

Steganographic Image Hiding Schemes Based on Edge Detection

Chin-Feng Lee¹, Jau-Ji Shen^{2(✉)}, and Zhao-Ru Chen²

¹ Department of Information Management, Chaoyang University of Technology,
Taichung, Taiwan
lcf@cyut.edu.tw

² Department of Management Information Systems, National Chung Hsing University,
Taichung, Taiwan
jjshen@nchu.edu.tw

Abstract. In 2010, Chen et al. proposed a steganography mechanism using a hybrid edge detector. The hybrid edge detector is combining the Canny and the fuzzy edge detectors. However, although this method has a high embedding payload (2.10 bpp) it is an irreversible data hiding scheme. A considerable amount of research has since been conducted to provide an improved method of data hiding that removes LSBs of the image pixel value and performs edge detection. This increases the payload as it is not necessary to store edge information in the stego image. This paper conducts a comprehensive study of irreversible and reversible data hiding based on the image texture data hiding method, and compares embedding capacities and visual image qualities.

Keywords: Data hiding · Irreversible data hiding · Reversible data hiding · Edge detector technique

1 Introduction

The internet has now developed to such an extent that information security needs to be extremely proficient with respect to using social media, internet banking, and sending and receiving highly confidential emails. Data hiding ensures that the confidential information transmitted is not found and destroyed. There are two types of data hiding schemes: irreversible information hiding and reversible information hiding. The former uses a process whereby the stego image cannot be restored to the original image after secret data has been removed from it, and the latter involves restoring the stego image to the original image after secret data has been removed from it. As the human vision system is less sensitive to changes on the edges of images, some researchers have hidden most of the secret data on the edge of an image; this gives the stego image a better quality. For example, Chen et al. [1] proposed an innovative steganography scheme that uses the LSB (Least Significant Bit) replacement method and a hybrid edge detector that combines a fuzzy edge detector and Canny edge detector. Furthermore, in the same year, Lee et al. [2] proposed a method to improve this concept. The edge image is generated

by four MSBs (Most Significant Bits) of the image pixel value, and it is thus not necessary to record the location of the edge pixels; this greatly improves the embedding capacity and image quality of the stego image. In 2017, Bai et al. [3] also proposed a method to improve the shortcomings inherent in Chen et al. study; by using the 3 MSBs of the original image pixel value they obtained the edge image without needing to hide the edge information, which improved both the stego image quality and embedding rate (the embedding rate can reach 3.11 bpp).

However, some researchers have proposed hiding secret data in the smooth area of the image to obtain a better image quality. For example, in 2010, Hong and Chen [4] proposed a reference pixel distribution mechanism (RPDM) to detect the complex and smooth area of the original image. Here the secret data are embedded in the pixel error of the smooth area of the image using interpolation, so that the image quality can be improved in the reversible case.

This paper is organized as follows. Section 2 introduces irreversible and reversible data hiding techniques based on image texture; a detailed analysis and comparison of the methods are presented in Sect. 3; and concluding remarks are in Sect. 4.

2 Data Hiding Schemes Based on Image Texture

2.1 Irreversible Data Hiding Schemes

High payload steganography mechanism using hybrid edge detector. In 2010, Chen et al. proposed a method that firstly generates an edge image using a hybrid edge detector. Firstly, an edge image, E , is obtained from the cover image, I , using a hybrid edge detector. Then, the edge image, E , is divided into non-overlapping blocks. The block is called a “ n -pixel block” with n pixels represented as (P_1, P_2, \dots, P_n) , respectively. The first pixel value P_1 of each block uses the LSB replacement method to record the edge information of the other pixels from P_2 to P_n in the block. Each edge pixel embeds ‘ x ’ bits of the secret message using the LSB replacement method, and each non-edge pixel embeds ‘ y ’ bits of the secret message using LSB replacement method. It is of note that there are more secret message bits in the edge pixel than in the non-edge pixel.

Furthermore, the process used to extract the secret message is as follows (with examples to follow). Step 1: Herein, the stego image, I' , is divided into non-overlapping blocks with n pixels in each block; this block is called a “ n -pixel block” and the n pixels are represented as $(P'_1, P'_2, \dots, P'_n)$, respectively. Step 2: The status of the pixels is extracted from P'_2 to P'_n , and is then classified into edge pixels and non-edge pixels. The ‘ x ’ LSBs of the edge pixels and the ‘ y ’ LSBs of the non-edge pixels are then extracted and concatenated as the secret message, S .

Example 1. The pixel A has a pixel value of $\{[1\ 0\ 1\ 0\ 0\ 0\ 1\ 1], [0\ 1\ 1\ 1\ 1\ 0\ 0\ 0], [1\ 1\ 1\ 1\ 1\ 1\ 1], [0\ 0\ 1\ 1\ 1\ 1\ 0\ 0]\}$, which is P_1, P_2, P_3 , and P_4 , respectively, and the secret message $S = '0\ 0\ 1\ 0\ 1\ 0\ 1'$. In this case, n is set to 4, so that the image A is a “4-pixel block.”

Firstly, after the cover image, A , is detected using the hybrid edge detection method, the edge image, E , is generated. Assuming that P_2 and P_4 are edge pixels in the image

A , the status of P_2, P_3 , and P_4 are ‘1 0 1’, respectively. The 3 LSBs of the pixel value P_1 are then replaced by ‘1 0 1’, so that the stored state of P_1 becomes P'_1 and the pixel value is [1 0 1 0 0 1 0 1]. We also assume that the parameters x and y are 3 and 1, respectively. P_2 and P_4 are embedded in 3 bits of the secret message, and P_3 is then embedded in the 1 bit of the secret message. The new pixel values of P_2, P_3 , and P_4 are subsequently [0 1 1 1 0 1 1], [1 1 1 1 1 1 0] and [0 0 1 1 1 1 0 1], respectively. Thus, a stego image A' is generated with pixel values of {[1 0 1 0 0 1 0 1], [0 1 1 1 0 1 1], [1 1 1 1 1 1 0], [0 0 1 1 1 0 1]}. The embedding procedure in this example is represented in Fig. 1, and the process of extracting secret data is shown in Fig. 2.

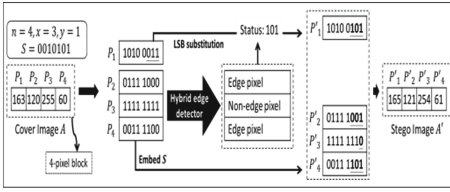


Fig. 1. Example of embedding procedure.

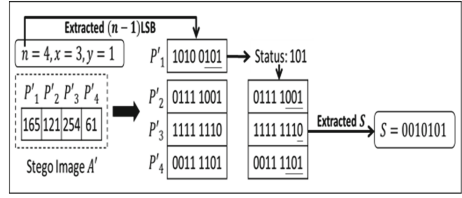


Fig. 2. Example of extraction procedure.

Data Hiding Scheme with High Embedding Capacity and Good Visual Quality Based on Edge Detection. In 2010, Lee et al. [2] proposed a method that aimed to improve the limitations inherent in the study of Chen et al. [1] Firstly, the 4 MSBs of the pixel values are extracted from the cover image, I , using Formula (1) to obtain the reference image I_R . M and N are the width and height of the cover image, respectively. For pixels $I(i, j)$ satisfying $i = 1, 2, \dots, M$ and $j = 1, 2, \dots, N$. Then, the edge image, E , is obtained from the edge information of the reference image, I_R , using the ED-MOF method by Kang and Wang’s edge detection method [5], where each pixel $E(i, j) \in \{0, 1\}$. If $E(i, j) = 1$. The relative pixels in the cover image, I , are then the edge pixel, otherwise they are the non-edge pixels. The secret message, S , is embedded in the LSBs of the cover image, I . The number of embedded bits in edge pixel is “ x ”, and the number of embedded bits in non-edge pixel is “ y ”. However, the 4 MSBs of the pixel of the cover image cannot be modified because of the edge detection, and thus, x and y cannot be greater than four and $x < y$.

$$I_R(i, j) = \left\lfloor \frac{I(i, j)}{16} \right\rfloor \times 16 \quad (1)$$

The process of extracting the secret message begins by applying ED-MOF method on the reference image, I_R to obtain an edge image, E , where I_R comes from the 4 MSBs of the stego image, I' , using Formula (1). If the position of the pixel is an edge pixel, x LSBs are extracted from the pixel, and if the pixel is a non-edge pixel, y LSBs are extracted from the pixel. When all the extracted LSBs are combined, they become the secret message, S .

Example 2. Firstly, the pixel value of the cover image, A , is $\{[1\ 0\ 1\ 0\ 0\ 0\ 1\ 1], [0\ 1\ 1\ 1\ 1\ 0\ 0\ 0], [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1], [0\ 0\ 1\ 1\ 1\ 1\ 0\ 0]\}$, which is denoted as P_1, P_2, P_3 , and P_4 , respectively, and the secret message $S = '0\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0'$. The 4 MSBs of each pixel are first extracted by Formula (1) and are recorded to the reference image, A_R . The edge information of the reference image, A_R , is then detected using the ED-MOF method, and the edge image, E , is obtained. If we assume that the edge image, E , is $\{0, 1, 0, 1\}$, then P_2 and P_4 are edge pixels. In this case, the parameters x and y are set to 3 and 2, so P_1 and P_3 are embedded in 2-bit secret messages. P_2 and P_4 are embedded in 3-bit secret messages. The embedded pixel value is $\{[1\ 0\ 1\ 0\ 0\ 0\ 0\ 0], [0\ 1\ 1\ 1\ 1\ 1\ 0\ 1], [1\ 1\ 1\ 1\ 1\ 1\ 0\ 1], [0\ 0\ 1\ 1\ 1\ 1\ 1\ 0]\}$, which is the stego image, A' . The embedding procedure in this example is shown in Fig. 3, and the process of extracting secret data is shown in Fig. 4.

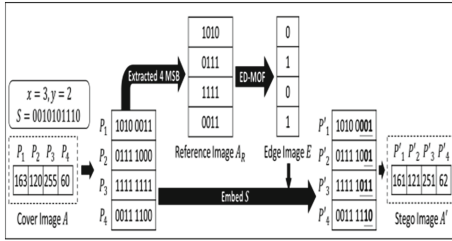


Fig. 3. Example of embedding procedure.

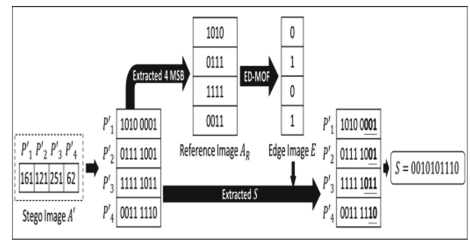


Fig. 4. Example of extraction procedure.

A high payload steganographic algorithm based on edge detection. In 2017, Bai et al. determined a limitation in Chen et al.'s method; that the index pixels occupy the embedding space of the image. Similar to Lee *et al.* [2], they thus designed a mechanism to make full use of the embeddable pixels in the cover image, and experimental results have shown that the embedding mechanism achieves better results under different edge detectors, such as Canny, Sobel, and Fuzzy. The process of embedding and secret extraction is as follows by an example.

Example 3. It is supposed that there are four pixels of the cover image, A , which are $\{[1\ 0\ 1\ 0\ 0\ 0\ 1\ 1], [0\ 1\ 1\ 1\ 1\ 0\ 0\ 0], [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1], [0\ 0\ 1\ 1\ 1\ 0\ 0]\}$ are P_1, P_2, P_3 , and P_4 , respectively, where $x = 4$ and $y = 2$ and the secret message $S = '0\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1'$. Firstly, the pixel value of the cover image, A , is extracted and recorded in the new image, A_{MSB} . The pixel value of the new image, A_{MSB} , is $\{[1\ 0\ 1\ 0\ 0\ 0\ 0\ 0], [0\ 1\ 1\ 1\ 1\ 0\ 0\ 0], [1\ 1\ 1\ 1\ 0\ 0\ 0\ 0], [0\ 0\ 1\ 0\ 0\ 0\ 0\ 0]\}$. The edge image, E , is generated by the new image, A_{MSB} , using the edge detector. We then assume that after edge detection, P_2 and P_4 are edge pixels, and P_1 and P_3 are non-edge pixels. Therefore, the secret message, S , is embedded in the 4 LSBs of the pixel values P_2 and P_4 using the LSB substitution method, and the two bits are embedded in P_1 and P_3 . Finally, the embedding of x and y in the last four pixels of the cover image, A , is complete. Therefore, the pixel values of the stego image, A' , are $\{[1\ 0\ 1\ 0\ 0\ 0\ 0\ 0], [0\ 1\ 1\ 1\ 1\ 0\ 1\ 0], [1\ 1\ 1\ 1\ 1\ 1\ 1\ 1], [0\ 0\ 1\ 1\ 1\ 0\ 0\ 1]\}$. The embedding procedure in this example is shown in Fig. 5, and the process of extracting secret data is shown in Fig. 6.

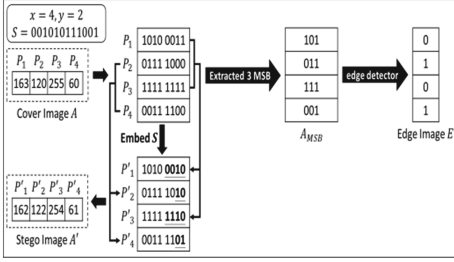


Fig. 5. Example of embedding procedure.

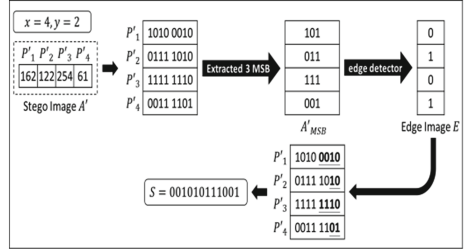


Fig. 6. Example of extraction procedure.

2.2 Reversible Data Hiding Scheme

Reversible data embedding for high quality images using interpolation and RPDM.

In 2011, Hong and Chen proposed a reversible data hiding technique based on image interpolation and detection of smooth and complex regions of the cover image. This method enables the most secret message to be hidden in the smooth area of the image rather than in the complex area. To detect the smooth and complex areas in the image, a reference pixel distribution mechanism (RPDM) is proposed, and a range function is used to evaluate the smoothness of the image. The range function $\text{Range}(x_1, x_2, \dots, x_n)$ is defined as the absolute difference between the maximum value and the minimum value of the given value x_1, x_2, \dots, x_n . For given a of pixel P , if the range of the upper, lower, left, and right reference pixels of P is smaller than the threshold, T_0 , then the pixel P is within the smooth region; however, if the range is larger than the threshold, T_1 , the pixel P is within the complex region. Assuming that the size of the cover image, I , is $M \times M$, the detailed steps involved in the RPDM are described below.

Step 1: According to Formula (2), an $M \times M$ sized image, B , is generated for recording the position of the reference pixel, where Δ is the number of pixels between reference and non-reference pixels. If the pixel is a reference pixel, then the relative position of the image B is recorded as 1; if not it is recorded as 0. In Fig. 7, $\Delta = 3$.

$$B_{i,j} = \begin{cases} 0, & \text{mod}(i, \Delta) = 0 \text{ and } \text{mod}(j, \Delta) = 0 \\ 1, & \text{otherwise} \end{cases} \quad (2)$$

Step 2: If the conditions $B_{i,j} = 0, \text{mod}(i/\Delta + j/\Delta, 2) = 0$, and $\text{Range}(I_{i-\Delta,j}, I_{i,j-\Delta}, I_{i+\Delta,j}, I_{i,j+\Delta}) < T_0$ hold, then $I_{i,j}$ is within a smooth region. Update $B_{i,j} = 1$.

Step 3: The pixel value, $I_{i,j}$, satisfying $(0 \leq i + \Delta, j + \Delta \leq M)$ in the cover image, I , shows that the pixel position has a pixel value in the right and lower intervals Δ distance. If $I_{i,j}$ is $\text{Range}(I_{i,j}, I_{i+\Delta,j}, I_{i,j+\Delta}, I_{i+\Delta,j+\Delta}) > T_1$, then $I_{i,j}$ is within a complex region. In this case, the pixel values $B_{i',j'}$ in the range $(B_{i',j'}, i \leq i' \leq i + \Delta, j \leq j' \leq j + \Delta)$ are all set to 0, which means that $I_{i,j}$ is a reference pixel.

The cover pixels of 0 or 255 are modified to 1 or 254. The location of the pixel is then recorded in a location map, and the location map is compressed by run-length encoding; the result is expressed as L_M . And L_s is the bit stream of concatenate L_M and the secret message, S . The modified original image, I'' , is used to generate a bitmap, B , using RPDm. And classify the bits of the image, B , into B_0 and B_1 classes. The pixel position, $(i, j) \in B_0$, since $B_{ij} = 0$; $(i, j) \in B_1$, because $B_{ij} = 1$. An interpolation method is apply to generate the interpolation image, P and the interpolation error $E_{ij} = I''_{ij} - P_{ij}$ is calculated using when satisfying $(i, j) \in B_1$.

The embedding rules are as follows. If $E_{ij} = p_e^+$ or $E_{ij} = p_e^-$, secret data bit b L_s is embedded through Formula (3); if $E_{ij} \neq p_e^+$ or $E_{ij} \neq p_e^-$, the interpolation error is shifted by Formula (4) and the result is recorded in E' . In Formula (3), b is extracted one bit from L_s and p_e^+ and p_e^- is the interpolation error value that occurs most frequently and second-most frequently, respectively. Finally, the modified interpolation error, E' , and the interpolation image, P , are added as the stego image, I' .

$$E'_{ij} = \begin{cases} E_{ij}, b = 0 \\ p_e^+ + 1, b = 1 \text{ and } E_{ij} = p_e^+ \\ p_e^- - 1, b = 1 \text{ and } E_{ij} = p_e^- \end{cases} \quad (3)$$

$$E'_{ij} = \begin{cases} E_{ij} + 1, E_{ij} > p_e^+ \\ E_{ij} - 1, E_{ij} < p_e^- \end{cases} \quad (4)$$

The process of extracting the secret message and restoring the image is using RPDm to generate the image, B , from the stego image, I' . Next, the interpolation image, P , is obtained with reference to the image, B . The embedded secret message can be obtained using $E'_{ij} = I'_{ij} - P_{ij}$, and the embedded bits, b , is extracted from the pixel value, E'_{ij} , in the interpolation error, E' , using Formula (6). After all the bits, b , have been extracted, L_M and S are obtained from the lengths of L_M and S .

$$b = \begin{cases} 0, E'_{ij} = p_e^+ \text{ or } E'_{ij} = p_e^- \\ 1, E'_{ij} = p_e^+ + 1 \text{ or } E'_{ij} = p_e^- - 1 \end{cases} \quad (6)$$

After the secret message, S , has been obtained, the interpolation error, E' , with the embedded secret message is restored to the interpolation error, E , without embedding the secret message, according to Formula (7),

$$E_{ij} = \begin{cases} E'_{ij} - 1, E'_{ij} > p_e^+ \\ E'_{ij} + 1, E'_{ij} < p_e^- \\ E'_{ij}, \text{ otherwise} \end{cases} \quad (7)$$

By adding the interpolation error, E , and the interpolation image, P , the modified cover image, $I''_{i,j}$, is obtained. Eventually, the cover image, I , is restored by modifying the pixel values, $I''_{i,j}$, of 1 and 254 back to 0 and 255 according to L_M .

Example 4. Assuming that the image to be embedded is A , the thresholds for smoothing and complex regions are $T_0 = 5$ and $T_1 = 50$, respectively, and the secret message, S , is 0110. Firstly, the binary image, B , is generated by RPDM, and the interpolation image, P , is obtained using the binary image, B , as a reference. The cover image, A , and the interpolation image, P , are subtracted to obtain an interpolation error image, E . The secret message, S , is embedded into the interpolation error image, E , by the Formula (4). The modified interpolation error image, E' , is then added to the interpolation image, P , as the stego image, A' . The embedding procedure in this example is shown in Fig. 7 and the process used to extract the secret message is shown in Fig. 8.

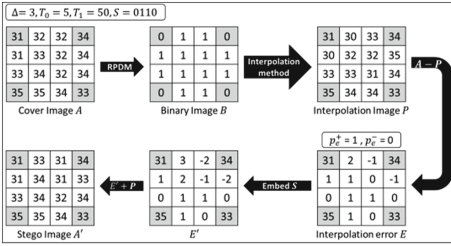


Fig. 7. Example of embedding procedure.

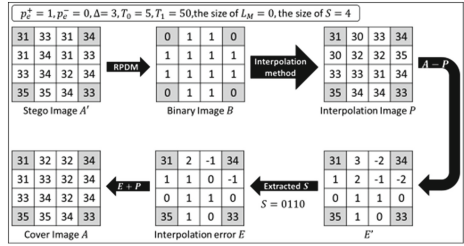


Fig. 8. Example of extraction procedure.

3 Comparison and Analysis

A considerable amount of research has focused on embedding a secret message in the texture features of the image to ensure reversibility and to achieve a better image quality and higher payload. In addition, a complex or smooth region within the embedded secret message has also been proposed. Here we compare the image quality (PSNR) and embedding rate (bpp) of each parameter according to whether the method is reversible, characteristic, or whether it has an image texture detection technique, as shown in Table 1.

In relation to the irreversible data hiding method in Table 1, under the parameter setting, the result of Chen et al. method [1] is PSNR = 37.5 dB and payload = 2.10 bpp. In relation to the limitations of Chen et al. study, Lee et al. proposed an improvement, in which the edge information is not recorded in the image, hybrid edge detection is not used, and only the pixel value of the four MSBs uses ED-MOF edge detection. In addition, the secret message is embedded in the 4 LSBs of the pixel value to increase the amount of embedding. It can be seen that the PSNR of Lena is increased by about 2.89 dB and that the embedding rate is increased by 0.04 bpp in the case of the reduced parameter, y. Bai et al. also improved the limitations inherent in the study of Chen et al., but this method is not limited to the edge detection method. We compare the results using Canny, Sobel, and Fuzzy, respectively, and although the results of the image quality are slightly

Table 1. Comparison of data hiding schemes based on image texture detection.

	Chen et al. [1]	Lee et al.[2]	Bai et al. [3]			Hong and Chen [4]
Parameters	$x = 4, y = 3, n = 2$	$x = 4, y = 2$	$x = 4, y = 3$	$x = 4, y = 3$	$x = 4, y = 3$	$T_0 = 8, T_1 = 60$
Block size	2×2	—	—			4×4
PSNR (dB)	Lena	Lena	Lena	Lena	Lena	Lena
	37.50	40.39	38.34	38.34	40.16	49.98
Embedding rate	2.10	2.14	3.11	3.05	2.79	0.18

lower than those of Lee et al., the embedding rate is improved and the maximum embedding rate is 3.11.

In relation to reversible data hiding, Hong and Chen's method proposed RPDM to detect the image texture. In this method, the secret information is embedded in the smooth region of the image rather than in the complex region of the image edge. Because it is reversible information hiding, so the embedded rate than the irreversible three methods are much lower. The embedding rate is 0.18 bpp, but the image quality is relatively high, with PSNR of 49.98 dB.

4 Conclusions

This paper studies the use of image texture to embed a secret message via data hiding technology. Chen et al. proposed an innovative method that uses hybrid edge detection to obtain edge information and LSB replacement to hide most of the edge information and the secret message in the edge pixels. However, the methods of Lee et al. and Bai et al. use the MSBs of extracted pixels to detect the edges, and embedding edge information is thus not necessary. As a whole, the embedding rate of Bai et al.'s method is superior and it reaches 3.11 bpp when Canny edge detection is used. However, this method is an irreversible data hiding method. As a reversible method, the image quality of Hong and Chen's method is superior, but because of reversibility the amount is lower. Therefore, despite the improvements made in image-based texture data hiding technologies in recent years, the embedding capacity requires a considerable amount of future research and is an important and challenging subject for researchers in this field.

Acknowledgements. This research was partially supported by the Ministry of Science and Technology of the Republic of China under the Grants MOST 105-2221-E-324-014.

References

1. Chen, W.J., Chang, C.C., Le, T.H.N.: High payload steganography mechanism using hybrid edge detector. *Expert Syst. Appl.* **37**(4), 3292–3301 (2010)
2. Lee, C.F., Chang, C.C., Tsou, P.L.: Data hiding scheme with high embedding capacity and good visual quality based on edge detection. In: 2010 Fourth International Conference on Genetic and Evolutionary Computing (ICGEC), pp. 654–657. IEEE (2010)
3. Bai, J., Chang, C.C., Nguyen, T.S., Zhu, C., Liu, Y.: A high payload steganographic algorithm based on edge detection. *Displays* **46**, 42–51 (2016)
4. Hong, W., Chen, T.S.: Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism. *J. Vis. Commun. Image Represent.* **22**(2), 131–140 (2011)
5. Kang, C.C., Wang, W.J.: A novel edge detection method based on the maximizing objective function. *Pattern Recogn.* **40**(2), 609–618 (2007)

Advances in Intelligent Information Hiding and
Multimedia Signal Processing
Proceedings of the Thirteenth International Conference
on Intelligent Information Hiding and Multimedia Signal
Processing, August, 12-15, 2017, Matsue, Shimane,
Japan, Part I

Pan, J.-S.; Tsai, P.-W.; Watada, J.; Jain, L.C. (Eds.)

2018, XVII, 451 p. 237 illus., Hardcover

ISBN: 978-3-319-63855-3