IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 29, 2017, accepted December 23, 2017, date of publication December 28, 2017, date of current version February 28, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2787803

Enhance Embedding Capacity of Generalized Exploiting Modification Directions in Data Hiding

YANXIAO LIU[1], CHINGNUNG YANG[2] (Senior Member, IEEE), AND QINDONG SUN[1]
[1]Department of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China
[2]Department of CSIE, National Dong Hwa University, Hualien 97401, Taiwan

Corresponding author: Yanxiao Liu (liuyanxiao@xaut.edu.cn)

This work was supported in part by the China National Natural Science Foundation under Grant 61502384 and Grant 61571360, in part by the Shaanxi Science and Technology Coordination and Innovation Project under Grant 2016KTZDGY05-09, and in part by the Innovation Project of Shaanxi Provincial Department of Education under Grant 17JF023.

ABSTRACT Data hiding is a useful technology to protect secret data through the Internet. Exploiting modification direction (EMD)-based data hiding uses a group of n cover-pixels to embed secret data. It achieves good image quality and high security level of resisting RS detection. However, the embedding capacity of EMD decreases fast when n increases. In 2013, a Generalized EMD (GEMD) was proposed to improve the embedding capacity of EMD, which is always more than 1 bpp (bits per pixel), and keeps the good stego-image quality. In this paper, we propose an enhanced GEMD by dividing a group of n cover-pixels into multiple groups. By this method, the embedding capacity can be further improved from GEMD. Our scheme maintains the good image quality and can resist the RS detection as well.

INDEX TERMS Data hiding, EMD (exploiting modification direction), GEMD (generalized exploiting modification direction), embedding capacity, RS detection.

I. INTRODUCTION

Data hiding can embed secret data into meaningful cover media such as image, audio and video. The least significant bit (LSB) replacement [1]–[3] is a common approach in data hiding that embeds secret data into meaningful cover-images. However, LSB replacement is vulnerable with some statistic analysis, such as RS detection [4]. In 2006, Zhang and Wang [5] introduced a new method of data hiding, which is called Exploiting Modification Direction (EMD) to resist the RS detection and improve the quality of cover image simultaneously. The EMD method is a block-wise data hiding, which groups n pixels into a block, and can embed a $(2n + 1)$-ary data by only modifying one pixel value ± 1 at most in this n-pixel group. The problem of EMD is that the embedding capacity will decrease fast with large n because of the redundancy caused by converting binary stream into $(2n + 1)$-ary notational system.

Many works [6]–[8] have been proposed to improve the embedding capacity of EMD. Some of those schemes used the combination of two or more different codes, some improved the imperceptibility using optimization method. In 2007, Lee *et al.* [9] introduced a LWC scheme that improves the embedding capacity from 1.16 to 1.5 for $n = 2$. However, this scheme is not flexible since the number n of cover-pixels in a group is fixed. In 2013, Kuo and Wang [10] proposed a generalized EMD (GEMD) method. GEMD still uses n cover-pixels in a group, and is capable of embedding $n + 1$ bits secret data. The embedding capacity of GEMD maintains over 1 bpp, and the quality of stego-image is good. In addition, GEMD can also resist RS detection as EMD. In 2017, Wang *et al.* [11] introduced a re-adjusted GEMD (RGEMD) that can embed $2n$ bits secret data into n-cover-pixels. However there are two shortcomings of [11], one is that it uses LSB replacement to embed $n-1$ bits secret data, which is vulnerable to RS detection; the other is that the quality of stego-image is worse than GEMD.

In this paper, we propose an enhanced GEMD by dividing the group of n cover-pixels into two sub-groups, each sub-group can embed secret data as GEMD. Using this approach, the embedding capacity of GEMD can be improved, and the properties of good stego-image quality and resistance from RS detection can be still maintained in our scheme. In addition, we extend the enhanced GMED to a generalized case that divide the group of n pixels into k sub-groups.

2169-3536 © 2017 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

The rest of this paper is organized as follows. In section II, we introduce some preliminaries, which includes the EMD and GEMD methods in data hiding. In section III, an enhanced GEMD is proposed to improve the embedding capacity from GEMD. Section IV gives the comparison of embedding capacity between EMD, GEMD and our scheme, as well as the experimental results of our scheme. The conclusion will be proposed in section V.

II. PRELIMINARIES

In this part, we introduce EMD and GEMD methods in data hiding, and show the embedding capacities of them respectively.

A. EMD

The EMD method [5] is a block-wise data hiding, which groups n pixels $(g_1, g_2, \ldots, g_n)$ into a block. The scheme can be divided into embedding phase and extracting phase, which is shown in following **Scheme 1**.

Scheme 1 EMD Method:

Embedding phase: Input: a cover-image I with n pixels $I = (g_1, g_2, \ldots, g_n)$, secret data s; Output: stego-image $I' = (g'_1, g'_2, \ldots, g'_n)$.

(1) Compute $f_{EMD} = [\sum_{i=1}^{n}(g_i \times i)] mod(2n+1)$, and transform s into $2n+1$-ary stream $s_{(2n+1)}$.

(2) Compute $d = (s_{(2n+1)} - f_{EMD}) mod(2n+1)$.

(3) If $(d = 0)$, $g'_i = g_i, i \in [1, n]$;
else if $(d \leq n)$, $g'_d = g_d + 1$, $g'_i = g_i, i \in [1, n]$, $i \neq d$;
else, $g'_{2n+1-d} = g_{2n+1-d} - 1$, $g'_i = g_i$, $i \in [1, n]$, $i \neq 2n+1-d$.
Output the stego-image: $I' = (g'_1, g'_2, \ldots, g'_n)$.

Extracting phase: Input: stego-image: $I' = (g'_1, g'_2, \ldots, g'_n)$; Output: secret data s.

(1) Compute $s_{(2n+1)} = f'_{EMD} = [\sum_{i=1}^{n}(g'_i \times i)] mod(2n+1)$.

(2) Transform $2n+1$-ary data $s_{(2n+1)}$ into binary stream s.

The embedding capacity of EMD is presented as $R_{EMD} = \frac{log_2(2n+1)}{n}$. When $n = 2$, EMD reaches its maximum embedding capacity 1.16 bpp, and the embedding capacity decreases fats when n increases. However, this result is not practical since the conversion from a binary stream into a $2n+1$-ary digits causes redundancy binary bits.

B. GEMD

Kuo and Wang [10], extended the scheme in [5] to a Generalized EMD (GEMD) that improved the embedding capacity. We give a description of GEMD as follows.

Scheme 2 GEMD:

Embedding phase: Input: a cover-image of n pixels $I = (g_1, g_2, \ldots, g_n)$, a secret s of $n+1$ bits; Output: a stego-image of n pixels $I' = (g'_1, g'_2, \ldots, g'_n)$.

(1) Compute $f_{GEMD} = [\sum_{i=1}^{n} g_i \times (2^i - 1)] mod 2^{n+1}$.

(2) Transform the $n+1$ bits secret s to decimal $s_{(10)}$.

(3) Compute $d = (s_{(10)} - f_{GEMD}) mod 2^{n+1}$.

- If $(d = 0)$, $g'_i = g_i, i = 1, 2, \ldots, n$.
- Else if $(d = 2^n)$, $g'_1 = g_1 + 1$, $g'_n = g_n + 1$, $g'_i = g_i$, $i = 2, 3, \ldots, n-1$.
- Else if $(0 < d < 2^n)$, transform d to binary $(b_n b_{n-1} \ldots b_0)_2$.

```
For($i = n; i \geq 1; i--$)
{ if($b_i == 0$ and $b_{i-1} == 1$) $g'_i = g_i + 1$;
else if ($b_i == 1$ and $b_{i-1} == 0$) $g'_i = g_i - 1$;
else $g'_i = g_i$ }
```

- Else $d' = 2^{n+1} - d$, transform d' to binary $(b_n b_{n-1} \ldots b_0)_2$

```
For($i = n; i \geq 1; i--$)
{ if($b_i == 0$ and $b_{i-1} == 1$) $g'_i = g_i - 1$;
else if ($b_i == 1$ and $b_{i-1} == 0$) $g'_i = g_i + 1$;
else $g'_i = g_i$ }
```

(4) Outputs stego-image: $I' = (g'_1, g'_2, \ldots, g'_n)$.

Extracting phase: Input: stego-image $I' = (g'_1, g'_2, \ldots, g'_n)$; Output: the $n+1$ bits secret s.

(1) The decimal secret $s_{(10)}$ can be extracted by: $s_{(10)} = f'_{GEMD} = [\sum_{i=1}^{n} g'_i \times (2^i - 1)] mod 2^{n+1}$.

(2) Transform $s_{(10)}$ into $n+1$ bits secret s.

Scheme 2 (GEMD) embeds a $n+1$ bits secret into n stego-pixels, the corresponding embedding capacity is $R_{GEMD} = \frac{n+1}{n}$. This embedding capacity always maintains over 1 bpp, which is enhanced from the embedding capacity of EMD.

III. ENHANCED GEMD WITH HIGHER EMBEDDING CAPACITY

In this part, we introduce an enhanced GEMD method to further improve the embedding capacity. In GEMD, a secret data of $n+1$ bits can be embedded using a n-pixel group cover image. In our scheme, a group of n-pixels is first divided into two sub-groups to embedding secret data. Through this approach, a $n+2$ bits secret data can be embedded instead of $n+1$ bits data in GEMD. Our scheme is described as follows.

Scheme 3: Enhanced GEMD

Embedding phase: Input: two cover-images $I_1 = (g_1, g_2, \ldots, g_{n_1})$, $I_2 = (h_1, h_2, \ldots, h_{n_2})$, $(n = n_1 + n_2)$ $n+2$ bits secret data s; Output: two stego-images $I'_1 = (g'_1, g'_2, \ldots, g'_{n_1})$, $I'_2 = (h'_1, h'_2, \ldots, h'_{n_2})$.

(1) Convert the $n+2$ bits data s into decimal $s_{(10)}$.

(2) Let $s_{(10)} = 2^{n_1+1} \times c + r$ where c and r are integers and $r < 2^{n_1+1}$.

(3) Embedding c, r into I_2, I_1 using the embedding approach in GEMD respectively, and output two stego-images I'_1, I'_2.

Extracting phase: Input: two stego-image: $I'_1 = (g'_1, g'_2, \ldots, g'_{n_1})$, $I'_2 = (h'_1, h'_2, \ldots, h'_{n_2})$; Output: $n+2$ bits secret data s.

(1) Extracting c and r from I'_2 and I'_1 respectively using the extraction approach in GEMD.

(2) Computing $s_{(10)} = 2^{n_1+1} \times c + r$.

(3) Converting $s_{(10)}$ into $n+2$ bits data s, and output s.

The correctness of our scheme is proved in following theorem.

Theorem 1: The enhanced GEMD can embed $n+2$ bits secret data into n cover-pixels.

Proof: In our scheme, n cover-pixels are divided into two groups I_1 and I_2 which has n_1 and n_2 cover-pixels respectively ($n = n_1 + n_2$). Suppose s is $n+2$ bits data, its corresponding decimal integer $s_{(10)}$ satisfies $s_{(10)} \in [0, 2^{n+2})$. It is easy to know that $s_{(10)}$ can be presented uniquely as:

$$s_{(10)} = 2^{n_1+1} \times c + r, (r < 2^{n_1+1}) \tag{1}$$

Since $2^{n+2} = 2^{n_1+1} \times 2^{n_2+1}$, c satisfies that $c < 2^{n_2+1}$. Therefore we can embed c, r into the cover-images with n_2, n_1 pixels respectively according to the embedding approach in GEMD. (see **Scheme 2**) When extracting the secret data, $c(< 2^{n_2+1})$ and $r(< 2^{n_1+1})$ can be extracted from I'_2 and I'_1 according to the extracting approach in GEMD, then $s_{(10)}$ can be computed in Eq (1). As a result, the $n+2$ bits secret data s can be converted from its decimal integer $s_{(10)}$. In Tab 1, we list all the value of c and r for 5-bits data.

Here we use an example to illustrate the embedding and extracting process of our enhanced GEMD. Let $n = 3$ and the cover-image is $I = (68, 72, 59)$. The secret data is $s = (11010)$ which is $n+2$ bits. First we divide I into two cover-images $I_1 = (68, 72)$ and $I_2 = (59)$ which has $n_1 = 2$ and $n_2 = 1$ pixels respectively. Then converting $s = (11010)$ into decimal $s_{(10)} = 26$, and it can be presented as $26 = 2^{n_1+1} \times 3 + 2$. Next we embed 3 and 2 into I_2 and I_1 using the embedding approach in GEMD respectively, and output $I'_1 = (69, 71)$, $I'_2 = (59)$. When extracting secret data, 3 and 2 can be extracted from I'_2 and I'_1 by: $3 = 59 \times (2^1 - 1) mod (2^2)$, $2 = (69 \times (2^1 - 1) + 71 \times (2^2 - 1)) mod 2^3$, then $s_{(10)}$ can be computed as $s_{(10)} = 2^{n_1+1} \times 3 + 2 = 26$, its corresponding binary presentation $s = (11010)$ is extracted.

Our scheme can embed $n+2$ bits secret data into n pixels, the corresponding embedding capacity is $R_{PRO} = \frac{n+2}{n}$. This embedding capacity is improved from $R_{GEMD} = \frac{n+1}{n}$. In addition, the enhanced GEMD can be also extended to a general case that all the n cover-pixels are divided into k groups instead of two group in **Scheme 3**. First the n cover-pixels are divided into k groups $I_1, I_2, \ldots, I_k$, each group has n_i, $i = 1, 2, \ldots, k$ pixels that $n = \sum_{i=1}^{k} n_i$. For any $n+k$ bits secret data s, it can be embedded using the following steps.

1 Convert s into decimal $s_{(10)}$.

2 Computing

$$\begin{aligned} s_{(10)} &= 2^{n_1+1} \times c_1 + r_1 \\ c_1 &= 2^{n_2+1} \times c_2 + r_2 \\ c_2 &= 2^{n_3+1} \times c_3 + r_3 \\ &\ldots \\ c_{k-2} &= 2^{n_{k-1}+1} \times c_{k-1} + r_{k-1} \end{aligned} \tag{2}$$

3 Embedding c_{k-1} into n_k cover-pixels in I_k, and embedding $r_i, i = 1, 2, \ldots, k-1$ into $I_1, I_2, \ldots, I_{k-1}$ respectively using embedding approach in GEMD.

TABLE 1. Values of c, r for all 5 bits data.

	$c=0$	$c=1$	$c=2$	$c=3$
$r=0$	00000	00001	00010	00011
$r=1$	00100	00101	00110	00111
$r=2$	01000	01001	01010	01011
$r=3$	01100	01101	01110	01111
$r=4$	10000	10001	10010	10011
$r=5$	10100	10101	10110	10111
$r=6$	11000	11001	11010	11011
$r=7$	11100	11101	11110	11111

When extracting the secret data, first extracting $r_1, r_2, \ldots, r_{k-1}$ and c_{k-1} from $I_1, I_2, \ldots, I_k$. Then $s_{(10)}$ can be computed according to Equation (2), the $n+k$ bits secret data s can be extracted.

The correctness of generalized enhanced GEMD is similar as **Scheme 3**. We only need to prove that $c_{k-1} < 2^{n_k+1}$ and $r_i < 2^{n_i+1}, i = 1, 2, \ldots, k-1$. In Equation (2), let $c_0 = s_{(10)}$, we have $c_{i-1} = 2^{n_i+1} \times c_i + r_i, i = 1, 2, \ldots, k-1$, it is easy to get that $r_i < 2^{n_i+1}, i = 1, 2, \ldots, k-1$. For each c_i, it satisfies that

$$c_i < \frac{c_{i-1}}{2^{n_i+1}}, i = 1, 2, \ldots, k-1 \tag{3}$$

Since $c_0 = s_{(10)} < 2^{n+k}$, we can get

$$c_i < 2^{(n-\sum_{j=1}^{i} n_j)+(k-i)}, i = 1, 2, \ldots, k-1 \tag{4}$$

From Equation (4), we can get $c_{k-1} < 2^{n_k+1}$. Therefore $r_i, i = 1, 2, \ldots, k-1$ and c_{k-1} can be embedded into n_i pixels in $I_i, i = 1, 2, \ldots, k$ using GEMD.

For example, suppose $n = 6$ and these n pixels are divides into $k = 3$ groups where $n_1 = 3, n_2 = 2, n_3 = 1$. $s = (101100101)$ is a $n+k = 9$ bits secret data, its decimal integer is $s_{(10)} = 357$. Then 357 can presented as

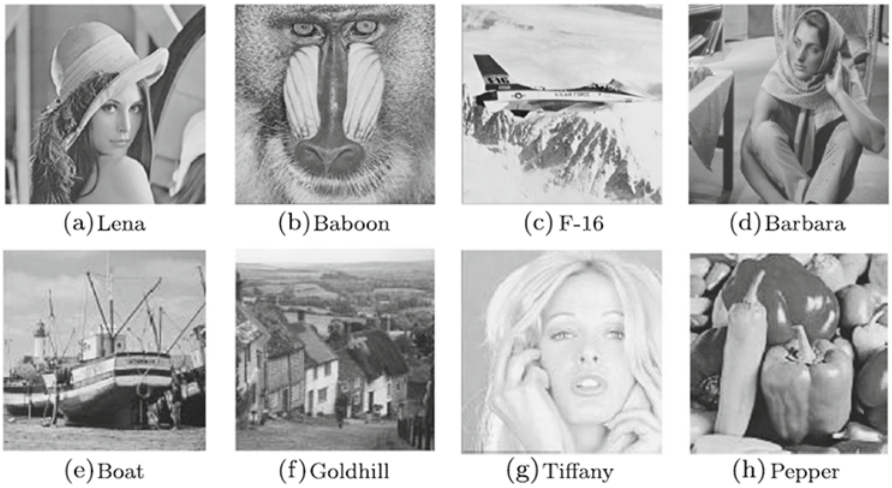
$$\begin{aligned} 357 &= 2^{n_1+1} \times 22 + 5 \\ 22 &= 2^{n_2+1} \times 2 + 6 \end{aligned} \tag{5}$$

Then $r_1 = 5$, $r_2 = 6$, $c_2 = 2$ are embedded into $n_1 = 3$, $n_2 = 2$, $n_3 = 1$ cover-pixels respectively. When extracting secret data, $r_1 = 5$, $r_2 = 6$, $c_2 = 2$ can be extracted from the three groups of stego-pixels, and then $s_{(10)} = 357$ can be computed from Equation (5), its corresponding $n+k = 9$ bits $s = (101100101)$ can be extracted successfully.

The embedding capacity of generalized enhanced GEMD is $\frac{n+k}{n}$. As the k increases, the embedding capacity will improve from **Scheme 3**, however more cover-pixel will change and the quality of stego-image will decrease.

IV. COMPARISONS AND EXPERIMENTAL RESULTS

In this part, comparisons of embedding capacities and stego-image qualities between EMD, GEMD and our enhanced GEMD are made to show the properties of data hiding. Section II gives the embedding capacities of EMD and GEMD, which are $R_{EMD} = \frac{log_2(2n+1)}{n}$ and $R_{GEMD} = \frac{n+1}{n}$ respectively. Our enhanced GEMD has embedding capacity of $R_{pro} = \frac{n+2}{n}$, which is improved from EMD and GEMD.


(a) Lena (b) Baboon (c) F-16 (d) Barbara

(e) Boat (f) Goldhill (g) Tiffany (h) Pepper

FIGURE 1. Eight 512 × 512 test cover images.

The following Tab 2 shows the embedding capacities of these three schemes for different n.

TABLE 2. Comparison of embedding capacities.

	EMD	GEMD	Enhanced GEMD
$n = 2$	1.16	1.50	2.00
$n = 3$	0.93	1.33	1.67
$n = 4$	0.79	1.25	1.50
$n = 5$	0.69	1.20	1.40
$n = 6$	0.61	1.16	1.33
$n = 7$	0.55	1.14	1.29
$n = 8$	0.51	1.12	1.25
$n = 9$	0.47	1.11	1.22
$n = 10$	0.43	1.10	1.20

The quality of stego-images is usually measured by Peak Signal to Noise Ratio (PSNR). The higher PSNR means the better quality of image. If PSNR is lower than 30 dB, the stego-image can be visually distinguished from the cover image. The PSNR and mean square error (MSE) are presented as following equation.

$$PSNR = 10 \times log_{10} \frac{255^2}{MSE}$$

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} (I(x, y) - I'(x, y))^2 \qquad (6)$$

where M and N represent the length and width of the image. In the experiment, eight 512 × 512 grayscale images (see Fig.1) are adopted as the cover images, and we use EMD, GEMD and Enhanced GEMD to embedding secret data. The PSNR values of stego-images from thes three schemes are shown in Tab.3.

Our scheme has lower PSNR than EMD and GEMD since more cover-pixels are changed with higher embedding capacity, and the PSNR in Enhanced GEMD still achieves good stego-image quality to avoid human eye detection.

TABLE 3. Comparison of PSNRs between three schemes.

	EMD	GEMD	Enhanced GEMD
$n = 2$	52.11	50.72	47.65
$n = 3$	53.57	50.79	47.69
$n = 4$	54.66	51.00	47.78
$n = 5$	55.53	51.09	47.85
$n = 6$	56.27	51.13	47.92
$n = 7$	56.87	51.15	47.99
$n = 8$	57.42	51.16	48.03
$n = 9$	57.90	51.16	48.10
$n = 10$	58.35	51.19	48.15

TABLE 4. Capacities and PSNRs of generalized enhanced GEMD.

	$k = 2$		$k = 3$		$k = 4$	
	capacity	PSNR	capacity	PSNR	capacity	PSNR
$n = 6$	1.33	47.92	1.50	45.31	1.67	43.01
$n = 7$	1.29	47.99	1.43	45.34	1.57	43.05
$n = 8$	1.25	48.03	1.38	45.38	1.50	43.07
$n = 9$	1.22	48.10	1.33	46.41	1.44	43.11
$n = 10$	1.20	48.15	1.30	46.44	1.40	43.13

In section III, we also introduced a generalized enhanced GEMD by dividing n cover-pixels into k groups. This approach can further improve the embedding capacity of enhanced GEMD, however the quality of stego-image will decrease when k increases. When using generalized enhanced GEMD to embedding secret data, one need to balance the embedding capacity and the quality of stego-image by choosing an appropriate parameter k. Normally, k is no more than 6, otherwise one can distinguish the difference between the steo-image and original image by human eyes. The Tab. 4 shows the embedding capacities and PSNRs of generalized enhanced GEMD.

V. CONCLUSION

Embedding capacity and quality of steo-image are two major concerns in data hiding schemes. GEMD method can embed $n+1$ bits data into n cover-pixels, it achieves high quality of stego-images and can resist RS detection which is an important approach in data hiding. In this paper, we introduce an enhanced GEMD by dividing the n cover-pixels into two groups. Our scheme can improve the embedding capacity of GEMD from $\frac{n+1}{n}$ bpp to $\frac{n+2}{n}$ bpp. The experimental results shows that our scheme also achieves high stego-image quality. In addition, we give an algorithm to extend the enhanced GEMD to a general case by dividing n cover-pixels into k groups. This generalized enhanced GEMD can further improve embedding capacity by choosing a larger parameter k, however the PSNR will decrease when k increases. One can use this approach to embed secret data by an appropriate k to balance the embedding capacity and the quality of stego-images.

REFERENCES

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

[2] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognit.*, vol. 34, no. 3, pp. 671–683, Mar. 2001.

[3] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Trans. Signal Process.*, vol. 51, no. 7, pp. 1995–2007, Jul. 2003.

[4] J. Fridrich, M. Goljan, and D. Rui, "Detecting LSB steganography in color, and gray-scale images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22–28, Oct./Dec. 2004.

[5] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.*, vol. 10, no. 11, pp. 781–783, Nov. 2006.

[6] X. Zhang, W. Zhang, and S. Wang, "Efficient double-layered steganographic embedding," *Electron. Lett.*, vol. 43, no. 8, pp. 482–483, Apr. 2007.

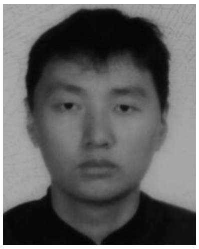
[7] X. Zhang, W. Zhang, and S. Wang, "A double layered 'plus-minus one' data embedding scheme," *IEEE Signal Process. Lett.*, vol. 14, no. 11, pp. 848–851, Nov. 2007.

[8] K. H. Jung and K. Y. Yoo, "Improved exploiting modification direction method by modulus operation," *Int. J. Signal Process., Image Process. Pattern*, vol. 2, no. 1, pp. 79–88, 2009.

[9] C.-F. Lee, Y.-R. Wang, and C.-C. Chang, "A steganographic method with high embedding capacity by improving exploiting modification direction," in *Proc. 3rd Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Nov. 2007, pp. 497–500.

[10] W.-C. Kuo and C.-C. Wang, "Data hiding based on generalised exploiting modification direction method," *Image Sci. J.*, vol. 61, no. 6, pp. 484–490, Nov. 2013.

[11] C.-C. Wang, W.-C. Kuo, Y.-C. Huang, and L.-C. Wuu, "A high capacity data hiding scheme based on re-adjusted GEMD," *Multimedia Tools Appl.*, vol. 8, pp. 1–15, 2017.



YANXIAO LIU received the Ph.D. degree in cryptography from Xi'dian University, China, in 2012. He is currently with the Department of Computer Science and Engineering, Xi'an University of Technology. He has authored over ten professional research papers on information security. His research interests include secret sharing scheme, secret image sharing, visual cryptography, and data hiding.

CHINGNUNG YANG (SM'11) received the B.S. and M.S. degrees from the Department of Telecommunication Engineering, National Chiao Tung University, and the Ph.D. degree in electrical engineering from National Cheng Kung University. He has been with National Dong Hwa University since 1999. He was a Visiting Professor with the University of Missouri–Kansas City, the University of Milan, and the University of Tokyo. He is currently a Professor with the Department of CSIE and a Fellow of the IET (IEE). He has done extensive researches on visual cryptography and secret image sharing, where he is currently the Chief Scientist in both areas. In fact, a very important innovation of visual cryptography, the probabilistic visual cryptography, was first proposed by Professor Yang. His areas of interest include error correcting code, multimedia security, cryptography, and information security. He has authored two books and has published over 200 professional research papers in the areas of information security and coding theory. In the meantime, he has served/is serving in international academic organizations. He was a recipient of the 2000, 2006, 2010, 2012, and 2014 Fine Advising Award in the Thesis of Master's/Ph.D. of Science by the Institute of Information and Computer Machinery. He serves as technical reviewers for over 40 major scientific journals in the areas of his expertise, and serves as editorial boards and editors of special issues for some journals. Also, he was invited as chairs, keynote speakers, and members of program committees for various international conferences.

QINDONG SUN received the Ph.D. degree from the School of Electronic and Information Engineering, Xi'an Jiaotong University, China. He is currently a Professor with the Department of Computer Science and Engineering, Xi'an University of Technology. His research interests include network information security, online social networks, and Internet of Things.