase of the proposed method

$$I = \left| \frac{I}{2^m} \right| \times 2^m, 5 < m < 8 \tag{7}$$

- Step 3: Apply edge detectors onto image. Edge image • is used for secret data classification and data embedding.
- Step 4: Classify secret data using edge image. If pixel • is edge, xLSBs secret data is embedded into the cover image. Otherwise, yLSBs secret data is embedded into the cover image. Eq. 8. mathematically describes the

presented data embedding function. Where OP is original pixel, SP is stego pixel and SD is secret data.

$$SP = \begin{cases} \left| \frac{OP}{2^x} \right| \times 2^x + SD, if \ OP = edge \\ \left| \frac{OP}{2^y} \right| \times 2^y + SD, if \ OP \neq edge \end{cases}$$
(8)

Step 5: Apply 2k correction to increase visual quality on the stego image. Mathematical description of the 2k correction is shown in Eq. 9 [35].

$$NSP = \begin{cases} SP - 2^{k}, if \ SP - 0P > 2^{k-1} and \ SP - 2^{k} \ge 0\\ SP + 2^{k}, if \ SP - 0P < -2^{k-1} and \ SP + 2^{k} \le 255\\ SP, 0 therwise \end{cases}$$
(9)

Where NSP is new stego pixel and data hiding function is kLSBs. If you use xLSBs data hiding function, k is x. If you use yLSBs data hiding function, k is y. The data extraction steps of the proposed edge adaptive data hiding methods are given below.

- Step 1: Load stego image.
- Step 2: Set 0 to mLSBs by using Eq. 7.
- Step 3: Apply edge detector to stego image. We use edge image as data extraction map.
- Step 4: If pixel value is edge, use Eq. 10. to data extraction. Where ED is extracted data.
 - $ED = NSP \pmod{2^x}$ (10)
- **Step 5:** If pixel value is not edge, use Eq. 11. to data extraction. E

$$D = NSP \ (mod \ 2^{y}) \tag{11}$$

IV. EXPERIMENTAL RESULTS

In this section, payload (also called Capacity) and visual quality (also called imperceptibility) are utilized to evaluate performance of the recommended method. Tseng and Leng's [30], Chen et al.'s [29] and Bai et al.'s [31] methods are used to obtain comparisons.

Capacity: One of the commonly used measurement criteria of the steganography. To evaluate edge adaptive data hiding methods is Capacity. In this method, mLSBs elimination and a hybrid edge detector are used for increasing the payload. In addition to, Canny, Sobel, LOG and BED edge detectors are applied on the test images to obtain experiments. The mathematical description of the Capacity of the proposed method is given in Eq. 12.

$$PC = \frac{(NE \times x) + (W \times H - NE) \times y}{W \times H}$$
(12)

Where PC is payload and bit per-pixel (bpp) is used to expression it, NE is number of edge pixels, W is width of image and H is height of image. Fig. 3 shows number of edge pixels by Canny, Sobel, LOG, BED and HED edge detectors.

Edge Detector	mLSBs Elimination	R		H		
Canny	No	1779	1833		1772	2153
	Yes m=6	2114	2374	2523	2499	2568
Sobel	No	669	827	673	927	862
	Yes m=7	1290	1433	1189	0 1169	
LOG	No	1143	1243	1637	1438	1439
	Yes m=6	1468		2042	1874	1637
BED	No	1061	2147	2133	2583	2636
	Yes m=6	1561	2415	2809	1799	3001
HED	No	3032	3735	4414	4299	4723
	Yes	4349	5305	5897	5161	5782

Fig. 3. The number of edge pixels by used edge detectors with test images 'Lena', 'Peppers', 'Goldhill', 'Boat' and 'Barbara'.

Fig. 3 shows that the mLSBs elimination method generally increases the Capacity. Additionally, Eq. 12 clearly showed that FLED Capacity of the Bai et al.'s [31]

method was incorrectly calculated and true payloads of the FLED and HED are shown in Table 1.

Image	FLED (Bai et al.'s [31] method)	HED (The proposed method)		
	x=2, y=1 Payload=1.2072 bpp	x=2, y=1 Payload=1.2654 bpp		
15	x=3, y=2 Payload=2.2072 bpp	x=3, y=2 Payload=2.2654 bpp		
Lena	x=4, y=3 Payload=3.2072 bpp	x=4, y=3 Payload=3.2654 bpp		
10.1	x=2, y=1 Payload=1.2089 bpp	x=2, y=1 Payload=1.3238 bpp		
	x=3, y=2 Payload=2.2089 bpp	x=3, y=2 Payload=2.3238 bpp		
Peppers	x=4, y=3 Payload=3.2089 bpp	x=4, y=3 Payload=3.3238 bpp		
The second	x=2, y=1 Payload=1.2133 bpp	x=2, y=1 Payload=1.3599 bpp		
H H	x=3, y=2 Payload=2.2133 bpp	x=3, y=2 Payload=2.3599 bpp		
Goldhill	x=4, y=3 Payload=3.2133 bpp	x=4, y=3 Payload=3.3599 bpp		
INK)	x=2, y=1 Payload=1.2197 bpp	x=2, y=1 Payload=1.3150 bpp		
	x=3, y=2 Payload=2.2197 bpp	x=3, y=2 Payload=2.3150 bpp		
Boat	x=4, y=3 Payload=3.2197 bpp	x=4, y=3 Payload=3.3150 bpp		

TABLE I

COMPARTIVELY RESULTS OF THE PROPOSED METHOD AND BAI ET AL.'S [31] METHOD FOR 128 X 128 SIZE OF IMAGES.

Table 1 clearly demonstrates that the proposed HED provides superior payload than FLED of Bai et al.'s [31] method. *Visual Quality:* Peak Signal Noise-to-Raito (PSNR) was used to measure visual quality in this model. The mathematical definition of PSNR is Eq. 13.

$$PSNR = 10 \times \log_{10}(\frac{255^2 \times W \times H}{\sum_{i=1}^{W} \sum_{j=1}^{H} (OI_{i,j} - SI_{i,j})^2})$$
(13)

Where OI is original image, SI is stego image. In this work, 2^k correction is applied on the stego images to increase visual quality. Lena, Peppers, Goldhill, Sailboat, Barbara and Tiffany test images used to obtain the experimental results. These images are 128 x 128 sized and gray-level. The secret data is also randomly generated. The obtained results of the proposed method are shown in Table 2.

TABLE II THE OBTAINED PSNR (DB) AND CAPACITY (BPP) RESULTS OF THE PROPOSED EDGE ADAPTIVE METHOD USING VARIABLE EDGE DETECTORS AND X AND Y VALUES

Image	x=2 v=1	x=3 $y=2$	x=4 v=3	x=5 v=4	
innage	. 2 , y 1	Canny	A 1, 9 5	, y .	
Lena	PSNR=50.12, C=1.12	PSNR=45.03, C=2.12	PSNR=39.28, C=3.12	PSNR=33.16, C=4.12	
Peppers	PSNR=50.07, C=1.14	PSNR=44.96, C=2.14	PSNR=39.15, C=3.14	PSNR=33.16, C=4.14	
Goldhill	PSNR=49.95, C=1.15	PSNR=44.86, C=2.15	PSNR=39.17, C=3.15	PSNR=33.18, C=4.15	
Sailboat	PSNR=49.97, C=1.15	PSNR=44.88, C=2.15	PSNR=39.14, C=3.15	PSNR=33.19, C=4.15	
Barbara	PSNR=49.93, C=1.15	PSNR=44.81, C=2.15	PSNR=39.13, C=3.15	PSNR=33.18, C=4.15	
Tiffany	PSNR=50.02, C=1.14	PSNR=44.97, C=2.14	PSNR=39.17, C=3.14	PSNR=33.24, C=4.14	
		Sobel			
Lena	PSNR=50.45, C=1.07	PSNR=45.58, C=2.07	PSNR=39.84, C=3.07	PSNR=33.80, C=4.07	
Peppers	PSNR=50.47, C=1.08	PSNR=45.46, C=2.08	PSNR=39.68, C=3.08	PSNR=33.75, C=4.08	
Goldhill	PSNR=50.54, C=1.07	PSNR=45.50, C=2.07	PSNR=39.84, C=3.07	PSNR=33.95, C=4.07	
Sailboat	PSNR=50.56, C=1.07	PSNR=45.60, C=2.07	PSNR=39.95, C=3.07	PSNR=33.99, C=4.07	
Barbara	PSNR=50.42, C=1.08	PSNR=45.44, C=2.08	PSNR=39.79, C=3.08	PSNR=33.85, C=4.08	
Tiffany	PSNR=50.57, C=1.07	PSNR=45.64, C=2.07	PSNR=39.92, C=3.07	PSNR=33.97, C=4.07	
		LOG			
Lena	PSNR=50.44, C=1.08	PSNR=45.46, C=2.08	PSNR=39.69, C=3.08	PSNR=33.73, C=4.08	
Peppers	PSNR=50.43, C=1.09	PSNR=45.41, C=2.09	PSNR=39.68, C=3.09	PSNR=33.75, C=4.09	
Goldhill	PSNR=50.16, C=1.12	PSNR=45.11, C=2.12	PSNR=39.41, C=3.12	PSNR=33.43, C=4.12	
Sailboat	PSNR=50.24, C=1.11	PSNR=45.21, C=2.11	PSNR=39.49, C=3.11	PSNR=33.53, C=4.11	
Barbara	PSNR=50.32, C=1.09	PSNR=45.36, C=2.09	PSNR=39.64, C=3.09	PSNR=33.68, C=4.09	
Tiffany	PSNR=50.29, C=1.10	PSNR=45.25, C=2.10	PSNR=39.48, C=3.10	PSNR=33.57, C=4.10	
BED					
Lena	PSNR=50.37, C=1.09	PSNR=45.45, C=2.09	PSNR=39.64, C=3.09	PSNR=33.69, C=4.09	
Peppers	PSNR=49.90, C=1.14	PSNR=44.92, C=2.14	PSNR=39.18, C=3.14	PSNR=33.15, C=4.14	
Goldhill	PSNR=49.83, C=1.17	PSNR=44.72, C=2.17	PSNR=38.95, C=3.17	PSNR=32.99, C=4.17	
Sailboat	PSNR=50.30, C=1.10	PSNR=45.25, C=2.10	PSNR=39.51, C=3.10	PSNR=33.54, C=4.10	
Barbara	PSNR=49.81, C=1.18	PSNR=44.60, C=2.18	PSNR=38.87, C=3.18	PSNR=32.90, C=4.18	
Tiffany	PSNR=50.81, C=1.03	PSNR=45.97, C=2.03	PSNR=40.33, C=3.03	PSNR=34.33, C=4.03	
HED					
Lena	PSNR=49.29, C=1.26	PSNR=43.97, C=2.26	PSNR=38.27, C=3.26	PSNR=32.17, C=4.26	
Peppers	PSNR=48.92, C=1.32	PSNR=43.69, C=2.32	PSNR=37.85, C=3.32	PSNR=31.86, C=4.32	
Goldhill	PSNR=48.79, C=1.35	PSNR=43.49, C=2.35	PSNR=37.60, C=3.35	PSNR=31.65, C=4.35	
Sailboat	PSNR=49.03, C=1.31	PSNR=43.67, C=2.31	PSNR=37.97, C=3.31	PSNR=31.96, C=4.31	
Barbara	PSNR=48.83, C=1.35	PSNR=43.51, C=2.35	PSNR=37.61, C=3.35	PSNR=31.69, C=4.35	
Tiffany	PSNR=49.22, C=1.28	PSNR=43.90, C=2.28	PSNR=38.07, C=3.28	PSNR=32.10, C=4.28	

The comparison results of the proposed method with existing state-of-art edge-based data hiding methods in the

literature are shown in Table 3. In this comparison, 128 x 128 size of gray level Lena image is used.

 TABLE III

 COMPARISON WITH THREE PREVIOUSLY PRESENTED EDGE BASED DATA HIDING METHOD.

	Teeng and Lang's [20] method	Chen et al.'s [29] method	Bai et al.'s [31] method		The proposed method	
	Iseng and Leng S [50] method		Canny	Sobel	Canny	Sobel
Parameters	y=3	x=4, y=3, n=4	x=4, y=3	x=4, y=3	x=4, y=3	x=4, y=3
PSNR (dB)	38.18	37.50	38.34	38.34	39.2866	39.8499
Capacity(bpp)	2.41	2.10	3.11	3.05	3.1290	3.0787
Parameters	y=4	x=5, y=4, n=3	x=5, y=4	x=5, y=4	x=5, y=4	x=5, y=4
PSNR (dB)	33.58	32	30.10	30.69	33.1663	33.8079
Capacity(bpp)	3.16	2.73	4.11	4.05	4.1290	4.0787

The merits of the proposed method are given as below. In this article two novel basic edge extractors are presented. 1- By using 2^k correction higher visual qualities are obtained than the other state of art methods.

- 2- HED based steganography method has very high payload.
- 3- In this article, flaw of the other steganography is presented. Mathematical notations of the edge adaptive steganography methods are defined.
- 4- The proposed methodology is very basic and effective.
- 5- Researchers and developers can simply apply the proposed method to their problem.
- 6- The proposed method is a cognitive method because there is not any meta-heuristic optimization method to increase either payload or visual quality.

The disadvantage of the proposed edge-based steganography method: It is not robust method because it uses pixel domain to embed hidden data.

V. CONCLUSIONS

In this article, a novel edge adaptive data hiding method is presented with high payload and high visual quality. The proposed method consists of preprocessing, secret data classification, data hiding and data extraction phases. In this method, edge detectors are used as data hiding map. 6LSBs and 7LSBs elimination methods are utilized to increase the capacity in the preprocessing phase. Canny, Sobel, Log, BED and HED are used as the edge detection method. Two edge detectors are proposed to increase the payload in this method. The BED method extracts binary edges using the OTSU thresholding method, 2 x 2 blocks and a rule table. Mathematical definition of this rule table is shown in Eq. 1. The HED method use Canny, Sobel, LoG and BED methods together. Briefly, HED is combination of Canny, Sobel, LoG and BED detectors. The main goal of the HED method is to obtain all edge data in an image. Two separate secret data classes named x and y are created using edge information. The x and y classes are embedded into edge and non-edge pixels using the xLSBs and yLSBs methods respectively. More secret data are embedded into edge pixels than texture pixels because Human Visual System (HVS) is more sensitive to changes in the texture pixels than edge pixels. To increase visual quality, 2k correction is applied on the stego images. Modulus operator is utilized to data extraction. Briefly, HED and mLSBs elimination are used to increase the payload of the edge adaptive method, and 2^k correction is used for increasing the visual quality.

Experimental and comparative results have shown that the proposed method superior than other edge-based data hiding methods. In the future works, novel edge-based steganography methods can be proposed using this method. Also, the proposed method can be used an image transformation for instance tunable q wavelet transform, discrete wavelet transform, discrete cosine transforms together. The other edge extractor can be used in this method.

REFERENCES

 S.A. Parah, J.A. Sheikh, A.M. Hafiz, G.M. Bhat, Data hiding in scrambled images: a new double layer security data hiding technique, Comput. Electr. Eng. (40) (2014) 70–82.

- [2] O. Cetin, A.T. Ozcerit, A new data hiding algorithm based on color histograms for data embedding into raw video streams, Comput. Secur. 28 (7) (2009) 670–682.
- [3] S.Y. Shen, L.-H. Huang, A data hiding scheme using pixel value differencing and improving exploiting modification directions, Comput. Secur. (48) (2015) 131–141.
- [4] G. Kipper, Investigator's Guide to Data hiding, Auerbach Publications A CRC Press Company, Boca Raton, London, New York, Washington, DC, (2004) 20– 26.
- [5] I.J. Cox, J. Killian, T. Leighton, T. Shamoon, A secure robust watermark for multimedia, IEEE Trans. Image Process. (12) (1997) 1673–1687.
- [6] A. Phadikar, S.P. Maity, On protection of compressed image in fading channel using data hiding, Comput. Electr. Eng. 38 (5) (2012) 1278–1298.
- [7] N.F. Johnson, Z. Duric, S. Jajodia, Information Hiding: Data hiding and Watermarking-Attacks and Countermeasures, Kluwer Academic Publishers, Boston, MA, 2001.
- [8] A. Miller, Least Significant Bit Embeddings: Implementation and Detection, May 2012.
- [9] S.H. Lee, DWT based coding DNA watermarking for DNA copyright protection, Inform. Sci. (273) (2014) 263–286.
- [10] E. Avci, T. Tuncer, D. Avci, A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain, Arabian Journal for Science and Engineering, 41, (8), (2016) 3153-3161.
- [11] H. Noda, M. Niimi, E. Kawaguchi, High-performance JPEG data hiding using quantization index modulation in DCT domain, Pattern Recogn. Lett. 27 (5) (2006) 455–461.
- [12] P.C. Chang, K.L. Chung, J.J. Chen, C.H. Lin, T.J. Lin, A DCT/DSTbased error propagation-free data hiding algorithm for HEVC intracoded frames, J. Vis. Commun. Image Represent. (2) (2014) 239– 253.
- [13] B. Chen, G. Coatrieux, G. Chen, X. Sun, J.L. Coatrieux, H. Shu, Full 4-D quaternion discrete Fourier transform based watermarking for color images, Digit. Signal Process. (28) (2014) 106–119.
- [14] P.-Y. Lin, C.-S. Chan, Invertible secret image sharing with data hiding, Pattern Recognition Letters (31) (2010) 1887–1893.
- [15] T. Tuncer, E. Avci, A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images, Displays, (41) (2016) 1-8.
- [16] M. I. S. Reddy, A. P. S. Kumar, Secured Data Transmission Using Wavelet Based Data hiding and Cryptography by Using AES Algorithm, International Conference on Computational Modeling and Security, Procedia Computer Science (85) (2016) 62 – 69.
- [17] E. J. S, P. Ramu, R. Swaminathan, Imperceptibility—Robustness tradeoff studies for ECG data hiding using Continuous Ant Colony Optimization, Expert Systems With Applications (49) (2016) 123– 135.
- [18] T.-S. Nguyen, C.-C. Chang, A reversible data hiding scheme based on the Sudoku technique, Displays (39) (2015) 109–116.
- [19] T. Tuncer, E. Avcı, Data Hiding Application with Gokturk Alphabet Based Visual Cryptography Method, Journal of the Faculty of Engineering and Architecture of Gazi University (31:3) (2016) 781-789.
- [20] Z.-H. Ou, L.-H. Chen, A steganographic method based on tetris games, Information Sciences 276 (2014) 343–353.
- [21] C.K. Chan, L.M. Cheng, Hiding data in images by simple LSB substitution, Pattern Recognit. (27) (2004) 469–474.
- [22] S. Mahato, D. K. Yadav, D. A. Khan, A minesweeper game-based data hiding scheme, journal of information security and applications (32) (2017) 1–14.
- [23] X. Liao, J. Yin, S. Guo, X. Li, A. K. Sangaiah, Medical JPEG image data hiding based on preserving inter-block dependencies, Computers and Electrical Engineering (2017) 1–10.
- [24] H.-J. Shiu, B.-S. Lin , C.-H. Huang, P.-Y. Chiang, C.-L. Lei, Preserving privacy of online digital physiological signals using blind and reversible data hiding, Computer Methods and Programs in Biomedicine (151) (2017) 159–170.
- [25] H.D. Yuan, Secret sharing with multi-cover adaptive data hiding, Inform. Sci. (254) (2014) 197–212.
- [26] D. Wu, W.H. Tsai, A steganographic method for images by pixel value differencing, Pattern Recognit. Lett. (24) (2003) 1613–1626.

- [27] M. S. Subhedar, V. H. Mankar, Image data hiding using redundant discrete wavelet transform and QR factorization, Computers and Electrical Engineering (54) (2016) 406–422.
- [28] S. U. Maheswari, D. J. Hemanth, Frequency domain QR code based image data hiding using Fresnelet transform, Int. J. Electron. Commun. (69) (2015) 539–544.
- [29] W.J. Chen, C.C. Chang, T.H.N. Le, High payload data hiding mechanism using hybrid edge detector, Expert Syst. Appl. (37) (2010) 3292–3301.
- [30] H.W. Tseng, H.S. Leng, High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion, IET Image Process. (8) (2014) 647–654.
- [31] J. Bai, C.-C. Chang, T.-S. Nguyen, C. Zhu, Y. Liu, A high payload steganographic algorithm based on edge detection, Displays (46) (2017) 42–51.
- [32] J. Canny, A computational approach to edge detection, IEEE Trans. Pattern Anal. Mach. Intell. (6) (1986) 679–698.
- [33] R. Maini, H. Aggarwal, Study and comparison of various image edge detection techniques, Int. J. Image Process. (3) (2009) 1–11.
- [34] E.K. Kaur, E.V. Mutenja, E.I.S. Gill, Fuzzy logic based image edge detection algorithm in MATLAB, Int. J. Comput. Appl. (1) (2010) 55–58.
- [35] S. Sun, A novel edge based image steganography with 2^k correction and Huffman encoding, Information Processing Letters (116) (2016) 93–99.
- [36] T. Y. Goh, S. N. Basah, H. Yazid, M. J. A. Safar, F. S. A. Saad, Performance analysis of image thresholding: Otsu technique, Measurement (114) (2018) 298–307.

BIOGRAPHY



TÜRKER TUNCER, was born in Elazig, 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, feature extraction, machine learning and biomedical engineering.



YASIN SÖNMEZ, was born in Diyarbakır, Turkey in 1986. He received the B.S. degree from the Firat University, Technical Education Faculty, Department of Electronics and Computer Education in 2010, M.S. degree in computer science from the Firat University in 2012 and Ph.D. degree department of software engineering at Firat University in 2018. His research interests include, , artificial intelligence, , and information security.