Multimed Tools Appl (2018) 77:6327–6341
DOI 10.1007/s11042-017-4541-0

A high capacity data hiding scheme based on re-adjusted GEMD

Chun-Cheng Wang[1] · Wen-Chung Kuo[2] · Yu-Chih Huang[3] · Lih-Chyau Wuu[2]

Received: 29 August 2016 / Revised: 19 January 2017 / Accepted: 21 February 2017 /
Published online: 6 April 2017

Abstract Steganography is a useful technology to protect secret data traveling through the Internet. Recently, Kuo and Wang proposed a useful data hiding scheme based on GEMD(Generalized Exploiting Modification Direction). They claim that the embedding capacity of their scheme is more than 1 bpp(bits per pixel) and keeps good stego-image quality. In addition, the GEMD scheme can prevent RS detection. However, the embedding capacity of GEMD decreases when pixel numbers in the group becomes large. To alleviate this shortcoming, we will propose a data hiding scheme which can embed extra secret data after the GEMD embedding procedure. The major contribution of the proposed scheme is the embedding capacity always maintains 2 bpp which is independent of the pixel numbers in the group. Finally, according to our experiments, our proposed scheme maintains good image quality and also prevents RS detection.

Keywords EMD(Exploiting modification direction) · GEMD(Generalized exploiting modification direction) · Embedding capacity · RS detection

✉ Wen-Chung Kuo
simonkuo@yuntech.edu.tw

[1] Graduate School of Engineering Science and Technology Doctoral Program, National Yunlin University of Science & Technology, Taiwan, Republic of China

[2] Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology, Taiwan, Republic of China

[3] Department of Information Management, Tainan University of Technology, Taiwan, Republic of China

1 Introduction

Because of the rapid growth of computer and internet technology, multimedia such as images, audio, and video are distributed through the Internet. How to protect digital content security is a very important issue. The two most common methodologies are cryptography and steganography which can maintain data security. Steganography can embed a secret message in a meaningful cover image and form a stego-image which is not apparent to other people. The most important characteristic is the imperceptibility. Another important characteristic is the capacity. If steganographic technology can embed more secret data in a cover image, the user transfers less stego-images and avoids the suspicions of unprivy people.

The most well known steganographic technology is the least significant bit(LSB) replacement method. This scheme is very simple, fast and has good stego-image quality. Unfortunately, it is not secure. There are many detection technologies which can detect LSB replacement methods. One famous of detection technology is RS detection [1]. In 2006, Zhang and Wang proposed a data hiding scheme based on Exploiting Modification Direction(EMD) [12]. The EMD scheme used n pixels for a group and only modified one pixel value $+1$ or -1 at most in a group. The most important contribution of EMD is that the image quality is very good and better than most data hiding schemes such as LSB replacement methods. But, there are two shortcomings. One is that it must transform the binary secret data to $(2n+1)$-ary to get full capacity before embedding by the using EMD method. The other is that the embedding capacity decreases fast when n increases. EMD maintains embedding capacity of slightly more than 1 bpp when $n = 2$. Afterwards, many similar EMD-type methods [2–11] were proposed. In 2007, Lee et al. proposed the LWC scheme [11] to improve the embedding capacity from 1.16 to 1.5 bpp when $n = 2$. However, it does not have the flexibility of changing pixel group size. In order to improve this shortcoming, the generalized EMD(GEMD) scheme [3] was proposed by Kuo et al. in 2013. The major contribution of GEMD scheme is that it used n pixels for a pixel group to embed (n+1) bits secret data. In other words, the embedding capacity of the GEMD scheme always maintains over 1 bpp. Specifically, the LWC scheme is the special case of GEMD scheme.

Besides the above benefits, the GEMD scheme can also prevent RS detection. In fact, the best embedding capacity of the GEMD scheme is 1.5 bpp when $n = 2$. Intuitively, the embedding capacity still decreases as n increases. In order to improve this shortcoming, a data hiding scheme based on re-adjusted GEMD method is proposed in this paper. We demonstrate that our scheme maintains embedding capacity at 2 bpp even when n increases and also maintains good image quality.

The rest of this paper is organized as follows: In Section 2, we will review the EMD [12], the LWC [11] and the GEMD schemes [3] briefly. Then, we introduce our proposed data hiding scheme and provide experimental results in Sections 3 and 4, respectively. Finally, some conclusions are given in Section 5.

2 Review data hiding schemes

The EMD type data hiding scheme maintains good stego-image quality and also prevents RS detection. In this section, we will introduce the EMD [12], LWC [11] and GEMD schemes [3] in detail.

2.1 EMD data hiding scheme [12]

In 2006, Zhang and Wang proposed a data hiding scheme based on Exploiting Modification Direction. They used n pixels for a group and define the extraction function as (1). They adjust one pixel value $+1$ or -1 at most to embed $(2n + 1)$-ary secret data.

$$f_{EMD}(g_1, g_2, \ldots, g_n) = \left[\sum_{i=1}^{n}(g_i \times i)\right] \mod (2n + 1), \tag{1}$$

where g_i is the i-th pixel value for adjusting, and n is the number of values required for implementing the selected pixels.

Algorithm 1 The EMD embedding algorithm

```
Input: cover image $I_c$ and secret data $s$
Output: stego-image $I_s$
 EMD-1 Divide $I_c$ into non-overlapping $n$ pixel groups and transform $s$ in to $(2n + 1)$-ary
    secret data stream $s'$.
 EMD-2 Use the cover pixel group and compute $f_{EMD}$ by (1).
 EMD-3 Obtain $(2n+1)$-ary data $s'_i$ from $s'$ and compute $d = (s'_i - f_{EMD}) \mod (2n+1)$.
 EMD-4 If $d \le n$, then $g'_d = g_d + 1$ and $g'_i = g_i \forall i \in \{1, 2, \cdots, n|i \neq d\}$, else
    $g'_{2n+1-d} = g_{2n+1-d} - 1$ and $g'_i = g_i \forall i \in \{1, 2, \cdots, n|i \neq (2n + 1 - d)\}$.
 EMD-5 Repeat from step EMD-2 until all secret data is embedded.
 Note $g_i$ is the cover pixel value and $g'_i$ is the stego-pixel value.
```

Example 1 Given three cover image pixels $(g_1, g_2, g_3) = (62, 63, 60)$ and secret data $s = (11)_2$, we can obtain output stego-image pixels $(g'_1, g'_2, g'_3) = (61, 63, 60)$ using the EMD embedding procedure as the following:

Step 1. Transform $s = (11)_2 = (3)_7$.
Step 2. Compute $f_{EMD} = (62 \times 1 + 63 \times 2 + 60 \times 3) \mod 7 = 4$.
Step 3. Compute $d = (3 - 4) \mod 7 = 6$.
Step 4. Compute $g'_{7-6} = 62 - 1 = 61$ because $d > n = 3$.

The stego-pixel value is $(g'_1, g'_2, g'_3) = (61, 63, 60)$. When the receiver gets the stego-pixel value, the secret data s is recovered by computing $s = f_{EMD} = (61 \times 1 + 63 \times 2 + 60 \times 3) \mod 7 = 3$ and transform $(3)_7$ to binary $(11)_2$.

The most important contribution of EMD is that the image quality is very good and embedding method by using the modulus function. However, there are two shortcomings. One is that it must transform the binary secret data to $(2n+1)$-ary to get full capacity before embedding by the using (1). The other is that the embedding capacity decreases fast when n increases.

2.2 LWC data hiding scheme [11]

For the EMD scheme, the embedding capacity decreases fast when n increases. It maintains slighty more than 1 bpp when $n = 2$ for [12]. In order to improve the embedding capacity from 1.16 to 1.5 bpp, Lee et al. proposed the improved LWC scheme [11] in 2007.

In the LWC scheme, they fixed two pixels for each pixel group and gave the the modified extraction function as (2).

$$f_{LWC}(g_1, g_2) = (g_1 \times 1 + g_2 \times 3) \mod 8, \tag{2}$$

where g_1 and g_2 are the two pixel values for adjusting.

Algorithm 2 The LWC embedding algorithm

```
Input: cover image $I_c$ and secret data $s$
Output: stego-image $I_s$
 LWC-1 Divide $I_c$ into non-overlapping 2 pixel groups.
 LWC-2 Get the cover pixel group and compute $f_{LWC}$ by (2).
 LWC-3 Obtain 3 bits secret data $s_i$ from $s$ and transform it to decimal.
 LWC-4 If $s_i = f_{LWC}(g_1, g_2)$, then $(g_1', g_2') = (g_1, g_2)$.
   If $s_i = f_{LWC}(g_1 + 1, g_2)$, then $(g_1', g_2') = (g_1 + 1, g_2)$.
   If $s_i = f_{LWC}(g_1 - 1, g_2)$, then $(g_1', g_2') = (g_1 - 1, g_2)$.
   If $s_i = f_{LWC}(g_1, g_2 + 1)$, then $(g_1', g_2') = (g_1, g_2 + 1)$.
   If $s_i = f_{LWC}(g_1, g_2 - 1)$, then $(g_1', g_2') = (g_1, g_2 - 1)$.
   If $s_i = f_{LWC}(g_1 + 1, g_2 + 1)$, then $(g_1', g_2') = (g_1 + 1, g_2 + 1)$.
   If $s_i = f_{LWC}(g_1 + 1, g_2 - 1)$, then $(g_1', g_2') = (g_1 + 1, g_2 - 1)$.
   If $s_i = f_{LWC}(g_1 - 1, g_2 + 1)$, then $(g_1', g_2') = (g_1 - 1, g_2 + 1)$.
 LWC-5 Repeat from step LWC-2 until all secret data is embedded.
```

Example 2 Given two pixels $(g_1, g_2) = (62, 63)$ and secret data $s = (110)_2$. We obtain the stego-image pixels $(g_1', g_2') = (62, 64)$ using the LWC scheme as the following:

Step 1. Compute $f_{LWC}(62, 63) = (62 \times 1 + 63 \times 3) \mod 8 = 3$
Step 2. Using $s = (110)_2$, find $s_i = f_{LWC}(g_1, g_2 + 1) = (62 \times 1 + 64 \times 3) \mod 8 = 6$

When the receiver gets the two stego pixels, the secret data $(110)_2$ is recovered by using (2) ($s = f_{LWC}(62, 64) = (62 \times 1 + 64 \times 3) \mod 8 = 6$).

2.3 GEMD data hiding scheme [3]

Although the embedding capacity of the LWC scheme can achieved 1.5 bpp, the pixel group size is always fixed. In other words, there are only two pixels in a group and it cannot be extended or changed. That is to say, the LWC scheme is inflexible. In 2013, Kuo et al. proposed a new data hiding scheme based on general EMD. The major property of the GEMD scheme is having n pixels for each pixel group and maintaining embedding capacity of more than 1 bpp. Moreover, the LWC scheme is a special case of the GEMD scheme when $n = 2$. In the GEMD scheme, the new extraction function is shown as (3).

$$f_{GEMD}(g_1, g_2, \ldots, g_n) = \left[\sum_{i=1}^{n}(g_i \times (2^i - 1))\right] \mod 2^{n+1}, \tag{3}$$

where g_i is the i-th pixel value for adjusting, and n is the number of values required for implementing the selected pixels.

Algorithm 3 The GEMD embedding algorithm

```
Input: cover image $I_C$ and secret data $s$
Output: stego-image $I_S$
 GEMD-1 Divide $I_C$ into non-overlapping $n$ pixel groups.
 GEMD-2 Using the cover pixel group, compute $f_{GEMD}$ by (3).
 GEMD-3 Obtain $(n+1)$ bits secret data $s_i$ from $s$ and then transform it to decimal.
 GEMD-4 Compute $d = (s_i - f_{GEMD}) \mod 2^{n+1}$.
 GEMD-5 If $d = 0$, then $k = 1$; else if $d = 2^n$, $k = 2$; else if $0 < d < 2^n$, $k = 3$;
   else $k = 4$.
 GEMD-6 switch($k$)
   Case 1. $g'_i = g_i \forall i \in \{1, 2, \cdots, n\}$.
   Case 2. $g'_1 = g_1 + 1, g'_n = g_n + 1, g'_i = g_i \forall i \in \{2, 3, \cdots, n-1\}$.
   Case 3. Transform $d$ to $(b_n b_{n-1} \ldots b_0)_2$,
     for $i = n$ to 1 do
         if $b_i = 0\&b_{i-1} = 1, g'_i = g_i + 1$;
           else if $b_i = 1 \& b_{i-1} = 0, g'_i = g_i - 1$;
             else $g'_i = g_i$;
     end.
  Case 4. $d' = 2^{n+1} - d$, transform $d'$ to $(b_n b_{n-1} \cdots b_0)_2$,
     for $i = n$ to 1 do
         if $b_i = 0 \& b_{i-1} = 1, g'_i = g_i - 1$;
           else if $b_i = 1 \& b_{i-1} = 0, g'_i = g_i + 1$;
             else $g'_i = g_i$;
     end.
  GEMD-7 Repeat from step GEMD-2 until all secret data is embedded.
```

Example 3 Given three cover image pixels $(g_1, g_2, g_3) = (62, 63, 60)$ and secret data $s = (1100)_2$, we obtain output stego-image pixels $(g'_1, g'_2, g'_3) = (62, 62, 60)$ using the GEMD embedding procedure.

Step 1 Compute $f_{GEMD} = (62 \times 1 + 63 \times 3 + 60 \times 7) \mod 16 = 15$.
Step 2 Using 4 bits secret data $(1100)_2$, transform it to decimal $(12)_{10}$.
Step 3 Compute $d = (12 - 15) \mod 16 = 13$.
Step 4 Obtain $k = 4$ since $d = 13 > 2^3$.
Step 5 Execute case 4, compute $d' = 2^4 - 13 = 3 = (0011)_2 = (b_3 b_2 b_1 b_0)_2$ to get $\left(g'_1, g'_2, g'_3\right) = (62, 62, 60)$.

Therefore, the receiver can recover the secret data $s = f_{GEMD} = (62 \times 1 + 62 \times 3 + 60 \times 7) \mod 16 = 12 = (1100)_2$ when receiving the stego-pixel values (62, 62, 60).

3 The proposed scheme

Kuo et al. proposed the GEMD scheme which has benefits of both EMD and LWC schemes. GEMD can maintain more than 1 bpp capacity and good image quality. However, we still think the capacity is not enough. Therefore, we will re-adjust stego-pixel value of GEMD to embed extra secret data and keeps the extraction function value changeless. Our embedding structure is shown as Fig. 1 and the detail algorithm is described in Algorithm 4.

Algorithm 4 The RGEMD embedding algorithm

```
Input: cover image $I_C$ and secret data $s$
Output: stego-image $I_S$
 RGEMD-1 Divide $I_C$ into non-overlapping $n$ pixel groups.
 RGEMD-2 Using the cover pixel group, compute $f_{GEMD}$ by (3).
 RGEMD-3 Use $(n + 1)$ bits secret data $s_i$ from $s$ and compute $d = (s_i - f_{GEMD}) \mod 2^{n+1}$.
 RGEMD-4 If $d = 0$, then $k = 1$; else if $d = 2^n$,
   $k = 2$; else if $0 < d < 2^n$, $k = 3$; else $k = 4$.
 RGEMD-5 Switch($k$)
   Case 1. $g'_i = g_i \forall i \in \{1, 2, \cdots, n\}$.
   Case 2. $g'_1 = g_1 + 1$, $g'_n = g_n + 1$, $g'_i = g_i \forall i \in \{2, 3, \cdots, n - 1\}$.
   Case 3. Transform $d$ to $(b_n b_{n-1} \cdots b_0)_2$,
     for $i = n$ to 1 do
       if $b_i = 0 \& b_{i-1} = 1$, $g'_i = g_i + 1$;
         else if $b_i = 1$ & $b_{i-1} = 0$, $g'_i = g_i - 1$;
           else $g'_i = g_i$;
     end.
   Case 4. $d' = 2^{n+1} - d$, transform $d'$ to $(b_n b_{n-1} \cdots b_0)_2$,
     for $i = n$ to 1 do
       if $b_i = 0$ & $b_{i-1} = 1$, $g'_i = g_i - 1$;
         else if $b_i = 1$ & $b_{i-1} = 0$, $g'_i = g_i + 1$;
           else $g'_i = g_i$;
     end.
 RGEMD-6 Obtain next $(n - 1)$ bits secret $s_{i+1} = (b'_{n-2} b'_{n-3} \cdots b'_0)_2$ from $s$.
     for $i = n - 2$ to 0 do
       if $b'_i \neq LSB(g'_{i+2})$ do
         if $g'_{i+2} \geq g_{i+2}$ & $g'_{i+1} \leq g_{i+1}$
           $g'_{i+2} = g'_{i+2} - 1$;
           $g'_{i+1} = g'_{i+1} + 2$;
           $g'_1 = g'_1 + 1$;
         else
           $g'_{i+2} = g'_{i+2} + 1$;
           $g'_{i+1} = g'_{i+1} - 2$;
           $g'_1 = g_1 - 1$;
         end.
       end.
     end.
 RGEMD-7 Repeat from step RGEMD-2 until all secret data is embedded.
```

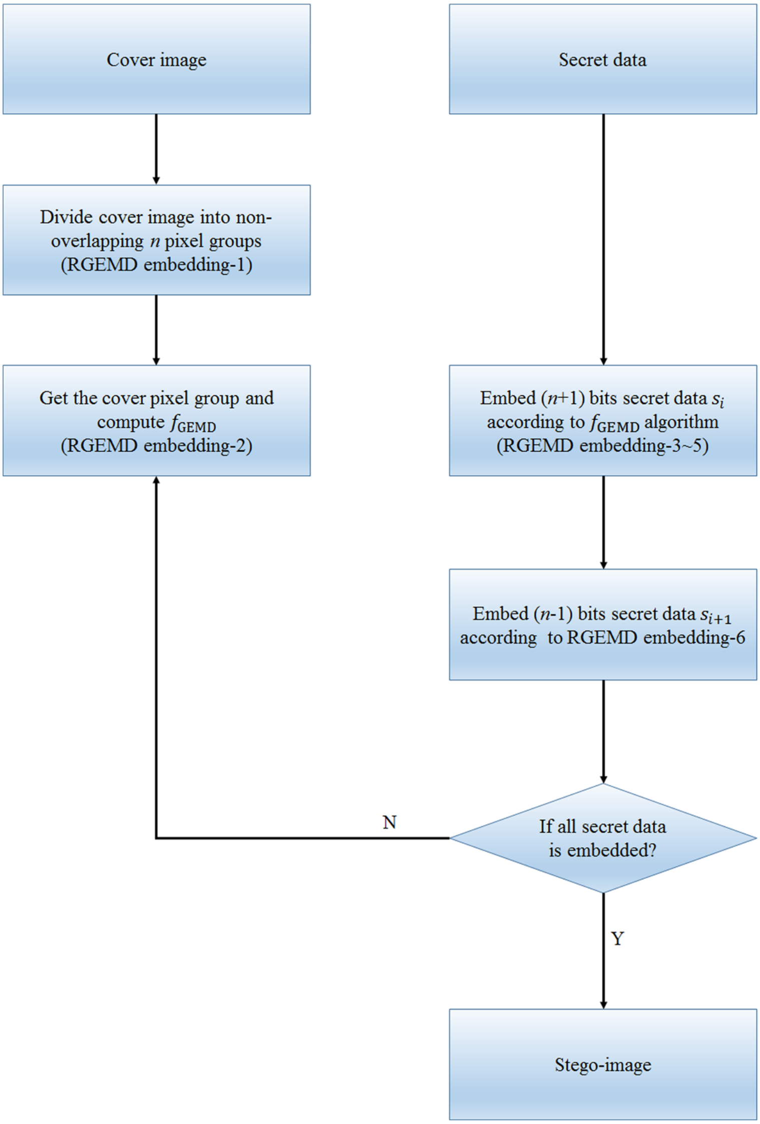

Cover image
Secret data
Divide cover image into non-overlapping n pixel groups (RGEMD embedding-1)
Get the cover pixel group and compute f_{GEMD} (RGEMD embedding-2)
Embed (n+1) bits secret data s_i according to f_{GEMD} algorithm (RGEMD embedding-3~5)
Embed (n-1) bits secret data s_{i+1} according to RGEMD embedding-6
If all secret data is embedded?
N
Y
Stego-image

Fig. 1 The structure of embedding phase

When the receiver gets the stego-image, he can extract $(n + 1)$ secret data bits by using GEMD extraction function. Then the receiver extracts $(n - 1)$ secret data bits for the LSB of n to 2 pixels in group. The extracting structure is shown as Fig. 2 and the detail algorithm is described in Algorithm 5.

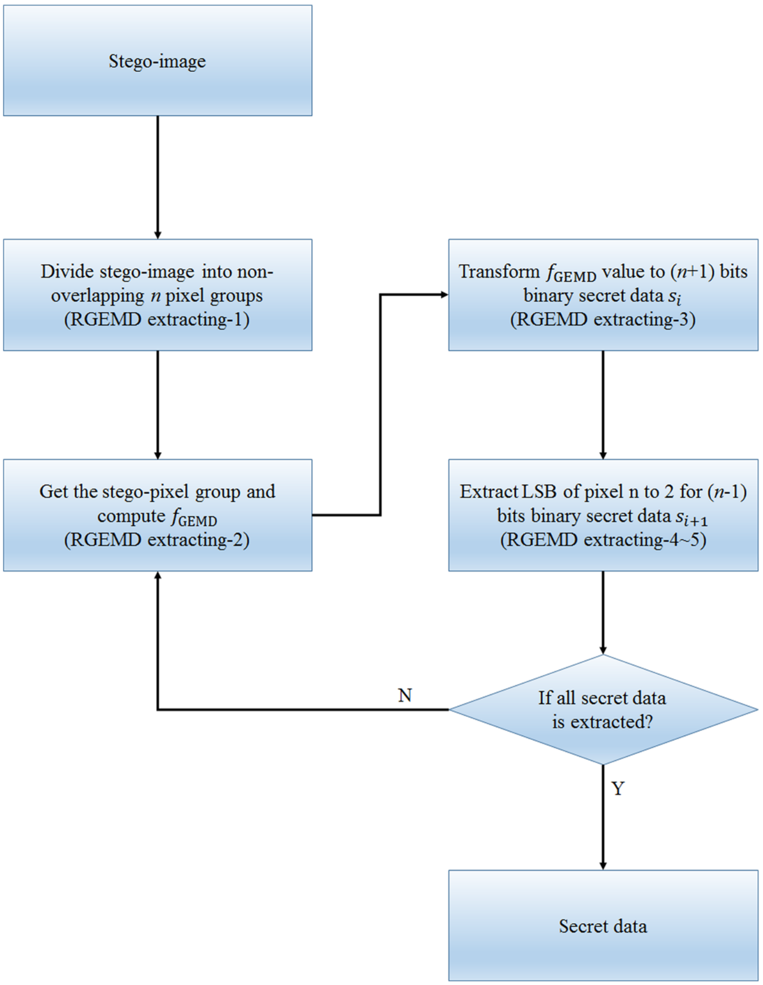

Stego-image
Divide stego-image into non-overlapping n pixel groups (RGEMD extracting-1)
Get the stego-pixel group and compute f_{GEMD} (RGEMD extracting-2)
Transform f_{GEMD} value to (n+1) bits binary secret data s_i (RGEMD extracting-3)
Extract LSB of pixel n to 2 for (n-1) bits binary secret data s_{i+1} (RGEMD extracting-4~5)
If all secret data is extracted?
N
Y
Secret data

Fig. 2 The structure of extracting phase

Algorithm 5 The RGEMD extraction algorithm

```
Input: stego-image $I_S$
Output: secret data $s$
  ERGEMD-1 Divide $I_S$ into non-overlapping $n$ pixel groups.
  ERGEMD-2 Using the stego-pixel group, compute $f_{GEMD}$ by (3).
  ERGEMD-3 Transform the $f_{GEMD}$ value to $(n+1)$ bits binary secret data $s_i$.
  ERGEMD-4 For $i = n$ to 2 do
               Get the secret bit $b'_{i-2} = LSB(g'_i)$;
           end.
  ERGEMD-5 Concatenate secret bits $(b'_{n-2}b'_{n-3}\cdots b'_0)_2 = s_{i+1}$.
  ERGEMD-6 Repeat from step ERGEMD-2 until all secret data is extracted
    and concatenate all $s_i$ and $s_{i+1}$ to get $s$.
```

The following two examples show use of the embedding and extracting procedure.

Example 4 Given three cover image pixels $(g_1, g_2, g_3) = (62, 63, 60)$ and secret data $s = (110011)_2$, we obtain output stego-image pixels $(g'_1, g'_2, g'_3) = (60, 65, 59)$ using the RGEMD embedding procedure as following:

Step 1. Compute $f_{GEMD} = (62 \times 1 + 63 \times 3 + 60 \times 7) \mod 16 = 15$.
Step 2. Access 4 bits secret data $(1100)_2$ and then transform it to decimal $(12)_{10}$.
Step 3. Compute $d = (12 - 15) \mod 16 = 13$.
Step 4. Get $k = 4$ because $d = 13 > 2^3$.
Step 5. Execute case 4, compute $d' = 2^4 - 13 = 3 = (0011)_2 = (b_3b_2b_1b_0)_2$ and get $\left(g'_1, g'_2, g'_3\right) = (62, 62, 60)$.
Step 6. Using the next 2 bits $(b'_1b'_0)_2 = (11)_2$,

$$\begin{aligned}
&b'_1 = 1 \neq LSB(g'_3) = LSB(60)\\
&\quad g'_3 = 60 \geq g_3 = 60 \& g'_2 = 62 \leq g_2 = 63,\\
&\quad g'_3 = 60 - 1 = 59;\\
&\quad g'_2 = 62 + 2 = 64;\\
&\quad g'_1 = 62 + 1 = 63;\\
&b'_0 = 1 \neq LSB(g'_2) = LSB(64)\\
&\quad g'_2 = 64 \geq g_2 = 63 \& g'_1 = 63 > g_1 = 62,\\
&\quad g'_2 = 64 + 1 = 65;\\
&\quad g'_1 = 63 - 2 = 61;\\
&\quad g'_1 = 61 - 1 = 60.
\end{aligned}$$

Finally the stego-image pixels are $(g'_1, g'_2, g'_3) = (60, 65, 59)$.

Example 5 Given three stego-image pixels $(60, 65, 59)$. We obtain the secret data $s = (110011)_2$ using the RGEMD extraction procedure as following:

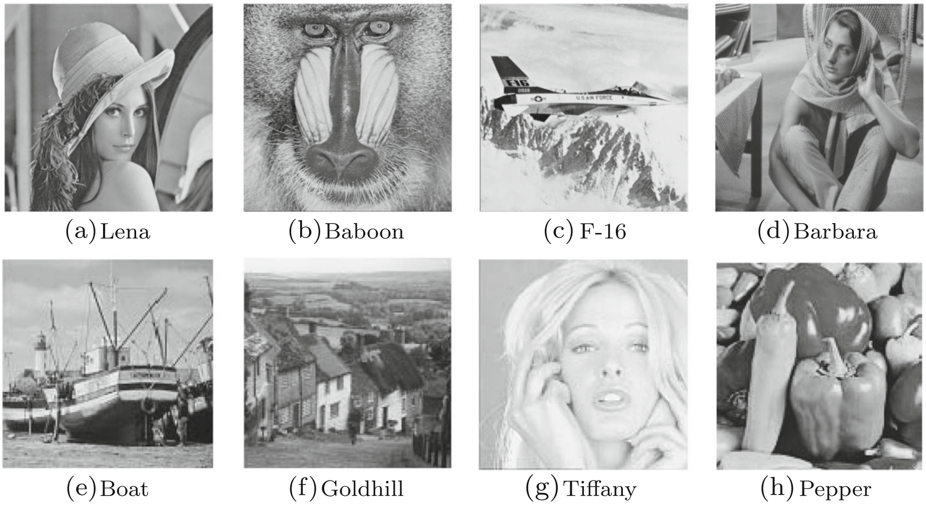
Step 1. Compute $f_{GEMD} = (60 \times 1 + 65 \times 3 + 59 \times 7) \mod 16 = 12 = (1100)_2$.
Step 2. $LSB(g'_3) = 1$ and $LSB(g'_2) = 1$, concatenate so $s_2 = (11)_2$.
Step 3. Concatenate s_1 and s_2 to get $s = (110011)_2$.

4 Experimental results

In this section, simulations and results of our proposed scheme are shown. For our experiment, the hardware environment is a personal computer with an Intel Core Duo 2 E4600 2.4 (GHz) CPU with 2G RAM. The operating system is Windows 7 running MATLAB. We use eight 512 × 512 grayscale images (Lena, Baboon, F16, Barbara, Boat, Goldhill, Tiffany and Pepper) and four 512512 color images (Lena, Baboon, Tiffany, Pepper) as shown in Figs. 3 and 4

4.1 Performance analysis

The major concerns for data hiding scheme analysis are capacity and image quality. Peak signal to noise ratio (PSNR) measures stego image quality. The higher the PSNR, the more similar the stego image is to the cover image. In general, if PSNR is lower than 30 dB, the


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

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

Fig. 3 Eight grayscale test images

stego image can be visually distinguished from the cover image as different. The PSNR and the mean square error (MSE) is calculated as follows:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}, \tag{4}$$

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} (I(x, y) - I'(x, y))^2, \tag{5}$$

where M and N represent the length and width of the image, respectively. The stego images were produced in raster-scan order.

The comparison between EMD, LWC, GEMD and our scheme are shown as Table 1. From this table, the image quality of all schemes are more than 44 dB, so the stego-image quality is good enough to avoid human eye detection. The embedding capacity of our proposed scheme maintains 2 bpp which is independent of n. However, other schemes suffer as n increases.

In Table 2, we show the color images capacity and PSNR comparison table for EMD, LWC, GEMD and our scheme. We can find that the capacity becomes triple because there

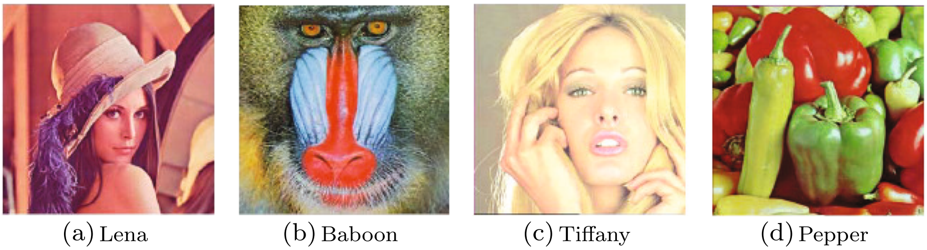

(a) Lena (b) Baboon (c) Tiffany (d) Pepper

Fig. 4 Four color test images

Table 1 Embedding capacity and PSNR comparison table for the gray stego image

Scheme	EMD [12]		LWC [11]		GEMD [3]		Proposed scheme	
	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR
$n = 2$	1.16	52.11	1.50	50.72	1.50	50.72	2.00	45.12
$n = 3$	0.93	53.57			1.33	50.79	2.00	44.62
$n = 4$	0.79	54.66			1.25	51.00	2.00	44.65
$n = 5$	0.69	55.53			1.20	51.09	2.00	44.72
$n = 6$	0.61	56.27			1.16	51.13	2.00	44.74
$n = 7$	0.55	56.87			1.14	51.13	2.00	44.74
$n = 8$	0.51	57.42			1.12	51.13	2.00	44.74
$n = 9$	0.47	57.90			1.11	51.13	2.00	44.74
$n = 10$	0.43	58.35			1.10	51.13	2.00	44.74

are three channels (RGB) in color images to embed secret bits. According to Table 2, the color stego image's quality(PSNR) is similar to the gray stego image's quality.

The performance comparison for gray images and color images are shown in Figs. 5 and 6, respectively. Since it is used the fixed points (i.e. $n = 2$) in the LWC scheme, there is only one point in the graph. According to Figs. 5 and 6, all points of proposed scheme are similar in our proposed scheme. In other words, the performance of our scheme is not concerned with the size of pixel group.

4.2 Steganalysis

Most EMD type data hiding scheme avoid RS detection. We confirm our scheme thwarts RS detection. In RS steganalysis, n adjacent pixels $(g_1, g_2, \cdots, g_n)$ are selected as a pixel group. Then the discrimination function $DF(g_1, g_2, \cdots, g_n) = \sum_{i=1}^{n} |g_{i+1} - g_i|$ is used to quantify the smoothness or regularity of each pixel group.

Table 2 Embedding capacity and PSNR comparison table for the color stego image

Scheme	EMD [12]		LWC [11]		GEMD [3]		Proposed scheme	
	bpp	PSNR	bpp	PSNR	bpp	PSNR	bpp	PSNR
$n = 2$	3.48	52.13	4.50	50.72	4.50	50.74	6.00	45.13
$n = 3$	2.79	53.58			4.00	50.78	6.00	44.62
$n = 4$	2.37	54.66			3.75	51.00	6.00	44.65
$n = 5$	2.07	55.55			3.60	51.10	6.00	44.71
$n = 6$	1.83	56.28			3.50	51.13	6.00	44.74
$n = 7$	1.65	56.89			3.43	51.13	6.00	44.74
$n = 8$	1.53	57.43			3.38	51.13	6.00	44.74
$n = 9$	1.41	57.90			3.33	51.13	6.00	44.74
$n = 10$	1.29	58.36			3.30	51.13	6.00	44.74

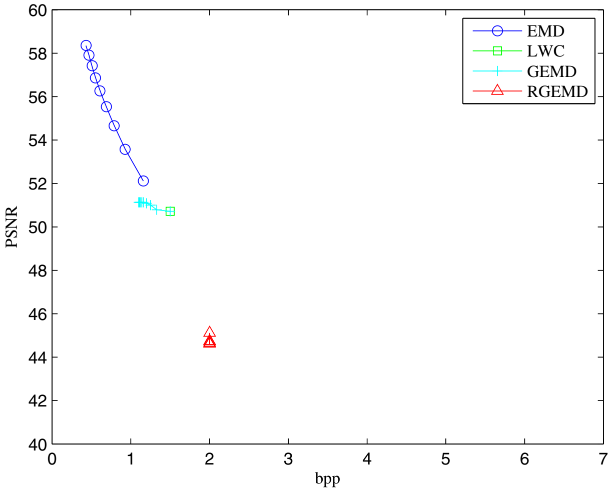


Fig. 5 The performance comparison for gray images

The discrimination function is used to define three types of pixel groups: Regular (R), Singular (S), and Unusable (U). The R means $DF\left(g_1', g_2, g_3, g_4'\right) > DF(g_1, g_2, g_3, g_4)$ and S means $DF\left(g_1', g_2, g_3, g_4'\right) < DF(g_1, g_2, g_3, g_4)$. We use masks $M = [1001]$ and $-M = [-100-1]$ to flip pixels (g_1, g_2, g_3, g_4) to $\left(g_1', g_2, g_3, g_4'\right)$. It measures that R_M, R_{-M}, S_M, and S_{-M} and then transform to percentages. The more detail RS detection method is described in [1]. The simulation results for 2-LSB and our proposed scheme are shown in Fig. 7. The statistical hypotheses of the RS-diagram are $R_M \approx R_{-M}$ and

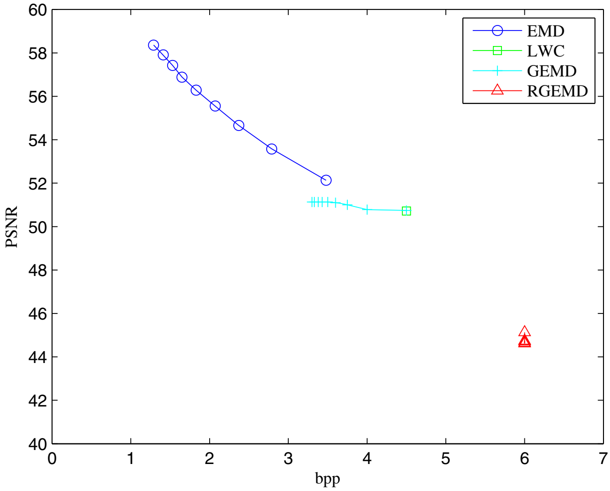
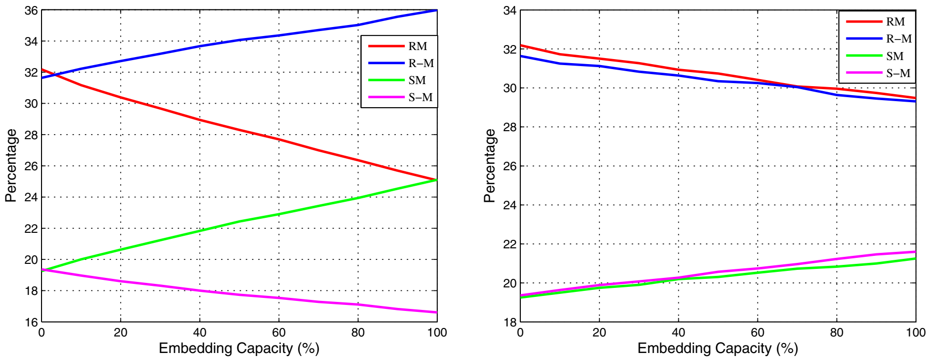


Fig. 6 The performance comparison for color images



(a)2-LSB scheme (b)Our proposed scheme

Fig. 7 RS detection

$S_M \approx S_{-M}$. The 2-LSB scheme is detected by RS steganalysis while our scheme avoids detection.

5 Conclusion

In this paper, we improve the GEMD data hiding scheme. After using GEMD to embed $(n+1)$ bits in each group, we re-adjust the stego-pixel values to embed $(n-1)$ bits and keep the extraction function the same. The most significant contribution of our approach is that the capacity maintains 2 bpp when n increases. Addition contributions in this paper include: the proposed scheme is more flexible, the stego-image quality is over 44 dB, and it is not detected by RS detection.

References

1. Fridrich J, Golijan M, Du R (2001) Reliable detection of LSB steganography in grayscale and color images, *Proceedings of ACM Workshop on Multimedia and Security*, pp. 27–30
2. Kieu TD, Chang CC (2011) A steganographic scheme by fully exploiting modification directions. Expert Syst Appl 38(8):10648–10657
3. Kuo WC, Wang CC (2013) Data hiding based on generalized exploiting modification direction method. Imaging Sci J 61(6):484–490
4. Kuo WC, Chen YH, Chuang CT (2014) High-capacity steganographic method based on division arithmetic and generalized exploiting modification direction. J Inf Hiding Multimed Signal Process 5(2):263–272
5. Kuo WC, Kuo SH, Wang CC, Wuu LC (2016) High capacity data hiding scheme based on multi-bit encoding function. Optik - Int J Light Electron Opt 127(4):1762–1769
6. Kuo WC, Wang CC, Hou HC (2016) Signed digit data hiding scheme. Inf Process Lett 116(2):183–191
7. Kuo WC, Kuo SH, Wuu LC (2017) Multi-Bit Data hiding scheme for compressing secret messages. Appl Sci 5(4):1033–1049

8. Kuo WC, Kao MC, Chang CC (2017) A generalization of fully exploiting modification directions data hiding scheme. J Inf Hiding Multimed Signal Process 6(4):718–727
9. Kuo WC, Lai PY, Wang CC, Wuu LC (2017) A formula diamond encoding data hiding scheme. J Inf Hiding Multimed Signal Process 6(6):1167–1176
10. Kuo WC, Wang CC, Huang YC (2017) Binary power data hiding scheme. AEU-Int J Electron Commun 69(11):1574–1581
11. Lee CF, Wang YR, Chang CC (2007) A steganographic method with high embedding capacity by improving exploiting modification direction, *Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (IIHMSP07), pp.497–500
12. Zhang X, Wang S (2006) Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 10(11):1–3

Chun-Cheng Wang received his M.S. degree from Southern Taiwan University of Science and Technology, Republic of China, in 2010. He is currently a Ph.D. student in Graduate School of Engineering Science and Technology- Doctoral Program at National Yunlin University of Science & Technology, Republic of China. His research interests are cryptography, image processing and information hiding.

Wen-Chung Kuo received the B.S. degree in Electrical Engineering from National Cheng Kung University and M.S. degree in Electrical Engineering from National Sun Yat-Sen University in 1990 and 1992, respectively. Then, He received the Ph.D. degree from National Cheng Kung University in 1996. Now, he is an associate professor in the Department of Computer Science and Information Engineering at National Yunlin University of Science & Technology. His research interests include steganography, cryptography, network security and signal processing.

Yu-Chih Huang received her B.S. degree in the Department of Mechanical Engineering from National Cheng Kung University and M.S. degree in the Department of Mechanical Engineering from National Chiao Tung University (HsinChu, Taiwan) in 1990 and 1993, respectively. Then, she received the Ph.D. degree in the Department of Mechanical Engineering from National Cheng Kung University in 2000. She is currently an Associate Professor in the Department of Information Management, Tainan University of Technology. Her research interests include e-Business strategy, ISMS, information society and cybersecurity.

Lih-Chyau Wuu received her B.S. degree in the Department of Information Engineering from National Taiwan University (Taipei, Taiwan) in 1982, and her Ph.D. degree in the Department of Computer Science from National Tsing Hua University (HsinChu, Taiwan) in 1994. She is currently a Professor in the Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology (Touliu, Taiwan). Her research interests include IP Switches/Routing, multicast routing, network security and distributed self-stabilizing systems.