Multimed Tools Appl (2014) 70:1729–1747
DOI 10.1007/s11042-012-1190-1

Reversible secret-image sharing with high visual quality

Ching-Chiuan Lin · Lun Hao Liao · Kuo Feng Hwang · Shih-Chieh Chen

Published online: 12 August 2012

Abstract This paper proposes a reversible secret-image sharing scheme for sharing a secret image among $2n$ shadow images with high visual quality (i.e., they are visually indistinguishable from their original images, respectively). In the proposed scheme, not only can the secret image be completely revealed, but the original cover images can also be losslessly recovered. A difference value between neighboring pixels in a secret image is shared by $2n$ pixels in $2n$ shadow images, respectively, where $n \geq 1$. A pair of shadow images which are constructed from the same cover image are called brother stego-images. To decrease pixel values changed in shadow images, each pair of brother stego-images is assigned a weighted factor when calculating difference values to be shared. A pixel in a cover image is recovered by calculating the average of corresponding pixels in its brother stego-images. A single stego-image reveals nothing and a pair of pixels in brother stego-images reveals partial difference value between neighboring secret pixels. The more brother stego-images are collected, the more information in the secret image will be revealed. Finally, a secret image will be completely revealed if all of its brother stego-images are collected.

Keywords Secret sharing · Friendly secret sharing · Secret image sharing · Shadow images

C.-C. Lin (✉) · K. F. Hwang · S.-C. Chen
Department of Information Management, Overseas Chinese University,
Taichung 40721, Taiwan
e-mail: cclin@ocu.edu.tw

K. F. Hwang
e-mail: kfhwang@ocu.edu.tw

S.-C. Chen
e-mail: jackie@ocu.edu.tw

L. H. Liao
Deptpartment of Information Management, Chaoyang University of Technology,
Taichung 41349, Taiwan
e-mail: Liao.Howard@gmail.com

1 Introduction

Nowadays information security is an important issue in applications such as electronic commerce and systems for military purpose. Secret sharing is a technique which hides secrets in different participants such that one cannot decrypt the secrets alone. In military applications, for example, if a figure of airplane designed by a group of people can be uncovered by a person alone, the secret information in it may be revealed by the person for some private purposes and unexpected risks may happen. In such a case, if the secret figure can be partitioned and shared by a group of people such that one cannot uncover it alone, the person can get only a piece of information about the secret and he/she cannot reveal the secret without getting the remaining shares. Therefore, sharing a secret image by a group of parties can effectively improve the security of the image.

Approaches to sharing a secret image may be classified into two categories: computational and non-computational. The former divides a secret image to be shared and reveals it by mathematical computation, whereas the latter hides a secret image in transparencies and reveals it by simply stacking them.

In 1979, Shamir [15] proposed a (k, n)-threshold sharing scheme based on polynomial interpolation. In his scheme, to share a secret value D among n participants, a prime number p and the equation $q(x) = D + a_1x + a_2x^2 + ... + a_{k-1}x^{k-1}$ are selected, where $a_1, a_2, ..., a_{k-1}$ are randomly selected integers and $0 \leq a_1, a_2, ..., a_{k-1} < p$. Then D is divided into n pieces–D_1, D_2, ...,D_n, and they are shared by n participants, respectively, where $D_1 = q(1) \bmod p, ..., D_i = q(i) \bmod p, ..., D_n = q(n) \bmod p$. To reveal $D = q(x) - a_1x - a_2x^2 - ... - a_{k-1}x^{k-1}$, at least k pieces must be gathered. Otherwise, D cannot be determined. Shamir's scheme is a typical approach to sharing a secret image by mathematical computation. Later, his scheme was extended by a number of secret sharing schemes [2, 3, 7, 11, 12, 16, 18, 19, 22] for sharing a secret image.

Thien and Lin [16] was inspired by Shamir's scheme and proposed a (k, n) secret image sharing method based on Lagrange's interpolation. In their method, a secret image is shared by n shadow images, which are noise-like, and at least k shadow images should be gathered to reconstruct the secret image. Briefly, the secret image is divided into blocks each of which contains k pixels, and the k pixel values in a block are taken as Lagrange's interpolation coefficients to calculate n pixel values for n shadow images, respectively. As a result, the number of pixels in a shadow image is $1/k$ of that in the secret image. Recently, Thien and Lin's method was extended by Wang and Shyu's image sharing scheme [19] in which a secret image is reconstructed in a scalable manner which is proportional to the number of shadow images gathered. The more the shadow images are gathered, the more information about the secret image will be revealed. When $k = n$, the secret image can be completely revealed.

Wang et al. [21] introduced an (n, n) secret sharing scheme based on Boolean operation. Let I be a secret image to be shared by n shadow images $I_1, I_2, ..., I_n$ and they are constructed by $I_1 = B_1$, $I_2 = B_1 \oplus B_2, ..., I_{n-1} = B_{n-2} \oplus B_{n-1}$, and $I_n = B_{n-1} \oplus I$, where $B_1, B_2, ..., B_{n-1}$ are randomly generated images with the same size as I and $\oplus$ is a bitwise XOR operator. Then I can be revealed by $I = I_1 \oplus I_2 \oplus$

$\ldots \oplus I_n$. Secret sharing schemes using noise-like shadow images may encounter a problem of identifying shadows, since their shadows look noisy. To overcome the problem, schemes [5, 17] using friendly shadow images have been developed, in which a shadow image is a meaningful image. A meaningful shadow image may not attract hacker's notice, and undesired attacks may also be avoided.

Based on stacking transparencies without performing mathematical computations, a new visual secret sharing scheme was proposed by Naor and Shamir [14] in 1995. In their scheme, a secret image can be revealed by simply stacking transparencies together. Given a pixel on a transparency is either black or white, the stacking rule is that any pixel stacking a black pixel together gives a black pixel, and stacking white pixels together gives a white pixel. In Naor and Shamir's approach, a secret pixel is expanded to a block consisting of m black-and-white sub-pixels. To distinguish a black pixel from a white one, blocks of sub-pixels are divided into groups A and B such that any k blocks in group A stacked together can give a darker block compared to stacking any k blocks in group B together. When constructing a share, a black or white secret pixel corresponding to that in the share is replaced by a block of sub-pixels in group A or B, respectively.

Approaches based on stacking transparencies [1, 4–6, 8–10, 14, 20] are usually applied to applications of sharing a halftone or black-and-white image in which a pixel is either black or white. Consequently, a gray-level image would be converted into a halftone image before applying visual secret sharing (VSS) schemes. In other words, VSS schemes are not good candidates for sharing a secret image with high visual quality. In addition, a stego-image with high visual quality is also unexpected. Recently, Liu et al. [13] proposed an image sharing scheme based on combination theory, whose concept is analogous to stacking transformed transparencies.

In this paper, a reversible secret-image sharing scheme using stego-images with high visual quality is proposed. Not only can a secret image be completely revealed, but cover images can also be losslessly recovered. In addition, shadow images sharing the secret image can obtain a high-visual-quality result, i.e., they are visually indistinguishable from their original images, respectively. First, differences between neighboring pixels in the secret image are calculated and converted into a difference image. Since neighboring pixels are similar in pixel intensity, most pixels in the difference image will have smaller pixel values (i.e., difference values) compared to those in the secret image. Then a difference value is shared by $2n$ shadow pixels, where $n \geq 1$. A pair of shadow images which are constructed from the same cover image are called *brother stego-images*. Each pair of pixels in brother stego-images share a weighted partial difference (WPD) value such that the difference value can be minimized, which implies a cover image can be less modified. Therefore, a shadow image with high visual quality can be expected. Reversibility of a pixel value in a cover image is obtained by calculating the average of a pair of corresponding pixels in its brother stego-images. A pixel value in the secret image can be revealed by adding the products of each WPD value for the pixel value and its weight.

The rest of this paper is organized as follows. Section 2 introduces the proposed scheme including an example illustrating the sharing and revealing processes. Section 3 shows the simulation results and gives a comparison with existing studies. Finally, conclusions are given.

2 Proposed scheme

The proposed scheme includes a sharing process, which shares a secret image among $2n$ stego-images, and a revealing process, which reveals the secret image and recovers a stego-image to its original cover image. Symbols in the processes are defined as follows:

$A_{i,k}$ or $A_{i,w}$	the total difference to be shared by S_1 to S_k or S_1 to S_w, respectively
$a_{i,k}$ or $a_{i,w}$	a WPD value of pixel i in cover image S_k or S_w, respectively
D	the remaining WPD value to be shared
d_i	the difference value between y_{i-1} and y_i
h, j, or m	an index of pixel in a cover image or stego-image
I	the secret image to be shared
i	an index of pixel in secret image I
k or w	an index for identifying a cover image
N	the number of pixels in secret image I
n	the number of cover images
$num(S_k)$	the number of pixels in S_k
R_k or R_w	the sum of weighted factors of the first k or w cover images S_1, ..., S_k or S_1, ..., S_w, respectively
r_k or r_w	a weighted factor for cover image S_k or S_w, respectively
S'_k and S''_k	brother stego-images of S_k
S_k or S_w	a cover image
$sign(d_i)$	a function returns -1 if $d_i < 0$, otherwise returns 1
$x_{j,k}$	the pixel value of pixel j in S_k
$x'_{j,k}$ and $x''_{j,k}$	brother stego-pixel values of pixel j in S'_k and S''_k, respectively
$\dot{x}_{j,k}$ and $\ddot{x}_{j,k}$	temporary brother stego-pixel values of pixel j in S'_k and S''_k, respectively
y_i	the pixel value of pixel i in secret image I

Figure 1 shows an overview of the proposed scheme. First, the sharing process converts security image I into a difference image and then dispatches it to $2n$ stego-images S'_1, S''_1, ..., S'_k, S''_k, ..., S'_n, S''_n where $1 \leq k \leq n$, S'_k and S''_k are a pair of brother stego-images constructed from cover image S_k. They can reveal partial shared difference values. Finally, if all stego-images are collected, the revealing process can completely reveal security image I.

2.1 Sharing process

The following process is applied to share a secret image among shadow images in which each pixel value is between 0 and 255.

Input: A secret image I to be shared and n cover images.
Output: $2n$ stego-images by which the secret image I is shared.

1. Scan the secret image I to be shared in a zigzag order. Let y_0 be the middle value of allowed pixel value. Calculate $d_i = y_{i-1} - y_i$, where $1 \leq i \leq N$. For a 256-level grayscale image, $0 \leq y_i \leq 255$ is satisfied and $y_0 = 128$ is selected. Therefore, an N-pixel image contains N differences in which the first difference is $y_0 - y_1$.

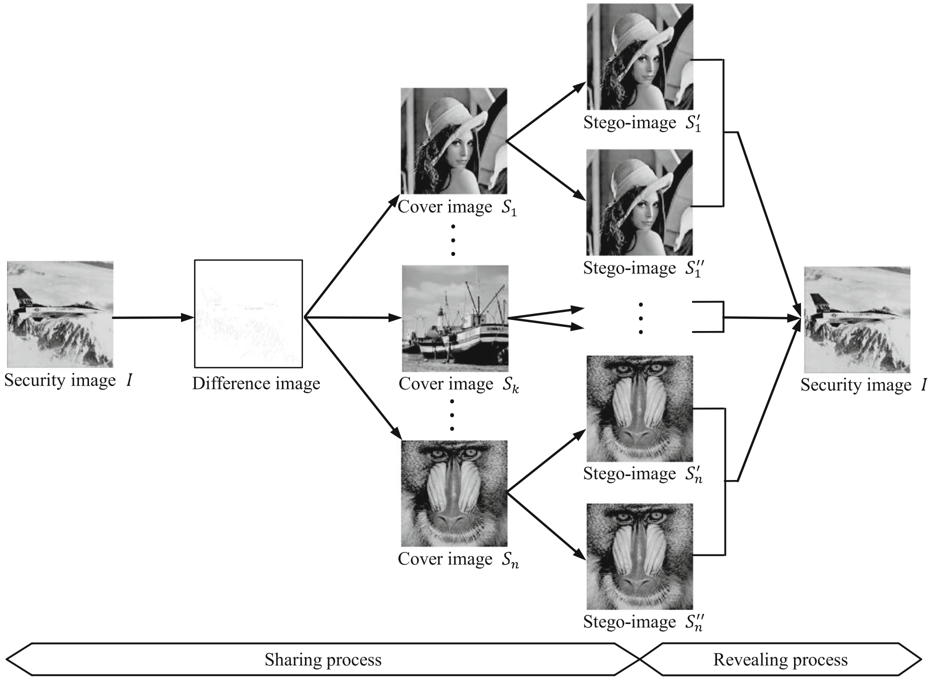


Fig. 1 An overview of the proposed scheme

2. Let $2n$ be the number of shadows which will share the secret image I. Select n cover images each of which is denoted by S_k, where $1 \leq k \leq n$.
3. For each pixel i in secret image I, calculate

$$A_{i,k} = \begin{cases} |d_i| & \text{if } k = n, \\ |d_i| - \sum_{w=k+1}^{n}(a_{i,w} \times r_w) & \text{otherwise,} \end{cases} \tag{1}$$

and

$$a_{i,w} = \begin{cases} 0 & \text{if } w > n \text{ or } A_{i,w} < r_w, \\ \lceil A_{i,w}/R_w \rceil & \text{otherwise,} \end{cases} \tag{2}$$

where $r_w = 2^{w-1}$ and $R_w = \sum_{k=1}^{w} r_k$. Detailed iterative calculation of $A_{i,w}$ (i.e. $A_{i,k}$) and $a_{i,w}$ is demonstrated after the sharing process.
4. For each cover image S_k, do steps 5–8.
5. Set $i = j = 1$ and $D = a_{i,k}$, where i and j are the indexes of pixels in I and S_k, respectively.
6. Compute $\dot{x}_{j,k} = x_{j,k} + \lfloor D/2 \rfloor$ and $\ddot{x}_{j,k} = \dot{x}_{j,k} - D$.
7. Calculate

$$(D, x'_{j,k}, x''_{j,k}) = \begin{cases} (a_{i,k}, x_{j,k}, x_{j,k}) & \text{if } x_{j,k} \in \{0, 255\}, \\ (2 \times |\ddot{x}_{j,k}|, \dot{x}_{j,k} + \ddot{x}_{j,k}, 0) & \text{if } \ddot{x}_{j,k} \leq 0, \\ (2 \times (\dot{x}_{j,k} - 255), 255, \dot{x}_{j,k} + \ddot{x}_{j,k} - 255) & \text{if } \dot{x}_{j,k} \geq 255, \\ (a_{i+1,k}, \dot{x}_{j,k}, \ddot{x}_{j,k}) & \text{if } 0 < \dot{x}_{j,k}, \ddot{x}_{j,k} < 255. \end{cases} \tag{3}$$

If $d_j < 0$, replace the values of $x'_{j,k}$ and $x''_{j,k}$ with each other such that $x'_{j,k} < x''_{j,k}$. The design concepts of calculating $(D, x'_{j,k}, x''_{j,k})$ in this step are explained after the sharing process.

8. Set $j = j + 1$. If $j > num(S_k)$ and $i < N$, which means all cover pixels in S_k are exhausted but WPD values are not completely embedded, then S_k cannot be a cover image for sharing the secret image and a larger one should be selected. If $0 < \dot{x}_{j,k}, \ddot{x}_{j,k} < 255$, set $i = i + 1$. If $j \le num(S_k)$ and $i \le N$, go to step 6.
9. Obtain $2n$ shadow images by which the secret image is shared.

As shown in step 3, R_w is related to $r_1, r_2, ..., r_w$ and $A_{i,k}$ is related to $a_{i,k+1}, a_{i,k+2}, ..., a_{i,n}$. To make them clearer, we use $R_w = \sum_{k=1}^{w} r_k$ and $A_{i,k} = |d_i| - \sum_{w=k+1}^{n}(a_{i,w} \times r_w)$ instead of $R_w = \sum_{w=1}^{w} r_w$ and $A_{i,k} = |d_i| - \sum_{k=k+1}^{n}(a_{i,k} \times r_k)$, respectively. Similarly, we have $R_k = \sum_{w=1}^{k} r_w$ and $A_{i,w} = |d_i| - \sum_{k=w+1}^{n}(a_{i,k} \times r_k)$. In the step, d_i is divided into n smaller integers (i.e., WPD values) and $d_i = \sum_{k=1}^{n} r_k \times a_{i,k} \times sign(d_i)$.

The calculation of $a_{i,w}$ and $A_{i,w}$ is demonstrated as follows. First, according to (1), $A_{i,n} = |d_i|$ is given. Then, either $a_{i,n} = 0$ or $a_{i,n} = \lceil A_{i,n}/R_n \rceil = \lceil |d_i|/R_n \rceil$ can be derived from (2). After calculating $a_{i,n}$, we have $A_{i,n-1} = |d_i| - \sum_{w=n}^{n}(a_{i,w} \times r_w) = |d_i| - a_{i,n} \times r_n$ from (1). Again, we can obtain $a_{i,n-1}$ from (2) after $A_{i,n-1}$ is calculated. The calculation of $a_{i,w}$ and $A_{i,w}$ continues until $a_{i,1}$ is obtained. For example, if $n = 4$, we can compute

$$\begin{aligned}
&A_{i,4} = |d_i|,\\
&a_{i,4} = \begin{cases} 0 & \text{if } A_{i,4} < r_4, \\ \lceil A_{i,4}/R_4 \rceil & \text{otherwise,} \end{cases}\\
&A_{i,3} = |d_i| - a_{i,4} \times r_4 = A_{i,4} - a_{i,4} \times r_4,\\
&a_{i,3} = \begin{cases} 0 & \text{if } A_{i,3} < r_3, \\ \lceil A_{i,3}/R_3 \rceil & \text{otherwise,} \end{cases}\\
&A_{i,2} = |d_i| - (a_{i,4} \times r_4 + a_{i,3} \times r_3) = A_{i,3} - a_{i,3} \times r_3,\\
&a_{i,2} = \begin{cases} 0 & \text{if } A_{i,2} < r_2, \\ \lceil A_{i,2}/R_2 \rceil & \text{otherwise,} \end{cases}\\
&A_{i,1} = |d_i| - (a_{i,4} \times r_4 + a_{i,3} \times r_3 + a_{i,2} \times r_2) = A_{i,2} - a_{i,2} \times r_2, \text{ and}\\
&a_{i,1} = \begin{cases} 0 & \text{if } A_{i,1} < r_1, \\ \lceil A_{i,1}/R_1 \rceil & \text{otherwise.} \end{cases}
\end{aligned}$$

Section 2.3 gives an example illustrating how to iteratively calculate $A_{i,w}$ and $a_{i,w}$.

Equation (3) is to adjust stego-pixels, such that their pixel values are between 0 and 255. The four conditions in the equation are explained as follows:

- First, if cover pixel $x_{j,k}$ is saturated (i.e., $x_{j,k} \in \{0, 255\}$), then the pixel cannot be used to share a WPD and both D and $x_{j,k}$ are kept unchanged. Therefore, we set $(D, x'_{j,k}, x''_{j,k}) = (a_{i,k}, x_{j,k}, x_{j,k})$.
- Next, if $\ddot{x}_{j,k} \le 0$, we set $x''_{j,k} = 0$ and add up $\ddot{x}_{j,k}$ and $\dot{x}_{j,k}$ to give $x'_{j,k}$. The remaining WPD value $2 \times |\ddot{x}_{j,k}|$ is saved by D which will be shared by the next stego-pixels $x'_{j+1,k}$ and $x''_{j+1,k}$. Therefore, we set $(D, x'_{j,k}, x''_{j,k}) = (2 \times |\ddot{x}_{j,k}|, \dot{x}_{j,k} + \ddot{x}_{j,k}, 0)$. Note that, in step 6, we calculate $\ddot{x}_{j,k} = \dot{x}_{j,k} - D$, so $\ddot{x}_{j,k} \le 255$.
- Then, if $\dot{x}_{j,k} \ge 255$, we set $x'_{j,k} = 255$ and the subtracted value $\dot{x}_{j,k} - 255$ is added to $\ddot{x}_{j,k}$ to give $x''_{j,k} = \ddot{x}_{j,k} + \dot{x}_{j,k} - 255$. Similar to the second condition, the remaining WPD value $2 \times (\dot{x}_{j,k} - 255)$ is saved by D. Since $\dot{x}_{j,k} = x_{j,k} + \lfloor D/2 \rfloor$ in step 6, the condition of $\dot{x}_{j,k} < 0$ may not be considered.

- Finally, if $0 < \dot{x}_{j,k}, \ddot{x}_{j,k} < 255$, the sharing process for $a_{i,k}$ is completed. Then the next WPD $a_{i+1,k}$ is saved by D for calculating next stego-pixels $x'_{j+1,k}$ and $x''_{j+1,k}$.

Since neighboring pixels in an image are similar, for most images, converting a secret image into a difference image may transform a larger pixel value into a smaller difference value. Sharing a smaller difference value by stego-images can reduce the adjustment of pixel values in the stego-images and obtain stego-images with high visual quality. To make pixels y_{i-1} and y_i to be geographically neighboring pixels, in step 1, the secret image I is scanned in a zigzag order, i.e., an odd line of pixels is scanned from left to right, whereas an even line of pixels is scanned from right to left. When scanning an image in a zigzag order, a pixel on the right side of an odd line of pixels and the one below the pixel are neighboring pixels. Similarly, a pixel on the left side of an even line of pixels and the one below the pixel are also neighboring pixels. If each line of pixels is scanned from left to right, a pixel on the right side of a line of pixels and the one on the left side below the line are not geographically neighboring pixels. Therefore, they are usually not similar. Figure 2 gives two examples illustrating the above image scanning orders: zigzag and raster, respectively, where y_i denotes a pixel value and i is the order of pixel visited. In Fig. 2a, for example, y_4 and y_5 are geographically neighboring pixels and they are usually similar. In addition, the difference between y_4 and y_5 is usually small. On the other hand, in Fig. 2b, y_4 and y_5 are not geographically neighboring pixels and, hence, they are usually not similar and their difference is usually not small. This is the reason why the secret image is scanned in a zigzag order.

The scanning order of cover images may not be the same as that of secret image I. However, in the revealing process in Section 2.2, the scanning order of stego-images must be the same as that of cover images. In this paper, for simplicity, all images are scanned in a zigzag order.

Note that two pairs of stego-images may be constructed from the same cover image. Although stego-images constructed from the same cover image are similar, brother stego-images must be those with brother stego-pixels constructed in step 7. For example, two pairs of brother stego-images (S'_1, S''_1) and (S'_2, S''_2) are stego-images constructed from cover image S and $S = S_1 = S_2$. Although the four stego-images are visually indistinguishable in the example, neither S'_1 and S'_2 , nor S''_1 and S''_2 are brother stego-images.

Since brother stego-images hide information about difference between secret pixels, they may roughly reveal a secret image. In step 3, the result of a weighted factor multiplied by the WPD value between a pair of brother stego-pixels shares a partial difference value between secret pixels. In general, brother stego-images

Fig. 2 Examples of scanning images: **a** zigzag scanning; **b** raster scanning

y_1	y_2	y_3	y_4
y_8	y_7	y_6	y_5
y_9	y_{10}	y_{11}	y_{12}
y_{16}	y_{15}	y_{14}	y_{13}

(a)

y_1	y_2	y_3	y_4
y_5	y_6	y_7	y_8
y_9	y_{10}	y_{11}	y_{12}
y_{13}	y_{14}	y_{15}	y_{16}

(b)

with a larger weighted factor can reveal more secret information than those with a smaller one.

Table 1 shows an example of 2, 4, 6, or 8 shadows sharing an absolute difference $|d_i|$ from 0 to 16. In the table, $|d_i| = \sum_{k=1}^{n}(2^{k-1} \times a_{i,k})$ is a difference value between pixels $i-1$ and i in the secret image to be shared, where 2^{k-1} is the weighted factor and $a_{i,k}$ is a WPD value for brother stego-images S'_k and S''_k . For example, a difference of 14 shared by two cover images (four shadows) is divided into two smaller values: 5 and 4 ($14 = 2^{2-1} \times 5 + 2^{1-1} \times 4$), instead of intuitively dividing it into 7 and 7 ($14 = 7 + 7$). As shown in the table, a significant contribution of the proposed scheme is that it introduces a weighted factor to divide a larger difference value into smaller WPD values such that a cover image can be less modified.

A difference value d_i is shared by $2n$ shadows and $d_i = \sum_{k=1}^{n} r_k \times a_{i,k} \times sign(d_i)$. If $a_{i,k}$ is too large to be completely shared by stego-pixels $x'_{j,k}$ and $x''_{j,k}$, the next cover pixel $x_{j+1,k}$ will be used to share the remaining value. Still, if $x'_{j+1,k}$ and $x''_{j+1,k}$ cannot completely share the remaining value, $x_{j+2,k}$ will be used to share the remaining remaining-value, and so on. In addition, a cover pixel with pixel value closing to a saturated value (a very small or large pixel value, i.e., $x_{j,k} \approx 0$ or $x_{j,k} \approx 255$ for a 256-level grayscale image) is not a good cover pixel for sharing a WPD, since its stego-pixels may not completely share a larger $a_{i,k}$. In such a case, more than one cover pixel may be consumed to share $a_{i,k}$. The above case is included in the example in Section 2.3. Increasing the number of cover images (i.e., n) is an effective solution to have a smaller $a_{i,k}$, since $d_i = \sum_{k=1}^{n} r_k \times a_{i,k} \times sign(d_i)$. A smaller $a_{i,k}$ may consume less cover pixels than a larger one. Table 1 has shown when n is increased, $a_{i,k}$ is significantly decreased.

Table 1 An example of $a_{i,k}$

$\|d_i\|$	Number of shadows									
	2	4		6			8			
	$a_{i,1}$	$a_{i,2}$	$a_{i,1}$	$a_{i,3}$	$a_{i,2}$	$a_{i,1}$	$a_{i,4}$	$a_{i,3}$	$a_{i,2}$	$a_{i,1}$
0	0	0	0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0	0	0	1
2	2	1	0	0	1	0	0	0	1	0
3	3	1	1	0	1	1	0	0	1	1
4	4	2	0	1	0	0	0	1	0	0
5	5	2	1	1	0	1	0	1	0	1
6	6	2	2	1	1	0	0	1	1	0
7	7	3	1	1	1	1	0	1	1	1
8	8	3	2	2	0	0	1	0	0	0
9	9	3	3	2	0	1	1	0	0	1
10	10	4	2	2	1	0	1	0	1	0
11	11	4	3	2	1	1	1	0	1	1
12	12	4	4	2	2	0	1	1	0	0
13	13	5	3	2	2	1	1	1	0	1
14	14	5	4	2	2	2	1	1	1	0
15	15	5	5	3	1	1	1	1	1	1
16	16	6	4	3	2	0	2	0	0	0

2.2 Revealing process

In the proposed scheme, a secret image is shared by $2n$ shadow images, where a pair of brother stego-pixels share a smaller difference value between a pair of neighboring pixels in the secret image. When all of the shared difference values are obtained, the secret image can be completely revealed. The following process is applied to reveal the secret image and restore the original cover images.

Input: $2n$ stego-images by which the secret image I is shared.
Output: A secret image I and n original cover images.

1. For each pair of brother stego-images S'_k and S''_k, do steps 2–4.
2. Set $i = j = 1$ and scan stego-images S'_k and S''_k as they were scanned in the sharing process.
3. Calculate

$$a_{i,k} = \begin{cases} (x'_{j,k} - x''_{j,k}) & \text{if } x'_{j,k}, x''_{j,k} \notin \{0, 255\}, \\ (x'_{j,k} - x''_{j,k}) + ... + (x'_{m,k} - x''_{m,k}) & \text{otherwise,} \end{cases}$$

where $j < m$, $x'_{m,k} \notin \{0, 255\}$, $x''_{m,k} \notin \{0, 255\}$, and either $x'_{h,k} \in \{0, 255\}$ or $x''_{h,k} \in \{0, 255\}$ for $j \leq h < m$. Then set

$$j = \begin{cases} j+1 & \text{if } x'_{j,k}, x''_{j,k} \notin \{0, 255\}, \\ m+1 & \text{otherwise.} \end{cases}$$

4. Set $i = i + 1$. Go to step 3 if $i \leq N$.
5. Restore each pixel j in S_k to its original value $x_{j,k} = \lceil (x'_{j,k} + x''_{j,k})/2 \rceil$.
6. Obtain the difference between pixels y_{i-1} and y_i, in the secret image, by calculating $d_i = \sum_{k=1}^{n} r_k \times a_{i,k}$, where $1 \leq i \leq N$.
7. For $1 \leq i \leq N$, reveal $y_i = y_{i-1} - d_i$ and follow the image scanning order in the sharing process to reconstruct the secret image. Note that $y_0 = 128$ for a 256-level grayscale image.

In step 3, if $x'_{j,k} \in \{0, 255\}$ or $x''_{j,k} \in \{0, 255\}$, it implies that a saturated stego-pixel is encountered. In this situation, to calculate $a_{i,k}$, we have to add up the result of $x'_{j,k} - x''_{j,k}$ and the coming difference values $x'_{j+1,k} - x''_{j+1,k}$, ... until a pair of unsaturated brother stego-pixels is encountered, i.e., $x'_{m,k}, x''_{m,k} \notin \{0, 255\}$. Recall that in step 7 in Section 2.1, more than one cover pixel is consumed when sharing a WPD and a saturated stego-pixel is encountered.

In the sharing process, a WPD value $a_{i,k}$ is always greater than or equal to 0. To embed the information about whether $d_i = y_{i-1} - y_i$ is smaller than 0 or not, the sharing process replaces the values of $x'_{j,k}$ and $x''_{j,k}$ with each other in step 7 if $d_i < 0$ such that $x'_{j,k} < x''_{j,k}$. Therefore, in the revealing process, if $a_{i,k}$ is a negative integer, it implies that $y_{i-1} < y_i$ in the secret image. Otherwise, it implies that $y_{i-1} \geq y_i$.

2.3 An example illustrating the proposed scheme

This section gives an example illustrating the proposed scheme. In the example, a secret image I in Fig. 3a with $N = 16$ would be shared by four shadows in Fig. 3e–h, i.e., $n = 2$. In both secret and cover images, each pixel value is between 0 and

255, i.e., they are 256-level grayscale images. Figure 3b lists the difference between y_{i-1} and y_i, where $1 \leq i \leq N$. For example, $y_0 - y_1 = 128 - 155 = -27$, $y_1 - y_2 = 155 - 157 = -2$, etc. Figure 3c and d are two cover images from which four stego images are constructed. The dimension of Fig. 3c is different from that of Fig. 3d. The secret and cover images are scanned in a zigzag order. For example, $y_1 = 155$, $y_5 = 150$, $x_{1,1} = 4$, $x_{5,1} = 12$, $x_{1,2} = 200$, $x_{5,2} = 220$, etc.

Given $d_1 = -27, r_1 = 1, r_2 = 2, R_1 = 1$, and $R_2 = 3$, in step 3 in Section 2.1,

$$\begin{aligned}
&A_{1,2} = |-27| = 27,\\
&a_{1,2} = \lceil 27/3 \rceil = 9,\\
&A_{1,1} = |-27| - \textstyle\sum_{w=1+1}^{2} r_w \times a_{1,w} = 27 - 2 \times 9 = 9, \text{ and}\\
&a_{1,1} = \lceil 9/1 \rceil = 9
\end{aligned}$$

are calculated. Then in step 6 in Section 2.1, $\dot{x}_{1,1} = 4 + \lfloor 9/2 \rfloor = 8$ and $\ddot{x}_{1,1} = 8 - 9 = -1$ are calculated. In the next step, $(D, x'_{1,1}, x''_{1,1})$ is first set to $(2 \times |-1|, 8 - 1, 0) = (2, 7, 0)$. Since $d_1 < 0$, $(D, x'_{1,1}, x''_{1,1})$ is then set to (2, 0, 7). As $a_{1,1} = 9$ cannot be

Fig. 3 An example illustrating the proposed scheme: **a** secret image I; **b** difference between y_{i-1} and y_i; **c** cover image S_1; **d** cover image S_2; **e** shadow S'_1; **f** shadow S'_2; **g** shadow S''_1; **h** shadow S''_2

155	157	150	147
170	180	175	150
180	182	190	183
195	190	193	195

(a)

–27	–2	7	3
10	–5	–25	–3
–10	–2	–8	7
–5	3	2	–12

(b)

4	15	3	6
8	2	9	12
6	5	4	7
3	0	0	8
5	4	6	9

(c)

200	230	198	199
221	224	240	220
190	198	197	195
203	205	207	204

(d)

0	14	3	6
6	0	8	12
5	6	3	7
3	0	0	7
3	4	6	8

(e)

195	229	199	199
223	223	235	219
188	197	195	196
202	205	207	202

(f)

7	16	3	5
10	3	9	11
6	4	5	7
2	0	0	9
7	4	5	9

(g)

204	230	196	198
219	225	244	220
192	198	198	193
204	204	206	206

(h)

completely shared by $x'_{1,1}$ and $x''_{1,1}$, the next pixel $x_{2,1} = 15$ must be used to share the remaining value of $9 - 7 = 2$ and the stego-pixels become $x'_{2,1} = 14$ and $x''_{2,1} = 16$. On the other hand, $a_{1,2}$ can be completely shared by $x'_{1,2} = 195$ and $x''_{1,2} = 204$, which also implies $d_1 < 0$. Similarly, $d_2 = -2$, $a_{2,1} = 0$, and $a_{2,2} = 1$, so $(x'_{3,1}, x''_{3,1})$ and $(x'_{2,2}, x''_{2,2})$ are set to $(3, 3)$ and $(229, 230)$, respectively, and the process continues. As $x_{14,1} = x_{15,1} = 0$, they cannot be used to share any secret pixel values and must be unchanged. Finally, four stego images are constructed as shown in Fig. 3e–h. In the example, since S_1 contains saturated pixels and the WPD value $a_{1,1}$ is spread to two cover pixels in S_1, the required size of S_1 must be greater than that of the secret image I. On the other hand, as S_2 does not contain any saturated pixel and each WPD value $a_{i,2}$ consumes only one cover pixel, the required size of S_2 is equal to that of the secret image I.

To reveal the secret image shared by the four shadows in Fig. 3e–h, the decoder calculates $a_{1,1} = (x'_{1,1} - x''_{1,1}) + (x'_{2,1} - x''_{2,1}) = (0 - 7) + (14 - 16) = -9$, $a_{1,2} = x'_{1,2} - x''_{1,2} = 195 - 204 = -9$, and $d_1 = a_{1,1} + a_{1,2} \times 2 = -27$, since $x'_{1,1} \in \{0, 255\}$ and $x'_{2,1}, x''_{2,1} \notin \{0, 255\}$. Given $d_1 = -27$, $y_1 = 128 - d_1 = 155$ is revealed. Similarly, $y_2 = y_1 - d_2 = 155 - (a_{2,1} + a_{2,2} \times 2) = 157$ is revealed, where $a_{2,1} = x'_{3,1} - x''_{3,1} = 3 - 3 = 0$ and $a_{2,2} = x'_{2,2} - x''_{2,2} = 229 - 230 = -1$. The revealing process continues until the secret image is completely revealed. To restore the original cover images S_k, the decoder simply calculates $x_{j,k} = \lceil (x'_{j,k} + x''_{j,k})/2 \rceil$ for each cover image S_k. For example, $x_{1,1} = \lceil (0 + 7)/2 \rceil = 4$, $x_{2,1} = \lceil (14 + 16)/2 \rceil = 15$, etc.

3 Simulation results

To show the feasibility and performance of the proposed scheme, Airplane (Fig. 4a) was selected to be a secret image shared by shadows constructed from 1–4 cover images (Fig. 4b–e), where both secret and cover images are 256-level grayscale images each of which contains 512 × 512 pixels. In the simulation, the visual quality of a shadow image with N pixels was evaluated by peak signal to noise ratio (PSNR) which was defined as follows:

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255 \times 255 \times N}{\sum_{j=1}^{N} (x_j - x'_j)^2} \ \mathrm{dB},$$

where x_j and x'_j were the pixel values of the original cover image and the stego image, respectively, and $0 \le x_j, x'_j \le 255$. Two images with a larger PSNR value means they are more similar than those with a smaller one.

Table 2 shows the PSNR values for sharing Airplane among 1–4 cover images, where PSNR$'$ and PSNR$''$ denotes the PSNR values for brother stego-images S'_k and S''_k, respectively. When $n = 1$ and Airplane is shared by two shadows created from Lena, 26 secret pixels cannot be completely shared by the two shadows. One of the reasons is that there exist some differences, between secret pixels, each of which consumes more than one cover pixel. The problem is the same as that in Fig. 3e and g in which four cover pixels are consumed by two differences. To solve this problem, a larger cover image may be selected. Alternatively, the encoder may select a smaller secret image to be shared. In the simulation, a smaller secret image with 511 × 512 pixels was used when $n = 1$. When $n \ge 2$, the secret image can be completely shared by the shadows with size equal to the secret image. In addition, when $n = 2$, $n = 3$,

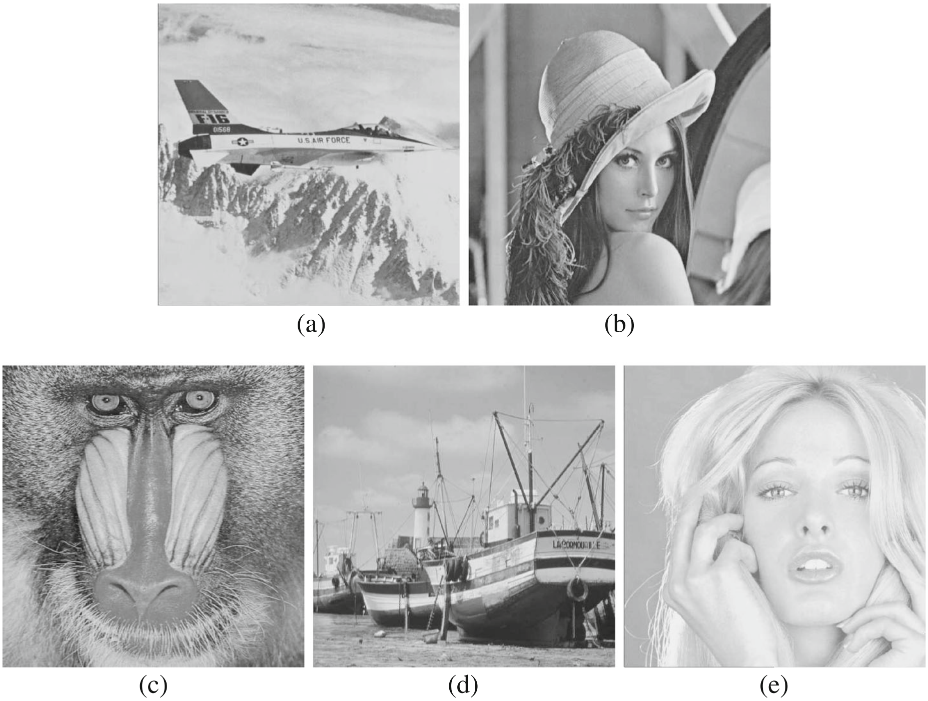


Fig. 4 Test images: **a** Airplane; **b** Lena; **c** Baboon; **d** Boat; **e** Tiffany

or $n = 4$, the average PSNR values can be up to 43.33 dB, 50.13 dB, or 54.70 dB, respectively. Obviously, a secret sharing application using the proposed scheme can obtain stego images with high visual quality.

In the simulation, when Airplane was shared between Lena and Baboon, four stego-images were constructed and the weighted factor for brother stego-images of Lena and Baboon were 1 and 2, respectively. Figure 5a and b show the revealed results by brother stego-images of Lena and Baboon, respectively. We can see that more secret information can be observed in Fig. 5b than that in Fig. 5a, since the weighted factor of Baboon is larger than that of Lena. If participants would like

Table 2 PSNR values of the simulation results

n	Cover images	PSNR$'$	PSNR$''$
1	Lena*	33.85	33.85
2	Lena	43.73	43.73
	Baboon	42.93	42.93
3	Lena	50.65	50.64
	Baboon	50.16	50.16
	Boat	49.58	49.58
4	Lena	53.72	53.71
	Baboon	54.32	54.34
	Boat	55.41	55.38
	Tiffany	55.36	55.34

*26 secret pixels cannot be shared

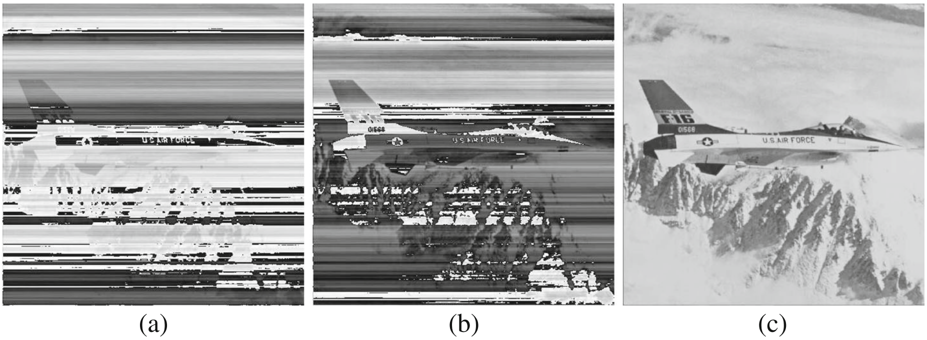


Fig. 5 Revealing results: **a** revealed alone by brother stego-images of Lena; **b** revealed alone by brother stego-images of Baboon; **c** revealed by all stego-images

to obtain more shared information, they may invite more participants to reveal the secret image. In the case of sharing Airplane between Lena and Baboon, if all brother stego-images of Lena and Baboon are gathered, the secret image can be completely revealed as shown in Fig. 5c.

Figure 6 shows the revealed results when Airplane was shared among Lena, Baboon, and Boat. Figure 6a, b, and c are the results revealed by brother

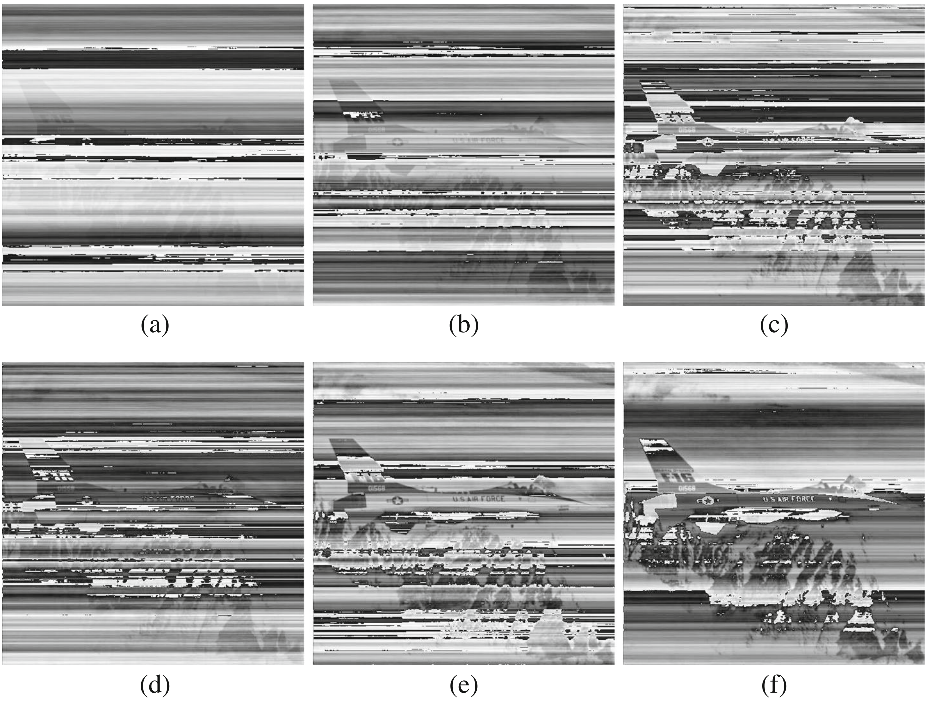


Fig. 6 Revealed results by various brother stego-images: **a** Lena; **b** Baboon; **c** Boat; **d** Lena and Baboon; **e** Lena and Boat; **f** Baboon and Boat

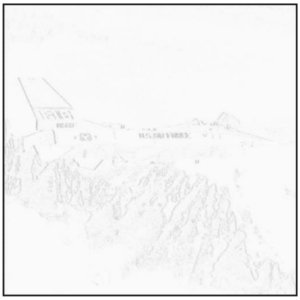
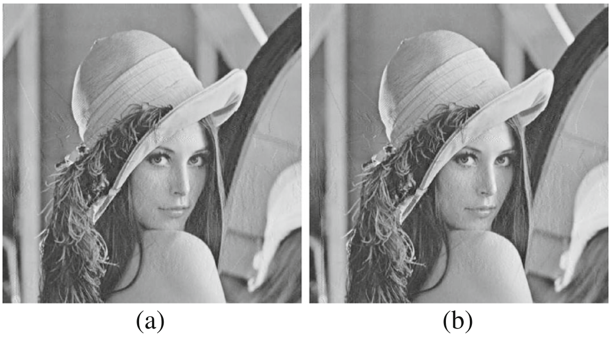


Fig. 7 Difference image shared by brother stego-images of Lena

stego-images of Lena, Baboon, and Boat, respectively, where their weighted factors are 1, 2, and 4, respectively. The figures also show that brother stego-images with a larger weighted factor can reveal more information than those with a smaller one. Figure 6d, e, and f are the results revealed by two families of brother stego-images. Figure 6d, e, and f are clearer than Fig. 6a, b, and c, respectively, since they are revealed by stego-images with larger weighted factors. For example, the weighted factors in Fig. 6a and d are 1 and $3 = 1 + 2$, respectively, and those in Fig. 6b and e are 2 and $5 = 1 + 4$, respectively.

To show the differences between neighboring pixels in the secret image, we converted WPD values into a 256-level difference image. In such a case, sharing a difference image is equivalent to sharing a secret image from which the difference image is created. The converted result is shown in Fig. 7 in which a whiter pixel denotes a smaller difference value compared to a darker one and a frame is added to identify the boundary of the image. It is expected that most pixels in the difference image are approximated to white ones, since most neighboring pixels in a natural image are similar. If the difference image is only shared by brother stego-images of Lena (one cover image is used and $n = 1$), 26 secret pixels cannot be shared, as listed in Table 2. Figure 8 depicts the results of brother stego-images and it shows that the stego-images are very similar to their cover image in Fig. 4b.

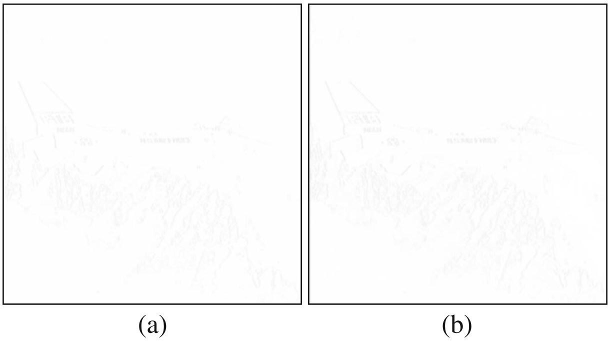
Figure 9 shows the converted WPD images for $n = 2$, where cover images are Lena and Baboon. Surprisingly, the images in Fig. 9 are significantly smoother than that in Fig. 7. The reason is that a difference is divided into smaller WPDs such that the



(a) (b)

Fig. 8 Brother stego-images of Lena for $n = 1$: **a** Lena′; **b** Lena″

Fig. 9 Difference images: **a** shared by brother stego-images of Lena; **b** shared by brother stego-images of Baboon



difference is equal to the sum of products of each WPD and its weight. For example, row 4 in Table 1 shows that $|d_i| = 3$ is divided into WPD values of $a_{i,2} = 1$ and $a_{i,1} = 1$ if $n = 2$, and $|d_i|$ is equal to $3 = a_{i,2} \times 2 + a_{i,1} \times 1$. As a result, the distortion of stego-images is significantly reduced.

Figure 10 demonstrates the brother stego-images for $n = 2$, where cover images are Lena and Baboon. Figure 10a and b are the brother stego-images of Lena and they are visually indistinguishable from their original image in Fig. 4b. Brother stego-images of Baboon are shown in Fig. 10c and d, and their visual quality is as high as that of Fig. 10a and b. As listed in Table 2, the more cover images are used, the

Fig. 10 Brother stego-images for $n = 2$: **a** Lena′; **b** Lena″; **c** Baboon′; **d** Baboon″

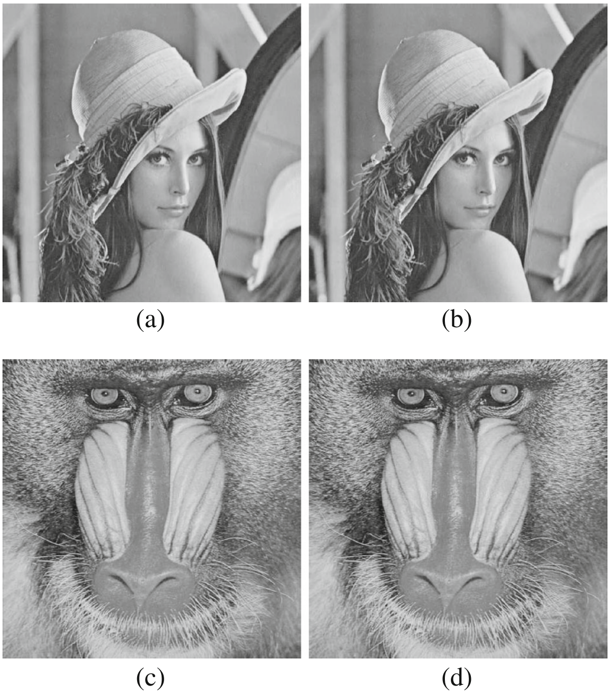


Table 3 A comparison of performances

Approaches	Progressive	Reversible	Friendly	Visual quality
Proposed	Yes	Yes	Yes	High
Fang [5]	Yes	No	Yes	Low
Liu et al. [13]	No	No	No	N/A
Thien and Lin [17]	No	No	Yes	Medium
Wang and Shyu [19]	Yes	No	No	N/A
Wang et al. [21]	No	No	No	N/A

higher visual quality of stego-images can be obtained. It can be expected that the visual quality of stego-images is much better than that of Figs. 8 and 10 if the number of cover images is more than two (i.e., $n > 2$). Accordingly, here the demonstration of converted WPD images and stego-images for $n > 2$ would be skipped.

The experimental results prove that the proposed scheme can obtain shadow images with high visual quality, the secret image can be progressively and completely revealed, and all cover images can be losslessly recovered. All shadow images are meaningful and they are friendly to be managed.

Table 3 compares the proposed scheme with a number of secret sharing approaches. As shown in Figs. 5 and 6, the proposed scheme can progressively and completely reveal a secret image. In the table, the proposed scheme is the only one which can completely recover the original cover image (i.e., reversible). It is not friendly to manage shares in secret sharing schemes [13, 19, 21] in which a share is a meaningless image. In Fang's scheme [5] and Thien and Lin's method [17], a meaningful image is used for constructing a share. However, a shadow image in their approaches is visually distinguishable from its original cover image. If the shadow image is an important image for medical purpose, an incorrect diagnosis may occur. The visual quality of shadow images is compared in the column of visual quality in the table. The PSNR values in Table 2 show that the proposed scheme can obtain a shadow image with higher visual quality compared to those in references [5, 17]. Note that, in Table 3, N/A denotes "not available" which means a scheme does not provide the compared item (i.e., visual quality), since a shadow image in the scheme is a visually meaningless one.

The contributions of the proposed scheme are summarized as follows. First, it transforms a larger pixel value in the secret image to be shared into a smaller difference value d_i. Then $|d_i|$ is divided into n WPD values ($a_{i,1}, a_{i,2}, ..., a_{i,n}$) such that $|d_i| = a_{i,1} \times 2^0 + a_{i,2} \times 2^1 + ... + a_{i,n} \times 2^{n-1}$, where the weight of $a_{i,w}$ is equal to 2^{w-1}. Finally, each WPD value is embedded into a difference between a pair of brother stego-pixels in stego-images. Since $|d_i| \geq a_{i,1} + a_{i,2} + ... + a_{i,n}$ and $a_{i,w}$ is minimal, the distortion of stego-images is also minimal. Therefore, participants sharing the secret image can obtain shadow images with high visual quality.

4 Conclusions

A reversible secret sharing scheme has been proposed in this paper. In the scheme, a secret image can be shared by shadow images with high visual quality. In addition, it can completely reveal the secret image and reversibly recover shadow images to their original cover images. A pixel value in a secret image is completely revealed by computing the sum of products of weighted difference values and their weights in brother stego-images. Any brother stego-images can completely recover themselves to their original cover image by simply calculating the average values of corresponding brother stego-pixel values. The simulation results have shown that the proposed scheme can construct a shadow image with higher visual quality compared to existing approaches. The proposed scheme is a good candidate for applications which need to reversibly recover shadow images with high visual quality and completely reveal a secret image shared among shadow images.

References

1. Chang CC, Hsieh YP, Liao CC (2011) A visual secret sharing scheme for progressively restoring secrets. Journal of Electronic Science and Technology 9(4):325–331
2. Chang CC, Lin CC, Lin CH, Chen YH (2008) A novel secret image sharing scheme in color images using small shadow images. Inf Sci 178(11):2433–2447
3. Chang CC, Lin CY, Tseng CS (2007) Secret image hiding and sharing based on t-n threshold. Fundam Inform 76(4):399–411
4. Chen YF, Chan YK, Huang CC, Tsai MH, Chu YP (2007) A multiple-level visual secret-sharing scheme without image size expansion. Inf Sci 177(21):4696–4710
5. Fang WP (2008) Friendly progressive visual secret sharing. Pattern Recogn 41(4):1410–1414
6. Feng JB, Wu HC, Tsai CS, Chang YF, Chu YP (2008) Visual secret sharing for multiple secrets. Pattern Recogn 41(12):3572–3581
7. Feng JB, Wu HC, Tsai CS, Chu YP (2005) A new multi-secret images sharing scheme using Largrange's interpolation. J Syst Softw 76(3):327–339
8. Hou YC (2003) Visual cryptography for color images. Pattern Recogn 36(7):1619–1629
9. Hou YC, Quan ZY (2011) Progressive visual cryptography with unexpanded shares. IEEE Trans Circuits Syst Video Technol 21(11):1760–1764
10. Hsu HC, Chen TS, Lin YH (2004) The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing. In: 2004 IEEE international conference on networking, sensing and control. Taipei, Taiwan, pp 996–1001
11. Lin PY, Lee JS, Chang CC (2009) Distortion-free secret image sharing mechanism using modulus operator. Pattern Recogn 42(5):886–895
12. Lin CC, Tsai WH (2004) Secret image sharing with steganography and authentication. J Syst Softw 73(3):405–414
13. Liu Z, Ahmad MA, Liu S (2008) Image sharing scheme based on combination theory. Opt Commun 281(21):5322–5325
14. Naor M, Shamir A (1995) Visual cryptography. In: Advances in cryptology—EUROCRYPT'94. Lecture notes in computer science, vol 950. Springer, Berlin, pp 1–15
15. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
16. Thien CC, Lin JC (2002) Secret image sharing. Comput Graph 26(5):765–770
17. Thien CC, Lin JC (2003) An image-sharing method with user-friendly shadow images. IEEE Trans Circuits Syst Video Technol 13(12):1161–1169
18. Ulutas M, Ulutas, G, Nabiyev VV (2011) Medical image security and EPR hiding using Shamir's secret sharing scheme. J Syst Softw 84(3):341–353
19. Wang RZ, Shyu SJ (2007) Scalable secret image sharing. Signal Process Image Commun 22(4):363–373
20. Wang FH, Yen KK, Jain LC, Pan JS (2007) Multiuser-based shadow watermark extraction system. Inf Sci 177(12):2522–2532
21. Wang D, Zhang L, Ma N, Li X (2007) Two secret sharing schemes based on Boolean operations. Pattern Recogn 40(10):2776–2785
22. Wu YS, Thien CC, Lin JC (2004) Sharing and hiding secret images with size constraint. Pattern Recogn 37(7):1377–1385

Ching-Chiuan Lin received his Ph.D. degree in Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan, in 2008. He is an Associate Professor with Department of Information Management, Overseas Chinese University. His research interests include image processing, data hiding, network computing, and software engineering. Dr. Lin was selected as an honorary member of Phi Tau Phi Scholastic Society of The Republic of China in 2008.

Lun Hao Liao (Howard Liao) is a Ph.D. Candidate as well as an Adjunct Instructor in Department of Information Management, Chaoyang University of Technology, Taichung, Taiwan. His research interests include watermarking, data mining, network computing, and software engineering.

Kuo Feng Hwang received his Ph.D. degree in Applied Mathematics from National Chung Hsing University, Taichung, Taiwan, in 2006. Dr. Hwang is an Assistant Professor with Department of Information Management, Overseas Chinese University. He is also the Director of the Global Logistics Center from 2009 till now at the Overseas Chinese University. His research interests include image processing, data mining, E-commerce, and data hiding.

Shih-Chieh Chen received the B.S. degree in Mathematics and M.S degree in Applied Mathematics from the Tunghai University, Taiwan, in 1991 and 1993 respectively, and the Ph.D. degree in Applied Mathematics from the National Chung Hsing University, Taiwan, in 2006. He was the Director of the Library and Information Center from 2007 to 2008, and the Director of the Teaching Development Center from 2008 to 2009 at the Overseas Chinese University, Taiwan. He is currently an Associate Professor of the department of Information Management at the Overseas Chinese University. His current research interests include evolutionary computation, optimization, data processing and cryptography.