Improved Exploiting Modification Direction Method by Modulus Operation

Ki-Hyun Jung
School of Computer Informatiion, Yeungjin College
218 Bokhyun-Dong, Buk-Gu, Daegu 702-721, Republic of Korea
kingjung@paran.com

Kee-Young Yoo
Department of Computer Engineering, Kyungpook National University
1370 Sankyuk-Dong, Buk-Gu, Daegu 702-701, Republic of Korea
yook@knu.ac.kr

Abstract

The EMD method proposed by Zhang and Wang fully exploited modification directions. Modifications in different directions were used to represent different secret data. According to the experimental results, the highest capacity was demonstrated in the 5-ary notational system, where only one secret digit is embedded for each two pixels. But this is an inefficient method because it can be hidden more secret data without revealing to the human visual system. To improve an embedding capacity, Chang et al. proposed two-stage EMD method, Lee et al. restricted to 8-ary embedding for the EMD method, and also Lee et al. segmented the pair of cover data into two parts to embed higher secret data. But still have a room for hiding more secret data. This paper proposes an improved method of the EMD method to hide more secret data while maintaining a high PSNR value. The proposed method can embed secret bit on every pixel of cover data. The experimental results demonstrate that the proposed method has a high capacity and good visual quality.

1. Introduction

As the computer and communication technology grow up rapidly, the digital contents like images, audio, and video are distributed easily to the internet. However, this also causes substantial financial damage and becomes an imperative concern of copyright protection. To prevent digital contents from being intercepted by unauthorized parties is a critical demand in information security. Data hiding or information hiding techniques have generated much interest on that. The most important requirement in data hiding is that the presence of the hidden message be undetectable. Secret data can be hidden many different ways in images. Generally common approaches are categorized as least significant bit insertion, masking and filtering, and algorithms and transformations [6][7]. LSB insertion is a common method that replaces two or more of the least significant bits of each pixel. Masking and filtering methods embed secret data in significant areas, so the secret data are more integral to the cover image than hidden in the noise level as in the LSB substitution

method. On the internet, high compression quality images are becoming more abundant, so embedding methods applied to transformation algorithms like DCT, DFT, and DWT were proposed. The primary challenge of hiding data in other cover data is a large amount of data that requires a special data embedding method that offers high capacity as well as transparency and robustness. The peak signal-to-noise ration (PSNR) is used to judge the quality of the embedded image. In general, if the PSNR value is higher than the standard measurement of 30 dB, then the secret data which is embedded in the cover data is imperceptible to human vision.

This paper proposes a method that yields a high capacity by improving the EMD embedding method proposed by X. Zhang and S. Wang and demonstrates the experimental results have high quality than four methods related to the EMD method which is described in Section 2.

This paper is organized as follows. Section 2 reviews the EMD and other embedding methods which improved the EMD method. In Section 3, our proposed method is described. In Section 4, the experimental results are presented and discussed. Finally, the conclusions are presented in Section 5.

2. Related Work

Steganographic embedding by exploiting modification directions (EMD) requires that each secret sub-stream in a (2*n*+1)-ary notational system is carried on *n* cover pixels, where *n* is a system parameter [17]. For high capacity, the two-stage, the 8-ary EMD, and pixel segmentation strategy methods were proposed [5][10][11]. In this section, the EMD method and three methods which proposed to improve a high quality than the EMD method are described.

2.1. EMD Method

Assume that gray pixel values of the cover images are grouped into g_1, g_2, ..., g_n, each group is segmented into *L* bits, and the decimal value of each secret piece is represented by *K* digits in a (2*n*+1)-ary notational system.

$$L = \lfloor K \times log_2 (2n+1) \rfloor \tag{1}$$

In this system, let a secret digit be d and assume an extraction function $f(g_1, g_2, ..., g_n)$ as a weighted sum modulo (2*n*+1). The difference value s is calculated as $s = d - f$.

$$f = f(g_1, g_2, ..., g_n) = [\sum_{i=1}^{n} (g_i \times i)] \; mod \; (2n+1) \tag{2}$$

If $f = d$, no modification is needed. In the case of $f \neq d$ and $s \leq n$, increase the value of g_s by 1. If $f \neq d$ and $s > n$, decrease the value of g_{2n+1-s} by 1.

In the extracting process, let the stego data be g'_1, g'_2, ..., g'_n for each sub-group. A secret digit d is calculated by Eq. (3).

$$d = f(g'_1, g'_2, ..., g'_n) = [\sum_{i=1}^{n} (g'_i \times i)] \; mod \; (2n+1) \tag{3}$$

For example, let $n = 2$, g_1=104, g_2=11. When d is 1_5, $f = f(g_1, g_2) = (104 \times 1 + 11 \times 2) \; mod \; 5 = 126 \; mod \; 5 = 1$. Since f is equal to d, there is no change, so $g'_1 = 104$, $g'_2 = 11$. In extraction, $d = f(g'_1, g'_2) = (104 \times 1 + 11 \times 2) \; mod \; 5 = 126 \; mod \; 5 = 1$, so a secret digit $d = 1$ is extracted. When d

value is 2_5, f = 1 and $s = d - f = 2 - 1 = 1$. Since this case belongs to the case $f \neq d$ and $s \leq n$, a new pixel value is obtained by $g_s = g_1 + 1 = 104 + 1 = 105$ and so $g'_1 = 105$. In extraction, $d = f(g'_1, g'_2) = (105\times1 + 11\times2) \ mod\ 5 = 127 \ mod\ 5 = 2$, so a secret digit d = 2 is extracted. When d is 4_5, f = 1 and $s = d - f = 4 - 1 = 3$. Since this belongs to the case $f \neq d$ and $s > n$, a new pixel value is obtained by $g_{2n+1-s} = g_2 - 1 = 11 - 1 = 10$ and so $g'_2 = 10$. In extraction, $d = f(g'_1, g'_2) = (104\times1 + 10\times2) \ mod\ 5 = 114 \ mod\ 5 = 4$, so a secret digit d = 4 is extracted. If n is set to 2 in the EMD embedding method, only one secret digit is embedded for two consecutive pixels, where the secret is converted to its 5-ary value. This is less efficient and yields a lower capacity compared with other embedding methods like LSB substitution which embeds 2 or 3 bits for one pixel without impinging on the human visual system.

2.2. Two-stage EMD Method

In the two-stage method, the gray values of pixels g_1, g_2, ..., g_n are divided into buckets with an equal interval size, m like as $\lfloor g_1/m \rfloor$, $\lfloor g_2/m \rfloor$, ..., $\lfloor g_n/m \rfloor$. f and d values are calculated by Eq. (1) and (2), where the new gray value of pixel is used instead of g_i. After first stage embedding, the original EMD embedding algorithm is applied to n pixels on the second stage. If the bucket number of the pixel is changed, the second stage can not be allowed. This method provide about two times capacity larger than the EMD and can hide the largest secret data when m = 2.

2.3. The 8-ary EMD Method

Lee et al. proposed high quality and capacity method by transforming secret messages into the 8-ary notational system, and the cover image is grouped into two sequence pixels, g_1 and g_2 for all pixels.

$$f_e = (g_1 \times 1 + g_2 \times 3) \ mod\ 8 \tag{4}$$

In this method, one 8-ary secret digit can be embedded by two cover pixels, which only one pixel is increased or decreased by one if the value of extraction algorithm is not equal. Compared with the EMD method, the embedding capacity is 1.5 times without loss of visual quality and security.

2.4. Pixel Segmentation Strategy EMD Method

Lee et al. proposed an improvement of the EMD method by pixel segmentation strategy which could hide large payloads [10]. In the proposed method, each secret bit in a (2n+1)-ary notational system was carried by a pair of cover data. The embedding method segmented the pair of cover data into two parts: a vector of coordinates (VCA) and a coordinate vector modification area (VMA). For two pixel group g_i and g_j, each pixel consists of most significant bits and least significant bits which are denoted as g_i^{msb}, g_j^{msb}, g_i^{lsb}, and g_j^{lsb}. VCA are defined as the g_i^{msb} + g_j^{msb} bits and VMA are the $16 - (g_i^{msb} + g_j^{msb})$ bits. For given n positive integer which sub-group number of VCA, extraction function f is given as Eq. (2). If a secret digit d is equal to f, no modification is needed. For the difference value $s = d - f$, when s is greater than n, the value of sub-group $g_{(2n+1)-s}$ has to be logically decreased by one, otherwise the value of g_s has to be increased by one. The embedding rate $R = log_2(2n+1)/2$ was greater than that of $R = log_2(2n+1)/n$ which the EMD embedding method proposed when n got larger without loss of quality and security.

Though the embedding methods above mentioned have high quality for the resulted image, it is possible to improve the embedding capacity. This paper proposes an improved embedding method

for exploiting modification direction, which yields a high capacity and good PSNR compared with other methods relating to the EMD.

3. Proposed Method

The main idea of the proposed data hiding method is that each secret digit in a $(2n+1)$-ary notational system can be carried by one cover pixel. By using one pixel for cover data, the method achieves a capacity double that of the EMD method.

3.1. Embedding Procedure

For a pixel value, g_i on each cover data, the function value f is calculated by Eq. (5), where $|x| \leq n$. If the value of a pixel falls between $0 \leq g_i \leq 1$ and $254 \leq g_i \leq 255$ for each, then x is selected satisfying the condition $0 \leq x < 2n+1$ and $-(2n+1) < x \leq 0$ respectively.

$$f = (g_i + x) \; mod \; (2n+1) \tag{5}$$

A new pixel value g_i' is obtained by Eq. (6), where the value x is selected to satisfy the $f = d$ condition.

$$g_i' = g_i + x \tag{6}$$

For example, let $n = 2$, $g_1 = 153$, and $d = 2_5$. In the first case, f is calculated by $f = (g_1 + x) \; mod \; (2n+1) = (153+2) \; mod \; 5 = 0$, $(153+1) \; mod \; 5 = 4$, $(153+0) \; mod \; 5 = 3$, $(153+(-1)) \; mod \; 5 = 2$, $(153+(-2)) \; mod \; 5 = 1$ for each x value. Then, since f is equal to d when $x = -1$, a new pixel value $g_1' = g_1 + x = 153 + (-1) = 152$ is obtained as shown Fig. 1.

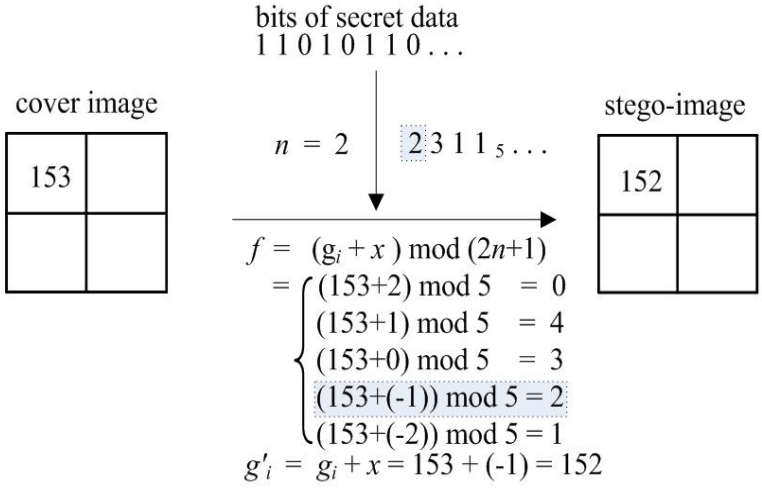


Figure 1. An example of the embedding method

3.2. Extracting Procedure

In the extraction method, a secret digit d is calculated by Eq. (7).

$$d = g_i' \ mod \ (2n+1) \tag{7}$$

For the embedding result depicted in Fig. 2, a secret digit $d = g_i' \ mod \ (2n + 1) = 152 \ mod \ 5 = 2$ is calculated directly.

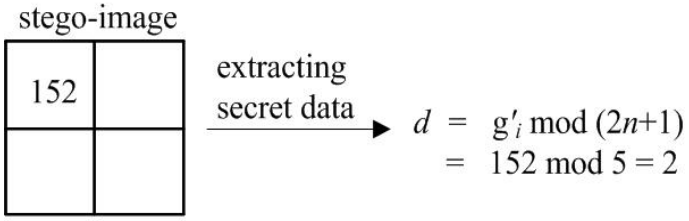


Figure 2. An example of the extracting method

Consider the pixel value belongs to $0 \leq g_i \leq 1$. Let $n = 2$, $g_1 = 0$, and $d = 4_5$, then f is calculated by $f = (g_1 + x) \ mod \ (2n + 1) = (0 + 0) \ mod \ 5 = 0, (0 + 1) \ mod \ 5 = 1, (0 + 2) \ mod \ 5 = 2, (0 + 3) \ mod \ 5 = 3, (0 + 4) \ mod \ 5 = 4$ for each x value. The $x = 4$ is selected and a new pixel value $g_1' = g_1 + x = 0 + 4 = 4$ is obtained. On the extracting process, $d = g_i' \ mod \ (2n + 1) = 4 \ mod \ 5 = 4$ can be calculated directly, In the case of $254 \leq g_i \leq 255$. Let $n = 2$, $g_1 = 254$, and $d = 4_5$, then f is calculated by $f = (g_1 + x) \ mod \ (2n + 1) = (254 + (-4)) \ mod \ 5 = 0, (254 + (-3)) \ mod \ 5 = 1, (254 + (-2)) \ mod \ 5 = 2, (254 + (-1)) \ mod \ 5 = 3, (254 + 0) \ mod \ 5 = 4$. Finally, if the $x = 0$ is selected, then the new pixel $g_1' = g_1 + x = 254 + 0 = 254$ is obtained. Also, $d = g_i' \ mod \ (2n + 1) = 254 \ mod \ 5 = 4$ can be extracted on the receiver.

4. Experimental Results

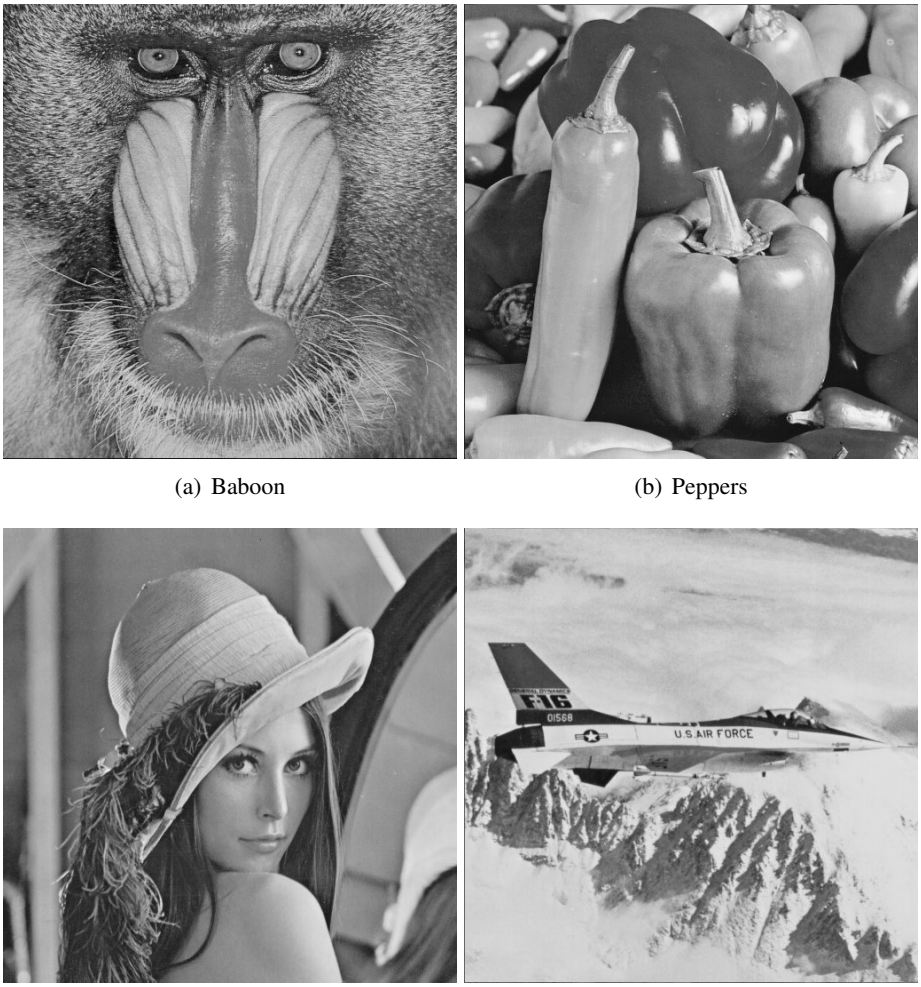
The peak signal-to-noise ratio (PSNR) is employed to evaluate the stego-image quality. If the PSNR for the embedding range is higher than the standard measurement of 30 dB, the secret which is stored behind the host image is imperceptible to the human visual system. Let width and height of cover image be w and h respectively.

$$PSNR \ = \ 10 \log_{10} 255^2 / \ MSE \tag{8}$$

Where *MSE* is the mean square error, which is defined as

$$MSE = \sum_{i=1}^{w \times h} (g_i - g_i')^2 / (w \times h) \tag{9}$$

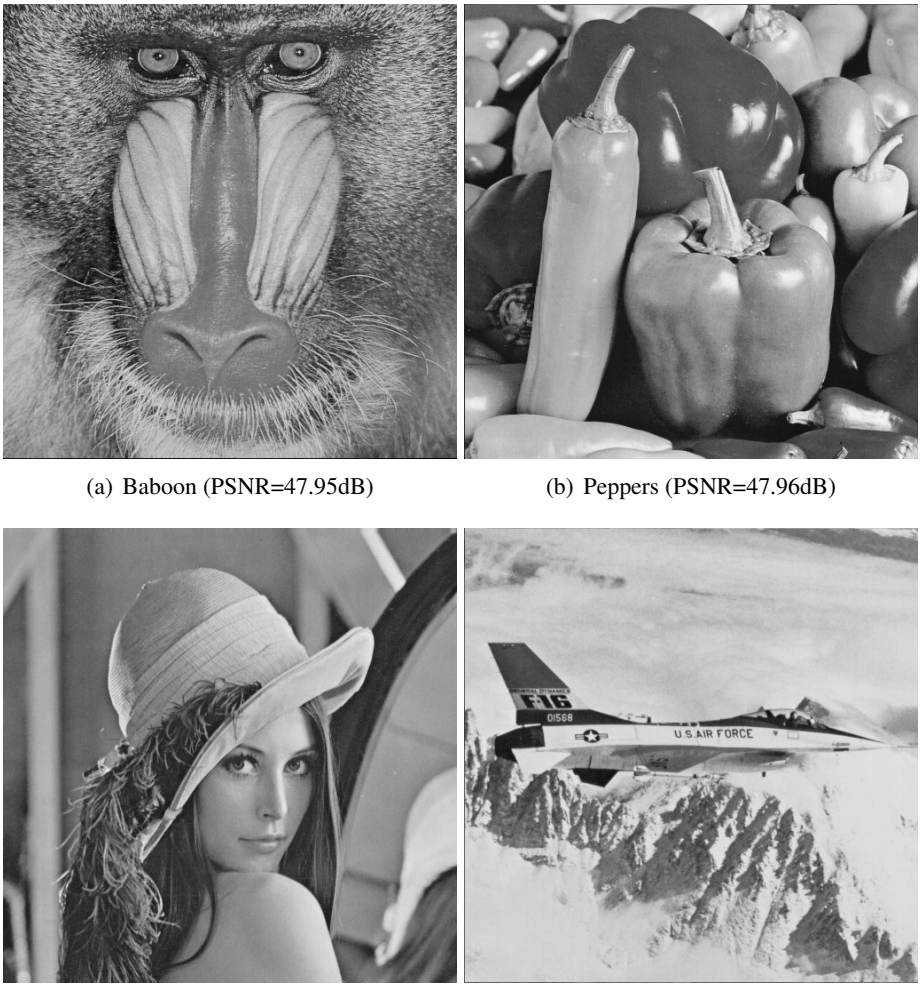
In our experiments, the four 512×512 gray images shown in Fig. 3 were used as cover data. Randomized data was used as secret data for each cover image.



(a) Baboon (b) Peppers

(c) Lena (d) Airplane

Figure 3. Four cover images



(a) Baboon (PSNR=47.95dB) (b) Peppers (PSNR=47.96dB)

(c) Lena (PSNR=47.92dB) (d) Airplane (PSNR=47.97dB)

Figure 4. Four stego-images for the proposed method

Table 1. The results of comparison with four EMD methods

Cover image	EMD		Two-stage EMD		The 8-ary EMD		Lee et al.'s EMD		Proposed	
	Capacity (byte)	PSNR (dB)	Capacity (byte)	PSNR (dB)	Capacity (byte)	PSNR (dB)	Capacity (byte)	PSNR (dB)	Capacity (byte)	PSNR (dB)
Baboon	45,551	51.80	91,012	41.87	87,374	44.36	57,006	44.28	91,141	47.95
Peppers	45,703	51.81	91,257	44.65	87,624	52.11	57,015	44.32	91,261	47.96
Lena	45,568	51.80	91,199	44.63	87,215	52.11	57,461	44.31	91,151	47.92
Airplane	45,625	51.79	91,213	44.62	87,628	52.1	55,239	44.45	91,197	47.97

Table 1 shows the results of detailed comparisons of three methods in terms of PSNR and capacity with different cover images. According to the table, the proposed method has higher capacity and good quality compared with other exploiting modification direction methods. The proposed method can hide 91,129 bytes sustaining 47.95 dB on average. Compared with the EMD method, the proposed method can hide more than 45,558 bytes. For the two-stage EMD method, the image quality is higher 4.01 dB and 12.5 bytes higher capacity on average. Also for the 8-ary and the pixel segmentation strategy EMD method, the proposed method can embed 3,793 and 34,449 bytes higher respectively.

The experimental results show that the stego-image after embedding secret data has 47.95 dB on average for the image quality, so the secret data are difficult to be detected by the human visual system.

5. Conclusions

We have proposed a data hiding method to improve the embedding capacity by exploiting modification direction proposed by Zhang and Wang. In the EMD embedding method, only one secret digit was embedded for two consecutive pixels, and the secret digit was converted to 5-ary value before embedding, which had the highest capacity. Three embedding methods like as the two-stage EMD method, the 8-ary EMD method, and pixel segmentation strategy EMD method were proposed to embed higher secret data, but still had a room for hiding more secret data. The proposed method for improving the capacity of the exploiting modification direction method could embed a secret digit in a $(2n+1)$-ary notational system on every pixel of the cover image. Our experimental results have shown that the proposed method could embed more secret data and obtained good image quality, which achieved 91,129 bytes and 47.95 dB on average.

References

[1] R. J. Anderson and F. A. P. Petitcolas. On the limits of steganography. *IEEE Journal on Selected Areas in Communications*, pages 474–481, 1998.

[2] W. Bender, N. Morimoto, and A. Lu. Techniques for data hiding. *IBM Systems Journal*, pages 313–336, 1996.

[3] T. D. K. C. C. Chang and Y. C. Chou. Reversible information hiding for (vq) indices based on locally adaptive coding. *Journal of Visual Communication and Image Representation*, pages 2123–2129, 2009.

[4] C. Y. W. C. H. Yang and S. J. Wang. Adaptive data hiding in edge areas of images with spatial (lsb) domain systems. *IEEE Transactions on Information Forensics and Security*, pages 488–497, 2008.

[5] C. C. Chang, W. L. Tai, and K. N. Chen. Improvements of EMD embedding for large payloads. *IIHMSP*, pages 473–476, 2007.

[6] N. F. Johnson and S. Jajodia. Exploring steganography: seeing the unseen. *Computer Practices*, pages 26–34, 1998.

[7] K. H. Jung, J. G. Yu, S. M. Kim, K. J. Kim, J. Y. Byun, and K. Y. Yoo. The hiding of secret data using the run length matching method. *LNCS, KES-AMSTA*, pages 1027–1034, 2007.
[8] T. M. T. K. C. Chang, P. S. Huang and C. P. Chang. Adaptive image steganographic scheme based on tri-way pixel-value differencing. *Systems, Man and Cybernetics, IEEE*, pages 1165–1170, 2007.
[9] A. Ker. Steganalysis of LSB matching in grayscale images. *IEEE Signal Processing Letters*, pages 441–444, 2005.
[10] C. F. Lee, C. C. Chang, and K. H. Wang. An improvement of EMD embedding method for large payloads by pixel segmentation strategy. *Image and Vision Computing*, 2008.
[11] C. F. Lee, Y. R. Wang, and C. C. Chang. A steganographic method with high embedding capacity by improving exploiting modification direction. *IIHMSP*, pages 497–500, 2007.
[12] J. Mielikainen. LSB matching revisited. *IEEE Signal Processing Letters*, pages 285–287, 2006.
[13] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn. Information hiding - a survey. *Proceedings of the IEEE, special issue on protection of multimedia content*, pages 1062–1078, 1999.
[14] Z. Wang and A. C. Bovik. A universal image quality index. *IEEE Signal Processing Letters*, pages 81–84, 2002.
[15] D. C. Wu and W. H. Tsai. A steganographic method for images by pixel-value differencing. *Pattern Regcognition Letters*, pages 1613–1626, 2003.
[16] C. H. Yang and C. Y. Weng. A steganographic method for digital images by multi-pixel differencing. *International Computer Symposium, IEEE*, pages 831–836, 2006.
[17] X. Zhang and S. Wang. Efficient steganographic embedding by exploiting modification direction. *IEEE Communications Letters*, pages 781–783, 2006.
[18] J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf. Modeling the security of steganographic systems. *2nd Workshop on Information Hiding*, pages 345–355, 1998.

Authors

Ki-Hyun Jung received his B.Sc. degree in Computer Engineering from Kyungpook National University in 1995 and the M.Sc. degree in Computer Engineering from Kyungpook National University in 1997, South Korea. He had been employed as a senior researcher at Agency of Defense Development, South Korea. He received the Ph.D. degree in Computer Science from Kyungpook National University in 2007, South Korea. Currently, he is an Assistant Professor at the School of Computer Information, Yeungjin College, South Korea. His current research interests are information hiding, watermarking, cryptography, and game programming.

Kee-Young Yoo received his B.Sc. degree in Education of Mathematics from Kyungpook National University in 1976 and the M.Sc. degree in Computer Engineering from Korea Advanced Institute of Science and Technology in 1978, South Korea. He received the Ph.D. degree in Computer Science from Rensselaer Polytechnic Institute in 1992, New York, USA. Currently, he is a Professor at the Department of Computer Engineering, Kyungpook National University, South Korea. His current research interests are cryptography, authentication technologies, smart card security, network security, DRM security, and steganography.