Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **4**, July **2015**

A Novel Information Hiding Scheme Based on Line Segments

Zhi-Hui Wang[1], Qing Wu[1], Zhong-Xuan Luo[1], Chin-Chen Chang[2,3]

[1]School of Software, Dalian University of Technology,
Dalian, Liaoning, China
E-mail: wangzhihui1017@gmail.com

[2]Department of Information Engineering and Computer Science,
Feng Chia University

[3]Department of Computer Science and Information Engineering,
Asia University Taichung 41354, Taiwan
*Corresponding Author
E-mail: alan3c@gmail.com

Received October, 2013; revised July, 2014

Abstract. *In the last few years, hiding information on grayscale images has been drawing more attention in many applications. In this paper we propose a novel hiding algorithm on grayscale images by using line segments. We generate an initial set of line segments and use Sobel operator, which is an edge detection method, to detect the complex area. We then embed more secret data into the line segments located in the complex area. On the other hand, we reduce the number of embedded data in the smooth area. The experimental results demonstrate the superiority of our proposed scheme in terms of high capacity. The hiding capacity can be 2 bpp for all test images with imperceptible image distortion.*
Keywords: Qrayscale image, Information hiding, Line segment, LSB replacement

1. **Introduction.** Steganography is a method of writing confidential messages in a seemingly unsuspicious-looking media. Hiding information is a steganographic way to hide secret messages into a cover medium in order to avoid attracting the attention of an attacker.

In the literature, secret data can be embedded into digital images through three domains, namely spatial domain [1,2,7,8], compressed domain [3], and transformed domain [4]. In spatial domain, a large data embedding capacity can be obtained because more redundant spaces are available to embed secret data. However, data hiding methods in spatial domain are more vulnerable to statistical attacks. As for compressed domain, a cover image is firstly compressed by using compression methods. Data hiding schemes in compressed domain are robust and suitable for low bandwidth transmission channels. The embedding capacity of these schemes is high, but additional time is needed for compression and decompression procedures. A transformation (e.g. discrete cosine transform [4], discrete wavelet transform [5], or discrete Fourier transform [6]) is first performed on a cover image to obtain frequency coefficients. Then, secret data are embedded into significant coefficients. By being embedded in the transform domain, the hidden data reside in more robust areas and provide better resistance against signal processing.

This paper is focused on spatial domain. The basic issues to consider for an image data hiding scheme are hiding capacity and visual quality. Hiding capacity is the number of bits embedded into a cover image. The visual quality is the quality of stego-image. It is technically challenging to achieve the high capacity and low image distortion at the same time.

Many special domain information hiding schemes based on grayscale images have been proposed [9,10]. A famous information hiding scheme is the least significant bit (LSB) replacement method, proposed by Turner in 1989 [10]. In the LSB replacement scheme, binary secret bits are embedded into a cover image by replacing the LSBs of cover pixels with secret bits to obtain a stego-image. This method either increases even-valued pixels by one or keeps them unchanged and odd-valued pixels are either kept intact or decreased by one. This asymmetric modification makes the method vulnerable to common attacks.

To improve visual quality of LSB matching method, in 2006, Mielikainen [11] proposed a new LSB matching-like method. Mielikainens method has the hiding capacity of 1 bit per pixel (bpp) and good visual quality, measured by peak signal-to-noise ratio (PSNR), by using a binary function, F_1. Mielikainens method is described as follows:The secret data in binary form is $S = b_0b_1b_2...b_{L-1}$ and L is the length of S. S is partitioned into secret bit pairs $(b_i, b_{i+1})'s$, where $i = 0, 1, ..., L-2$. The cover image I sized $H \times W$ is partitioned into cover pixel pairs, $(p_i, p_{i+1})'s$. During the embedding process, each secret bit pair (b_i, b_{i+1}) is hidden into one cover pixel pair (p_i, p_{i+1}) at a time by adding and subtracting p_i or p_{i+1} by one, or keeping p_i or p_{i+1} unmodified. The secret bit pair (b_i, b_{i+1}), least significant bit of p_i (i.e.$LSB(p_i)$, the returned value of the binary function F_1 (i.e. $F(p_i, p_{i+1})$ or $F_1(p_i, p_{i+1})$, and whether the $p'_{i+1}s$ grayscale value is even or odd are four factors that determine the embedding rules. The aforementioned binary function F_1 is defined as

$$\dot{F}(p_i, p_{i+1}) = LSB(\left\lfloor \frac{p_i}{2} \right\rfloor + p_{i+1}) \tag{1}$$

Zhang and Wang proposed a new exploiting modification direction (EMD) method [9] to fully utilize the modification of Mielikainens scheme. In Zhang and Wangs method, each secret digit in a $(2n+1)$ary notational system is carried by n cover pixels. Based on this, the hiding capacity of Zhang and Wangs method is $\log_2(2n+1) = n$ bpp.

With the purpose of achieving both high embedding and good visual quality, we propose our method. The main idea of the proposed method is to divide pixels into line segments and embed secret data into each line segment. We define a line segment contains more than one pixels. Thus, the high visual quality of stego-image can be achieved by dispersing the distortion into pixels on line segment. Moreover, we detect the complex area by using Sobel operator and divide these line segments according to whether they are located in complex area. We embed more secret data into the line segment in complex area while reduce the number of secret data in smooth area.

Based on the proposed method, the embedding rate equals to 2 bits per pixel (bpp). Mielikainens method and Zhang and Wangs method successfully embed the secret message with tiny distortions. But the embedding rates of their methods are only 1 bpp. Our experimental result not only has superior embedding rate representation but also maintains the visual quality.

The rest of the paper is organized as follows. The review of the Sobel operator is presented in Section 2. The proposed scheme is explored in Section 3. In Section 4, we show and analyze the experimental results. The conclusions are finally drawn in Section 5.

2. **Problem Statement and Preliminaries.** The Sobel operator is widely used edge detection procedures. We all know that the areas near edge pixels are more complex than the other area in the image. In other words, the Sobel operator can be used to detect the complex area and the smooth section. At each point in the image, the result of the Sobel operator is either the corresponding gradient vector or the norm of this vector. In simple terms, the algorithm calculates the gradient of the image intensity at each point, giving the direction of the largest possible increase from light to dark and the rate of change in that direction.

The algorithm uses two 3×3 kernels which are convolved with the original image to calculate approximations of the derivatives one for horizontal changes and one for vertical. If we define A as the source image, and G_x and G_y are two images which at each point contain the horizontal and vertical derivative approximations, the computations are as follows:

$$\dot{G}_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix} * A \tag{2}$$

$$G_y = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} * A \tag{3}$$

where * denotes the 2-dimensional convolution operation. The x-coordinate is defined here as increasing in the "right" direction, and the y-coordinate is defined as increasing in the "down" direction. At each point in the image, the resulting gradient approximations can be combined to give the gradient magnitude, using:

$$\dot{G} = \sqrt[2]{G_x^2 + G_y^2} \tag{4}$$

2.1. **Edge threshold.** To classy the edge pixels, we use an edge threshold T. For simplicity, T is defined as a fixed parameter, namely T is 180.

For a pixel k, we compute the gradient magnitude of k, as $G(k)$. If $G(k)$ is larger than T, then pixel k is an edge pixel. Otherwise, the pixel is a non-edge pixel.

3. **The proposed method.** Based on the idea of line segment and the Sobel operator, we propose a novel scheme. Subsection 3.1 introduces the details of the data embedding phase, followed by a demonstrative example given in Subsection 3.2. The data extracting phase is described in Subsection 3.3.

3.1. **Edge threshold.** We suppose that the cover image I is 256 gray levels and sized $H \times W$. Let binary secret message be S. The embedding algorithm is composed of three steps, which are detecting edges by using the Sobel operator, generating line segments and embedding step. The proposed method works as follows.

Firstly, we detect the edge pixels in cover image I. We define the edge pixels and the pixels around the edge pixels are unchangeable. For example, if the edge pixel is $p_{i,j}$, the pixels $p_{i,j+1}$ are unchangeable pixels. That is because we need to ensure that edge pixels are invariable in the receiver side. Except for these unchangeable pixels, the rest pixels in the cover image are all changeable.

Secondly, we use squares to mark the complex area. We defined the distance is R which means the distance between the interest pixel and interest edge pixel. The length of the squares sides is settled as $2R + 1$ and the center of square is the interest edge pixels (e.g.

$p_{i,j}$). The changeable pixels within the square are considered as in the complex area, else the changeable pixels are in smooth area.

We identify the number of pixels (L) included in each line segment. Then, the process is as follows: read sequential changeable L pixels in raster-scan style to generate line segments. More specifically, the grayscale values of pixels in an L-sized line segment as an L-sized vector $(i_1, i_2, ..., i_L)$ is denotedthen the value (M_1) of the extraction function f as a weighted modulo N is calculated.

$$\dot{M}_1 = f(i_1, i_2, ..., i_L) = \left\lfloor \frac{\sum_{j=1}^{L} i_j}{L} \right\rfloor modN \tag{5}$$

Based on the concept that the visual quality of stego-image is better when the cover image is more complex, we design our scheme. We can adjust the number of embedded data by changing the value of N. In complex area, the value of N is larger, and we can embed more data in that area. On the other hand, reduce the value of N and the number of embedded data in the smooth area. N_1 and N_2 ($N_1 < N_2$) are the moduli used in smooth area and complex area respectively. Judge whether the line segment contains pixels in the complex area. If it is, set the modulus N as modulus N_2 or else set N as modulus N_2. Finally, embed secret data into the line segment. the binary secret data S is partitioned into the K-sized segments of bits. Secondly, each K-sized segment is converted into M_2 secret digits in the base-N numeral system. The value of K is computed by:

$$\dot{K} = \lfloor M_2 \times \log_2 N \rfloor \tag{6}$$

Compute the D-value d between M_1, M_2 as $d = M_1 - M_2$. Add d to each pixel in $(i_1, i_2, ..., i_L)$. Repeat the second and third steps until the end of cover image, and output the stego-image. The flowchart is shown in Fig.1.

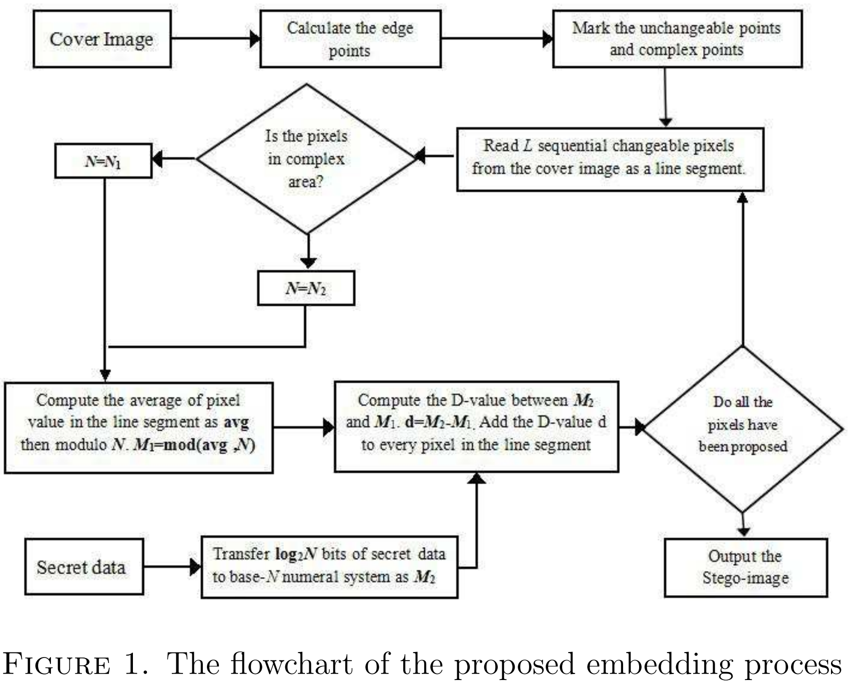


FIGURE 1. The flowchart of the proposed embedding process

3.2. **Embedding example.** The embedding method is illustrated by the following example. For simplicity, we assume that L equals 8, R equals 2. N_1 and N_2 are set to 2 and 4, respectively. We use Lena as an example. The chart of the dividing area (complex area or smooth area) is shown in Fig.2 and Fig.3. Fig.2 is the global view of the dividing area

FIGURE 2. The global view of the dividing area.

and Fig.3 is the enlarged view sampled from Fig.2 In Fig.3, the gray area presents edge

	5	6	7	8	9	10	11	12
430	39	50	62	69	103	113	129	146
431	39	50	62	69	99	109	126	144
432	39	50	62	69	97	107	125	143
433	30	39	49	56	96	106	122	138
434	30	39	49	56	95	105	121	138
435	30	39	49	56	93	103	120	137
436	30	39	49	56	89	100	118	137
437	30	39	49	56	86	97	116	136
438	30	39	49	56	83	94	114	135
439	30	39	49	56	80	92	113	135

FIGURE 3. The enlarged view of dividing area.

points. We chose these edge pixels by using the Sobel operator. The red area shows the unchangeable pixels, which are the parameters used in the Sobel operator. Both the edge pixels in gray and red areas are invariable, and these pixels are excluded in the complex area. The length of the squares side is 5. The complex area is the green area, which are the pixels around edge points. We take Rows 430 and 431 as examples. The length of line segment is 8. In Row 430, none of the first 8 changeable pixels is in the green area, so the modulus N is set as 2. In Row 431, some of the first 8 changeable pixels are in the green area, so the modulus N is set as 4. By using different modulus, we can embed 1 bit of secret data in the first line of Row 430, while embedding 2 bits in the first line of Row 431.

3.3. **Secret extracting phase.** The extraction of the message is very simple. The receiver shares the same image database with sender. After receiving the stego-image, the receiver uses the original image to detect the complex area and smooth area based on the embedding rules. Then, embedded secret digits can be extracted from the stego-image only using the complex area and the pre-shared parameters L, N_1, N_2 and R the extraction function f. The flowchart of the proposed secret extracting process is displayed in Fig. 4. The proposed extracting process works as follows. Firstly, using relative original

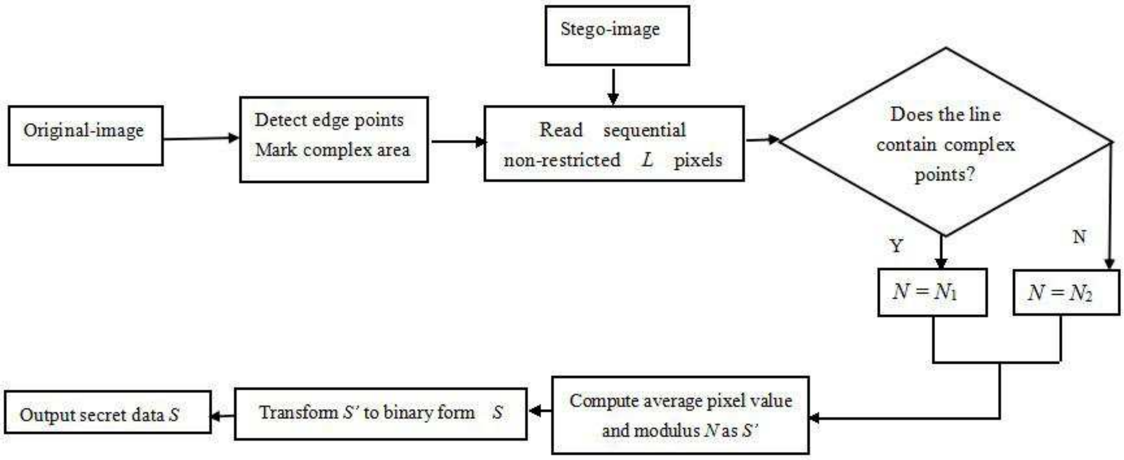


FIGURE 4. The flowchart of the proposed extracting process

image to choose edge pixels and compute the complex area according to the parameter R.

Then, a line segment is generated, and from this, it can be judged whether some pixels of the line segment are located in the complex area. If they are, set modulus N as modulusN_1 , else set N as modulus N_2. Then use the extraction function f to get secret data.

4. **The proposed method.** In this section, some experimental results are presented to prove the validity of the proposed scheme. The secret bit stream S was randomly generated using the library function rand() in the MATLAB 2010 library.

In image data hiding, hiding capacity and visual quality play an important role. The embedding rate can be embedded into one pixel, and it is measured by bit per pixel (bpp). Usually, PSNR is favored to evaluate the quality of the stego-images. The definition of PSNR is illustrated as follows:

$$\dot{P}SNR(dB) = 10\log_{10}(\frac{255^2}{MSE}) \tag{7}$$

$$MSE = \frac{1}{H \times M}\sum_{i=1}^{H}\sum_{j=1}^{W}(I_{ij} - I'_{ij})^2 \tag{8}$$

Here MSE (mean-square error) is used to measure the difference between images I and I' sized $H \times M$ pixels, and I_{ij} and I'_{ij} are the (i, j)th pixel values of the cover image I and the stego-image I'. A high PSNR value of a stego-image means that the stego-image is very similar to the original image. Fig.5 shows the six 512512 test grayscale images used in our experiment.

L (the length of line segments) and the modulus $N(N_1, N_2)$ are two factors that affect capacity and PSNR. If L is smaller, there will be more line segments to hide secret data. On the other hand, if the modulus N is larger, there can embed more secret data into each line segment.

In order to see how L and N influence the performance of the test images, we have done two series of experiments. Table 1 shows the length of line segments L is set as 2, 4 and 8, respectively, while the modulus N_1 and N_2 are set as 8 and 16. Table 2 presents the experimental results when the modulus N_1 and N_2 are set as 2 and 4, 4 and 8, 8 and 16, 16 and 32, respectively, while L remains static (as 2). The character C in Table 1 and Table 2 represents hiding capacity.

(a) Baboon (b) Pepper (c) Zelda

(d) Elaine (e) Toys (f) Lena

FIGURE 5. Six grayscale test images of size 512*512

From Table 1, it can be seen that hiding capacity improves from about 0.37 bpp to nearly 1.50 bpp when L is reduced and the PSNR of the stego-image is about 40 for every level. In column 1, the capacity could achieve about 1.5 bpp while the stego-image quality is still about 40 for all kinds of images. This proves the quality of a stego-image is slightly changed when L is reduced. However, the hiding capacity improves significantly when L is reduced. So we set the smallest length 2 as the length of line segments.

From Table 2, it can be seen that the hiding capacity improves nearly 0.5 bpp for each column while the PSNR of stego-images reduces about 7dB for every level. In Column 1, the PSNR could achieve more than 54dB for all kinds of images, which is mostly perceptual image visual value for the human visual system, while the capacity is 0.5 bpp. In Column 4, the capacity increases to 2 bpp while the PSNR is still acceptable at about 34dB. We achieve the highest embedding rate when the modulus N_1 and N_2 are set as 2

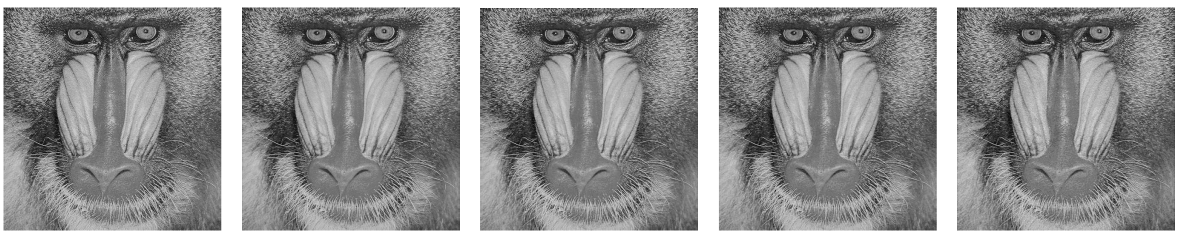
TABLE 1. L is set as different values while the modulus N_1 and N_2 are set as 8 and 16

Images \ L		L=2	L=4	L=8
Baboon	C	1.51	0.75	0.38
	PSNR	40.53	41.07	40.53
Pepper	C	1.50	0.74	0.37
	PSNR	40.73	40.78	40.73
Zelda	C	1.50	0.74	0.37
	PSNR	40.88	40.90	40.93
Elaine	C	1.50	0.74	0.37
	PSNR	40.87	40.81	40.87
Toys	C	1.50	0.74	0.37
	PSNR	41.08	41.12	41.19
Lena	C	1.50	0.75	0.38
	PSNR	40.66	40.59	40.67

TABLE 2. N_1 and N_2 are set as different values while the modulus L is set as 2

Images \ N_1 N_2		N_1=2 N_2=4	N_1=4 N_2=8	N_1=8 N_2=16	N_1=16 N_2=32
Baboon	C	0.51	1.00	1.51	2.06
	PSNR	53.65	46.73	40.53	34.61
Pepper	C	0.50	1.00	1.50	2.04
	PSNR	54.08	47.07	40.73	34.74
Zelda	C	0.50	1.00	1.50	2.06
	PSNR	54.17	47.13	40.88	34.85
Elaine	C	0.51	1.00	1.50	2.04
	PSNR	54.11	47.11	40.87	34.85
Toys	C	0.51	1.00	1.50	2.06
	PSNR	54.12	47.20	41.08	34.56
Lena	C	0.50	1.00	1.50	2.06
	PSNR	53.93	46.93	40.66	34.42

and 4, respectively, and achieve the best visual quality when the modulus N_1 and N_2 are set as 16 and 32, respectively.



(a) Original image (b) stego-images 1 (c) stego-images 2 (d) stego-images 3 (e) stego-images 4

FIGURE 6. The visual quality of the stego-image

Proposed method	LSB revised	Zhang and Wang

FIGURE 7. The comparative results for visual quality comparison

Fig.6. shows the original Baboon image and stego-images 1, 2, 3, and 4 as the results of the proposed scheme when $L = 2$ and modulus N_1 and N_2 have been set as 2 and 4, 4 and 8, 8 and 16, 16 and 32, respectively. When comparing these images, it is difficult for the human eyes to recognize the difference between them. Even stego-image 4, after embedding 524,288 secret bits the visual quality is still quite good.

TABLE 3. The performances of LSB revised, Zhang and Wangs, and the Proposed methods

method / Images	LSB revised		Zhang and Wang		Proposed method			
	C	PSNR	C	PSNR	C	PSNR	C	PSNR
Baboon	1	52.51	1	52.10	1.51	40.53	2.06	34.61
Pepper	1	52.53	1	52.12	1.50	40.73	2.04	34.74
Zelda	1	52.50	1	52.02	1.50	40.88	2.06	34.85
Elaine	1	52.49	1	52.03	1.50	40.87	2.04	34.85
Toys	1	52.48	1	52.02	1.50	41.08	2.06	34.56
Lena	1	52.50	1	52.11	1.50	40.66	2.06	34.42

The proposed method can embed 524,288 secret bits into a 512512-sized image, which means the embedding rate is 2 bpp. In this situation, the stego-image is very similar to the original image, which means the human visual system can hardly detect the difference between them. The LSB revised method can embed 262,144 bits into a 512512-sized image, which means the embedding rate is 1 bpp. In Zhang and Wangs method,the maximum hiding capacity could achieve almost 1 bpp.

Table 3 shows the hiding capacity and PSNR of LSB revised, Zhang and Wangs method, and the experimental result of our proposed method when N_1 and N_2 are set as 8 and 16, 16 and 32, respectively, while the modulus L is settled as 2. Obviously, the hiding capacity of the proposed method is significantly greater than that of the LSB revised method and Zhang and Wangs methods, while the visual quality of the stego-image is still good. The PSNR values of the proposed method are less than those of the LSB revised and Zhang and Wangs methods. However, the visual quality of stego-images produced by the proposed method is still very good. That is, the PSNR values of the proposed method are always greater than 40dB for all test images when the hiding capacity is increased to 1.5 bpp. Moreover, the appearance difference between the cover image and stego-image is indistinguishable by the human visual system when the hiding capacity achieves 2 bpp.

Although the value of PSNR of our proposed method is less than that of LSB revised method and Zhang and Wangs method, the visual quality of the proposed method is quite good. We also implemented the LSB revised method and Zhang and Wangs method. Fig.7 shows the comparative results for visual quality among Zhang and Wangs method, LSB revised method, and our proposed method when the capacity of proposed method is 2 bpp. By observing the comparative results, the embedded images can be seen to be very similar. Moreover in the last Row, we enlarged part of the view from the third Row (the toys images). When comparing those images, it is very hard to recognize the difference between them by the human eyes. That is, our method has the good visual quality of a stego-image even in the enlarged view.

Table 4 compares the experimental results between the proposed scheme with Feng et al.s method[12]. Feng et al.s method was proposed in 2010, which is a data embedding method using edge information. The results in Table 4 are the average results from the six test images. From the results we can seen that, the maximum hiding capacity of our scheme and Feng et al.s method is almost the same, which is about 2bpp. Moreover, when the visual quality is similar, our scheme can embed more secret data. So our method has impressive experimental results. Since our users share the same image database for accuracy. The users could be in a certain local area network , the same company or the same system.

Table 4. The performances of the Feng et al.s method and Proposed methods

	Feng et al.s method		Proposed method	
The average results of six test images	C	PSNR	C	PSNR
	1.18	46.00	1.00	47.03
	1.29	41.40	1.50	40.80
	2.02	39.69	2.05	34.70

5. **Conclusions.** In this paper, we propose a steganographic scheme with high capacity based on line segments. The proposed method technically achieved high visual quality of the stego-image by dispersing distortion into pixels on line segments. Moreover, based on the concept that the visual quality of the stego-image is better when the cover image is more complex, we further improved the visual quality by combining Sobel operator to divide the image into complex areas and smooth areas. We embedded more data in the complex area and reduced the number of embedded data in the smooth area. The experimental result shows that the proposed method produces a stego-image with good visual quality and carries a large secret message. The maximum capacity of our proposed method achieves 2 bpp with imperceptible image distortion. In conclusion, the proposed method is applicable to steganographic applications, where a high hiding capacity and good visual quality are desired.

REFERENCES

[1] C. K. Chan ,and L. M. Cheng, Hiding data in images by simple LSB substitution, *Pattern Recognition* vol. 37, no. 3, pp. 469–474, 2004.

[2] W. L. Tai, C. M. Yeh, and C. C. Chang, Reversible data hiding based on histogram modification of pixel differences, *IEEE Trans. Circuits and Systems for Video Technology*, vol. 19, no. 6, pp. 906–910, 2009..

[3] C. C. Chang , W. L. Tai, and C. C. Lin, A reversible data hiding scheme based on side match vector quantization, *IEEE Trans. Circuits and Systems for Video Technology*, vol. 16, no. 10, pp. 1301–1308, 2006.

[4] Y. T. Wu, and Y. S. Frank, Digital watermarking based on chaotic map and reference register, *Pattern Recognition*, vol. 40, no. 12, pp. 3753–3763, 2007.

[5] S. Lee, C. D. Yoo, and T. Kalker , Reversible image watermarking based on integer-to-integer wavelet transform, *IEEE Trans. Information Forensics and Security*, vol. 2, no. 3, pp.321–330, 2007.

[6] H. C. Huang, J. S. Pan, Y. H. Huang, F. H. Wang, and K. C. Huang, Progressive watermarking techniques using genetic algorithms, *Circuits, Systems, and Signal Processing*, vol.26, no.5, pp.671–687, 2007.

[7] Y. Hu, H. K. Lee,and J. Li, DE-based reversible data hiding with improved overflow location map, *IEEE Trans. Circuits and Systems for Video Technology*, vol. 19, no. 2, pp. 250–260, 2009..

[8] T. H. Lan, and A. H. Tewfik, A novel high-capacity data-embedding system, *IEEE Trans. Image Processing*, vol. 15, no. 8, pp. 2431–2440, 2006.

[9] X. Zhang, and S. Wang, Efficient steganographic embedding by exploiting modification direction, *IEEE Communications Letters*, vol. 10, no. 11, pp. 1–3, 2006.

[10] L. F. Turner, Digital data security system, *Patent IPN*, WO 89/08915, 1989.

[11] J. Mielikainen, LSB matching revisited, *Proc. of IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285–287, 2006.

[12] C. F. Lee, C. C. Chang, and P. L. Tsou, Data Data Hiding Scheme with High Embedding Capacity and Good Visual Quality Based on Edge Detection, *010 Fourth International Conference on Genetic and Evolutionary Computing*, pp.654–657, 2010.