A Sudoku-based Secret Image Sharing Scheme with Reversibility (Invited Paper)

Chin-Chen Chang
Department of Information Engineering and Computer Science,
Feng Chia University, 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan.
Email: ccc@cs.ccu.edu.tw

Pei-Yu Lin[a], Zhi Hui Wang[b] and Ming Chu Li[b]
[a]Department of Information Communication,
Yuan Ze University, 135 Yuan-Tung Rd., Chung-Li, 32003, Taiwan.
Email: pagelin3@gmail.com
[b]School of Software, Dalian University of Technology, Dalian, Liaoning, China.
Email: Wangzhihui1017@yahoo.cn; li_mingchu@yahoo.com

***Abstract*—A common drawback of the image sharing with steganography approaches is that the revealed secret image is distorted due to the truncation of the grayscale secret image. To lossless reveal the secret image in the (*t*, *n*)-threshold, we provide a novel sharing scheme in this article. Moreover, the original host image can be recovered by the embedded shadow images. To accomplish the above purposes, the proposed scheme derives the secret shadows and generates the meaningful shadow images by adopting the sudoku. In the new scheme, the sudoku grid is setting to 16×16 and divided into sixteen 4×4 blocks. Thus, we can embed 4×(*t*-1) secret bits into each pixel pair of the host image. Besides, the embeddable secret capacity can be improved according to the threshold *t* in the (*t*, *n*)-threshold sharing system. The experiments show that the shadows can be successfully camouflaged in the host image with satisfactory quality. The distortion of the embedded host pixels is limited within range [0, 3]. Moreover, the proposed scheme provides a large capacity for embedded secret data.**

***Index Terms*—secret sharing, steganography, reversible, sudoku, puzzle**

I. INTRODUCTION

The purpose of secret sharing mechanisms [1-4] is to share a secret data among participants. The secret data has been divided into several shadows, and the shadows are dispatched to the corresponding participants. To recover the secret data, authorized participants with sufficient shadows can cooperate to recover the secret data. Blakely [1] and Shamir [2] first introduced the (*t*, *n*)-threshold secret sharing system in 1979. In this system, a dealer can encode and divide the secret data into *n* shadows. Then, the dealer distributes the shadows to the involved participants. Any *t* out of *n* authorized participants can provide their shadows and cooperate to recover the secret data.

Manuscript received April 20, 2009; revised October 7, 2009; accepted December 7, 2009.

Recently, the concept of (*t*, *n*)-threshold secret sharing has been usually exploited to share precious and confidential imagery [5-8]. Thien and Lin [9] proposed a secret image sharing scheme. In their scheme, a dealer generates *n* distinct shadows from the secret image for all participants. Any *t* out of *n* participants can cooperate to recover the lossless secret image. Based on Thien and Lin's scheme, Wang and Shyu [10] introduce a scalable secret image sharing scheme with three sharing modes, which are the multisecret, the priority, and the progressive modes. Each participant can be assigned a different priority shadow. Hence, the quality of the recovered secret image depends on the priorities of the shadows. Nevertheless, the generated *n* shadows in [9] and [10] are random-like images. A malicious intruder may attract attraction to such meaningless (random-like) shadows delivered via an insecure channel. Besides, to share the secret image with lossless, the size of the original secret image may be expanded in [9, 10].

To accomplish the purpose of meaningful shadows, the steganography approach is utilized to camouflage the shadows in host images. The embedded host images are also called the shadow images (or the stego images) [11-13]. From the visual perception, the content of the shadow image is meaningful so the shadows can be concealed from intruders. Thus, the quality of the shadow images is an important essential in the secret sharing mechanism. The image sharing methods proposed by Lin and Tsai [12] and Wu et al. [13] produce shadows based on the (*t*-1)-degree polynomial and embed shadows to host images. However, the revealed secret image is distorted due to truncating gray pixels with values larger than 250. If the shared media are artistic and medical images, any slight distortion may be intolerable.

To reveal the secret image with lossless, Zhao et al. [14] and Chang et al. [15] used two pixels to represent the exceeding gray values. Unfortunately, these improved processes result in the expansion of the secret image. It may reduce the capacity of the embedded secret data and distort the quality of shadow images. In addition, the

doi:10.4304/jcm.5.1.5-12

maximum secret capacity of [12, 16] is a quarter of the size of the host image. In [9, 11, 13, 15], the capacity of the embedded secret is also limited.

In general, the derived shadows often lead to problems of shadow expansion, meaninglessness, quality and fidelity [14, 17, 18]. The sharing schemes shall encode the secret image without expanding the image size or requiring any extra information. The shadow must be meaningful for camouflaged purposes. Hence, the quality of the shadow images must be satisfactory. Moreover, the fidelity of the revealed secret data must be distortion-free (lossless).

In this article, we propose a new image sharing scheme that satisfies all of these essentials and possesses reversible characteristics. The reversibility of the proposed scheme allows authorized participants to reconstruct the distorted host image to the original one after retrieving the secret data. Reconstructing an original host image without distortion [19, 20] is especially important for medical, military, or artistic images. Recently, many image-processing techniques, including image hiding, steganography, image authentication, and digital watermarking [21-23], focus on achieving reversibility. Unfortunately, current meaningful sharing schemes [9, 11-13, 15, 16] are incapable of reconstructing the shadow image to the original host image. Inspired by potential practicability, we design a reversible image sharing scheme based on sudoku for preserving the fidelity of valuable host images.

Sudoku [24-27] is a logic-based number placement puzzle which is presented on a square grid. The proposed scheme utilizes the concept of sudoku to conceal the shadow with reversibility. The rest of this article is organized as follows. Shamir's (t, n)-threshold system and sudoku are introduced in Section II. The novel reversible sharing scheme is elaborated in Section III, followed by the experimental results and performance analyses in Section IV. Finally, the conclusions are given in Section V.

II. Related Works

In this section, we briefly introduce Shamir's (t, n)-threshold sharing mechanisms [1, 2]. We subsequently describe the concept of sudoku which is adopted for embedding and restoring the secret of the proposed sharing scheme.

A. The (t, n)-threshold System

To share a secret s, a dealer determines a prime m and generates a (t-1)-degree polynomial $F(x)$ as

$$F(x) = (s + a_1 x + \ldots + a_{t-1} x^{t-1}) \bmod m . \quad (1)$$

Here, the coefficients a_1, a_2, …, a_{t-1} are randomly determined by the integers within [0, m-1]. The dealer then can derive n shadows $y_1, y_2, \ldots, y_n$ as

$$y_1 = F(1), \quad y_2 = F(2), \quad \ldots, \quad y_n = F(n) . \quad (2)$$

Afterward, the dealer distributes the shadows y_i's to the involved participants.

Generally, a shadow set is called a qualified set if the number of participants is greater than or equal to t. Authorized participants in a qualified set can cooperate to reconstruct $F(x)$ using the Lagrange interpolation polynomial. That is, authorized participants can construct $F(x)$ to recover all coefficients s, a_1, a_2, …, and a_{t-1}. Hence, the secret s can be obtained among the authorized participants. On the contrary, we label a shadow set as a forbidden set the number of cooperative participants is less than t participants. No one in the forbidden set can correctly reconstruct $F(x)$ by Lagrange interpolation polynomial.

Note that the values of y_i is within [0, m-1]. While arranging the shadows, it appears meaningless (random-like). To conceal the shadows from intruders, the proposed scheme produces n meaningful shadow images by camouflaging the shadows in a host image.

B. Sudoku

Sudoku [24-27] is a puzzle that presented on a square grid. The size of sudoku grid is usually 9×9 and it is divided into nine 3×3 blocks. The objective is to fill the grid using the digits from 1 to 9. That is, some elements of the original sudoku grid have been assigned by the digits within 1 to 9 as shown in Fig. 1(a). The goal is to complete the sudoku grid such that every 3×3 block, every row and column of the grid contains different digits form 1 to 9 exactly once. Fig. 1(b) shows one of the sudoku solutions of 1(a).

	5		2				9	1
	4				1	6		
	1		6	7				
3				9	6			
	9	8		3		2	6	
			1	2				8
				1	3		7	
		1	4				2	
9	3				2		1	

(a) An 9×9 Sudoku puzzle

6	5	3	2	4	8	7	9	1
7	4	9	3	5	1	6	8	2
8	1	2	6	7	9	4	5	3
3	2	5	8	9	6	1	4	7
1	9	8	7	3	4	2	6	5
4	7	6	1	2	5	9	3	8
2	8	4	9	1	3	5	7	6
5	6	1	4	8	7	3	2	9
9	3	7	5	6	2	8	1	4

(b) One of the solutions of (a)

Figure 1. Example of a sudoku puzzle

The sudoku puzzle is invented in 1979 by Garns and Dell Magazines, and called "Number Place". Sudoku became popular in Japan in 1986 by the publisher Nikoli, and it was internationally known in 2005. In 2005, Felgenhauer and Jarvis compute the classic 9×9 sudoku

solutions to show that total number of possible solutions is 6,670,903,752,021,072,936,960 ≈ 6.671×10^{21}. In 2007, Russell and Jarvis [26] showed that if various possible symmetries (e.g. rotation, reflection, and etc.) are allowed, then the number of fundamental solutions of 9×9 Sudoku grid is 5,472,730,538.

Based on the characteristic of sudoku puzzle, we treat the secret shadows as the sudoku digits in the proposed embedding procedure to satisfy the steganography, security, and reversibility essentials.

III. The Proposed Scheme

Given a shared secret image, the dealer is responsible for deriving shadows from secret image and producing n shadow images (steganography). The new sharing process is introduced in Subsection 3.1. Given any t out of n shadow images, the involved participants can losslessly reconstruct the secret image and the host image. Subsection 3.2 discusses how to retrieve the secret image and reconstruct the original host image.

10	0	11	5	8	5	1	2	9	3	6	4	12	14	7	13
13	8	4	5	7	6	9	0	10	14	11	12	2	15	3	1
12	7	14	1	10	3	4	15	0	8	13	2	9	6	11	5
6	2	3	9	12	13	14	11	7	15	5	1	10	4	0	8
2	5	6	7	0	9	11	14	3	4	12	15	8	1	13	10
9	12	1	4	15	8	7	13	5	2	10	0	11	3	6	14
11	3	13	10	6	12	2	5	8	1	9	14	15	0	4	7
0	15	8	14	4	1	10	3	13	11	7	6	5	2	12	9
7	1	10	12	11	0	6	8	4	13	3	5	14	9	3	15
8	9	5	11	2	7	15	4	14	12	0	10	6	13	1	3
3	4	15	13	5	14	12	9	1	6	2	7	0	8	10	11
14	6	0	2	13	10	3	1	15	9	8	11	7	12	5	4
15	14	2	6	3	2	8	10	11	7	4	13	1	5	9	0
5	13	2	8	9	15	0	7	12	10	1	3	4	11	14	6
4	10	9	3	1	11	5	6	2	0	14	8	13	7	15	12
1	11	7	0	14	4	13	12	6	5	15	9	3	10	8	2

Figure 2. Instance of 16×16 sudoku grid using the digits from 0 to 15

A. The (t, n) Sharing Procedure

Let S be a shared secret image formed by a sequence of bit streams. To share the secret S with sudoku, the new scheme extends the size of a sudoku grid to 16×16 to increase the secret capacity. Besides, to suit the embedding process, the sudoku grid filled with the digits from 0 to 15. Fig. 2 demonstrates an instance of a 16×16 sudoku grid using the digits from 0 to 15.

Preliminaries

In the proposed sharing scheme, the dealer has to assign a unique key K_i to each participant, where i =1, 2, …, n. In addition, suppose that O is the grayscale host image with $H\times W$ pixels. The pre-process is listed as follows.

Step 1: Pair each pixel in O. That is, there are $(H\times W)/2$ pixel pairs.

Step 2: Generate a matrix M with the size of $H\times W$. Here, M is consisted of sudoku grids with the size 16×16, as shown in Fig. 3.

Step 3: Divide the secret bit stream S into non-overlapping segments with 4 bits, where $S=(s_1, s_2, \ldots, s_m)_{16}$. Here, s_1, s_2, …, s_m are the base-16 numeral system digits.

For instance, when the secret bit stream is $(\underline{1010\ 0011})_2$, we can segment the stream into two digits $(10, 3)_{16}$. In the new approach, instead of embedding one secret pixel into the polynomial $F(x)$ [12, 16], the new scheme embeds $(t-1)$ secret digits into $F(x)$. This increases the capacity of the embedded secret data. For convenience, assume that the shared (t-1) digits of S are s_1, s_2, …, s_{t-1}. The processes of how to generate and camouflage the shadows is described in the following phases.

Shadow Derivation Phase

Let g_a and g_b be the selected pixel pair. The purpose of reversible sharing is to share the secret digits s_1, s_2,…, s_{t-1} and to preserve the original values of g_a and g_b.

Step 1: Learn the value m of the sudoku digit by mapping the row g_a and column g_b at a matrix M, where

$$m = M(g_a, g_b). \quad (3)$$

Step 2: Formulate an invertible polynomial $F(x)$ as

$$F(x) = (m + s_1x^1 + s_2x^2 + \ldots + s_{t-1}x^{t-1}) \bmod 16\,. \quad (4)$$

Step 3: Generate n shadows y_i's by feeding the secret key K_i into $F(x)$, where

$$y_1 = F(K_1),\ y_2 = F(K_2),\ \ldots,\ \text{and}\ y_n = F(K_n). \quad (5)$$

For example, in the (3, 3)-threshold system with the matrix M (shown in Fig. 3), the dealer can share two digits $(10)_{16}$ and $(3)_{16}$ of S into a pair of O, whose pixel pair (g_a, g_b) is (14, 7). The value of m can be computed by $m = M(g_a, g_b) = 6$ in Equation (3). Thus, $F(x)$ can be formulated as

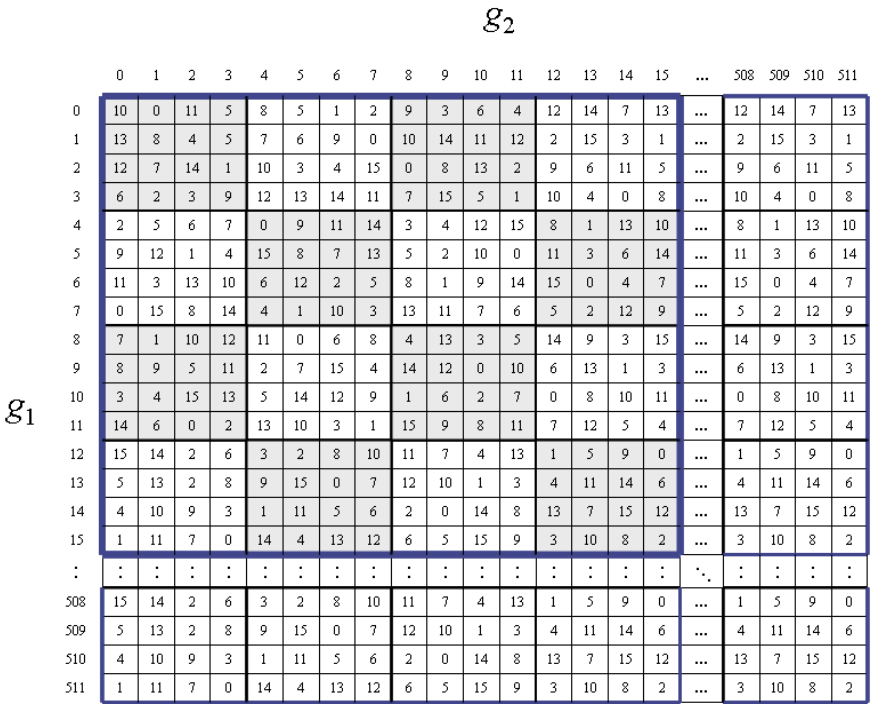
$$\begin{aligned} F(x) &= (m + s_1x^1 + s_2x^2) \bmod 16 \\ &= (6 + 10x^1 + 3x^2) \bmod 16. \end{aligned}$$

Camouflage Phase

To achieve the purposes of steganography, most shadow embedding approaches are based on bit replacement [12, 15, 16], which leads to the distortion of the host image. That is, these methods are incapable of reconstructing the shadow image to the original host image. To satisfy the property of reversibility, the proposed scheme preserves the feature of the original pixel pair g_a and g_b by utilizing the sudoku operation.

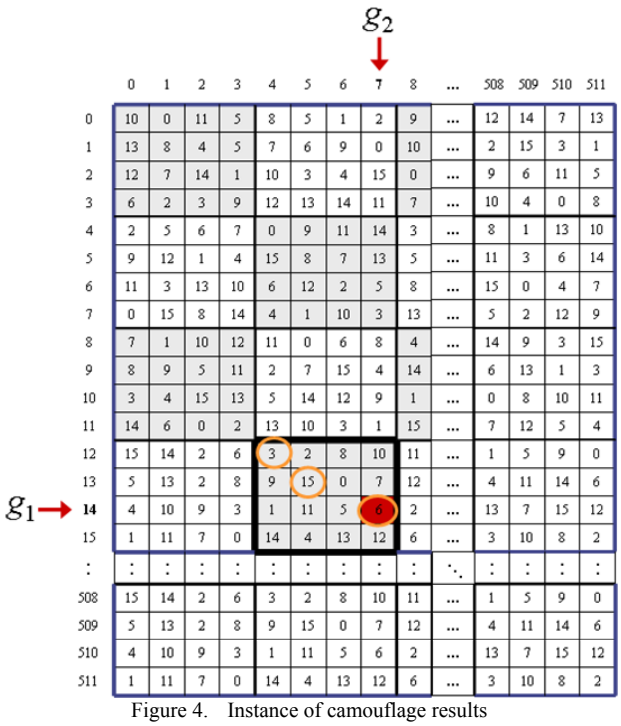
According to the generated shadows y_i's in Equation (5), the dealer subsequently embeds the shadows y_i's into the host pair g_a and g_b to obtain the embedded pair. From the located sudoku block of pair (g_a, g_b) at matrix M, there have sixteen digits ranged from 0 to 15. The dealer can obtain the new embedded pair (g_{a_i}, g_{b_i}) by selecting the corresponding shadow y_i at the row g_{a_i} and the column g_{b_i} in the same sudoku block. That is,

$$M(g_{a\_i}, g_{b\_i}) = y_i \ \text{ for } i = 1, 2, \ldots, n. \quad (6)$$



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...	508	509	510	511
0	10	0	11	5	8	5	1	2	9	3	6	4	12	14	7	13	...	12	14	7	13
1	13	8	4	5	7	6	9	0	10	14	11	12	2	15	3	1	...	2	15	3	1
2	12	7	14	1	10	3	4	15	0	8	13	2	9	6	11	5	...	9	6	11	5
3	6	2	3	9	12	13	14	11	7	15	5	1	10	4	0	8	...	10	4	0	8
4	2	5	6	7	0	9	11	14	3	4	12	15	8	1	13	10	...	8	1	13	10
5	9	12	1	4	15	8	7	13	5	2	10	0	11	3	6	14	...	11	3	6	14
6	11	3	13	10	6	12	2	5	8	1	9	14	15	0	4	7	...	15	0	4	7
7	0	15	8	14	4	1	10	3	13	11	7	6	5	2	12	9	...	5	2	12	9
8	7	1	10	12	11	0	6	8	4	13	3	5	14	9	3	15	...	14	9	3	15
9	8	9	5	11	2	7	15	4	14	12	0	10	6	13	1	3	...	6	13	1	3
10	3	4	15	13	5	14	12	9	1	6	2	7	0	8	10	11	...	0	8	10	11
11	14	6	0	2	13	10	3	1	15	9	8	11	7	12	5	4	...	7	12	5	4
12	15	14	2	6	3	2	8	10	11	7	4	13	1	5	9	0	...	1	5	9	0
13	5	13	2	8	9	15	0	7	12	10	1	3	4	11	14	6	...	4	11	14	6
14	4	10	9	3	1	11	5	6	2	0	14	8	13	7	15	12	...	13	7	15	12
15	1	11	7	0	14	4	13	12	6	5	15	9	3	10	8	2	...	3	10	8	2
:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	:	⋱	:	:	:	:
508	15	14	2	6	3	2	8	10	11	7	4	13	1	5	9	0	...	1	5	9	0
509	5	13	2	8	9	15	0	7	12	10	1	3	4	11	14	6	...	4	11	14	6
510	4	10	9	3	1	11	5	6	2	0	14	8	13	7	15	12	...	13	7	15	12
511	1	11	7	0	14	4	13	12	6	5	15	9	3	10	8	2	...	3	10	8	2

Figure 3. Instance of 512×512 matrix M



	0	1	2	3	4	5	6	7	8	...	508	509	510	511
0	10	0	11	5	8	5	1	2	9	...	12	14	7	13
1	13	8	4	5	7	6	9	0	10	...	2	15	3	1
2	12	7	14	1	10	3	4	15	0	...	9	6	11	5
3	6	2	3	9	12	13	14	11	7	...	10	4	0	8
4	2	5	6	7	0	9	11	14	3	...	8	1	13	10
5	9	12	1	4	15	8	7	13	5	...	11	3	6	14
6	11	3	13	10	6	12	2	5	8	...	15	0	4	7
7	0	15	8	14	4	1	10	3	13	...	5	2	12	9
8	7	1	10	12	11	0	6	8	4	...	14	9	3	15
9	8	9	5	11	2	7	15	4	14	...	6	13	1	3
10	3	4	15	13	5	14	12	9	1	...	0	8	10	11
11	14	6	0	2	13	10	3	1	15	...	7	12	5	4
12	15	14	2	6	3	2	8	10	11	...	1	5	9	0
13	5	13	2	8	9	15	0	7	12	...	4	11	14	6
14	4	10	9	3	1	11	5	6	2	...	13	7	15	12
15	1	11	7	0	14	4	13	12	6	...	3	10	8	2
:	:	:	:	:	:	:	:	:	:	⋱	:	:	:	:
508	15	14	2	6	3	2	8	10	11	...	1	5	9	0
509	5	13	2	8	9	15	0	7	12	...	4	11	14	6
510	4	10	9	3	1	11	5	6	2	...	13	7	15	12
511	1	11	7	0	14	4	13	12	6	...	3	10	8	2

Figure 4. Instance of camouflage results

Fig. 4 illustrates an example of the camouflage processes. Assume that the generated shadows in Equation (5) are $y_1 = F(1) = 3$, $y_2 = F(2) = 6$, and $y_3 = F(3) = 15$. To camouflage the shadows, the dealer can derive the first shadow pair $(g_{a\_1}, g_{b\_1}) = (12, 4)$ from to the shadow $y_1 = 3$ in the 12-th row and 4-th column of the same sudoku block. According to the second shadow $y_2 = 6$, the adjusted shadow pair is $(g_{a\_2}, g_{b\_2}) = (14, 7)$. And, the third shadow pair (g_{a_3}, g_{b_3}) is (13, 5) by selecting the shadow $y_3 = 15$ in the sudoku block.

By repeating the shadow derivation and camouflage phases, the dealer can generate and camouflage all secret shadows into the host pairs in order to obtain n shadow images O_i's. Then, the dealer can distribute the meaningful shadow image O_i and the key K_i to the involved participants.

B. Secret Revealing Procedure

Given any t out of n shadow images O'_j's and the keys K_j's from the involved participants, the secret image S and the lossless host image O can be reconstructed, where $j = 1, 2, \ldots, t$. We first assume that (g'_{a_j}, g'_{b_j}) is the corresponding pixel pair of O'_j. To extract the (t-1) secret digits and restore the original pixel pair, the authorized participants must derive the polynomial $F(x)$ from t pairs. Thus, the participants obtain the shadows y'_j's by mapping the row g'_{a_j} and the column g'_{b_j} at the same sudoku matrix M, where

$$y'_j = M(g'_{a\_j}, g'_{b\_j}). \quad (7)$$

With t shadows y'_j's and secret keys K_j's, the polynomial $F(x)$ can be reconstructed by Lagrange's interpolation formula:

$$F(x) = (m + s_1 x^1 + s_2 x^2 + \ldots + s_{t-1} x^{t-1}) \bmod 16 . \quad (8)$$

The authorized participants can thereby obtain the secret digits $s_1, s_2, \ldots, s_{t-1}$ by extracting the last (t-1) coefficients of $F(x)$. Meanwhile, they can obtain the feature value m at the first coefficient of $F(x)$. The participants can restore the original pixel pair (g_{a_j}, g_{b_j}) by selecting the row g_{a_j} and the column g_{b_j} which is corresponding to the element value m at the same sudoku block.

Repeating the above processes, authorized participants can restore the host image O losslessly and extract all secret digits. Finally, they can recover the secret image S by transforming all secret digits into binary representation.

IV. Experimental Results and Analysis

We demonstrate the performance of the proposed (t, n)-threshold sharing scheme using different types of images. Fig. 5 shows grayscale test images with 512×512 pixels. Fig. 6 shows the shared secret image. To estimate the quality of the shadow images, the peak signal-to-noise rate (*PSNR*) is used:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\text{dB}. \qquad (9)$$

The mean square error (*MSE*) of an image with $H\times W$ pixels is defined as

$$MSE = \frac{1}{H\times W}\sum_{u=1}^{H}\sum_{v=1}^{W}\left(p_{uv} - p'_{uv}\right)^2 . \qquad (10)$$

where p_{uv} is the original host pixel value and p'_{uv} is the shadow pixel value.

(a) *Airplane* (b)*Cameraman* (c) *Clown*
(d) *Couple* (e) *Elaine* (f) *Goldhill*
(g) *House* (h) *Lena* (i) *Mandrill*
(j) *Peppers* (k) *Sailboat* (l) *Splash*
(m) *Tiffany* (n) *Toys* (o) *Zelda*

Figure 5. Test image

Figure 6. Secret image

To evaluate the performance of the proposed image sharing with steganography approach, the capacity of the secret image and the quality of the shadow images are the main consideration. Table 1 lists the qualities of the shadow images with various test images. This experiment is implemented in the case of the (2, n) -threshold system. Each of the host pair can be embedded one secret digit (i.e. 4 bits). Hence, the embeddable secret capacity equals to $4\times(t\text{-}1)\times((H\times W)/2) = 4\times1\times((512\times512)/2) = 52{,}4288$ bits. The average *PSNR* values of shadow images 1 and 2 are about 44.10 dB and 44.33 dB, respectively.

Table 1. The *PSNR* value (dB) of the shadow images, where t = 2 and secret capacity = 52,4288 bits

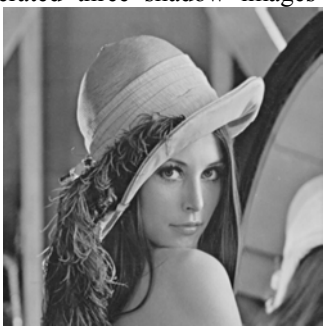
Test images	*PSNR* (dB)	
	shadow image 1	shadow image 2
Airplane	44.04	44.33
Cameraman	44.02	44.36
Clown	44.09	44.56
Couple	44.93	44.27
Elaine	44.00	44.23
Goldhill	44.04	44.28
House	44.09	44.37
Lena	44.03	44.30
Mandrill	44.02	44.26
Peppers	44.03	44.30
Sailboat	44.03	44.29
Splash	44.04	44.31
Tiffany	44.03	44.29
Toys	44.04	44.29
Zelda	44.03	44.47
Average	*44.10*	*44.33*

Table 2. The *PSNR* value (dB) of the shadow images, where t = 3 and secret capacity = 104,8576 bits

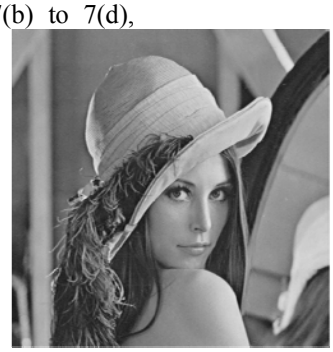
Test images	*PSNR* (dB)		
	shadow image 1	shadow image 2	shadow image 3
Airplane	44.10	44.39	44.13
Cameraman	44.15	44.44	44.15
Clown	44.19	44.54	44.21
Couple	44.08	44.34	44.08
Elaine	44.10	44.30	44.10
Goldhill	44.12	44.34	44.16
House	44.18	44.47	44.17
Lena	44.14	44.36	44.15
Mandrill	44.12	44.31	44.15
Peppers	44.14	44.36	44.15
Sailboat	44.14	44.36	44.15
Splash	44.11	44.40	44.15
Tiffany	44.13	44.34	44.14
Toys	44.11	44.35	44.14
Zelda	44.14	44.52	44.14
Average	*44.13*	*44.39*	*44.14*

Table 2 shows the qualities of the shadow images in the case of the (3, *n*)-threshold system. Averagely, the *PSNR* values of three shadow images are around 44.13 dB, 44.39 dB, and 44.14 dB. The capacity of the secret image is increased to 4×2×((512×512)/2) = 104,8576 bits while t = 3. Due to the new scheme adopts the sudoku block with 16 digits, in which the block size is 4×4 and the distortion for each host pixel is limited within [0, 3]. As the *PSNR* results, we can observe that the quality of the shadow image is satisfactory.

From the visual perception of shadow images, we display the original host image *Lena* in Fig. 7(a) and the generated three shadow images in Figs. 7(b) to 7(d), respectively. Compared the original host image with these three shadow images, the distortion is imperceptible. That is, the new scheme can successfully camouflage shadows from intruders. The authorized participants can later extract the secret image from these three shadow images. The extracted secret image is shown in Fig. 7(e). Note that the revealed secret image is lossless. Fig. 7(f) presents the restored host image without any loss (which is the same as the Fig. 7(a)). Hence, the reversible approach can protect the valuable host image from being distorted.



(a) The original host image, *Lena*



(b) The shadow image 1, PSNR= 44.14 dB

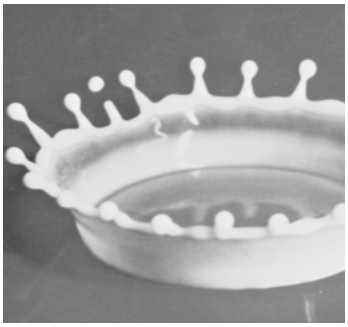
(c) The shadow image 2, PSNR= 44.36 dB

(d) The shadow image 3, PSNR= 44.15 dB

(e) The extracted secret image with 104,8576 bits

(f) The restored lossless host image

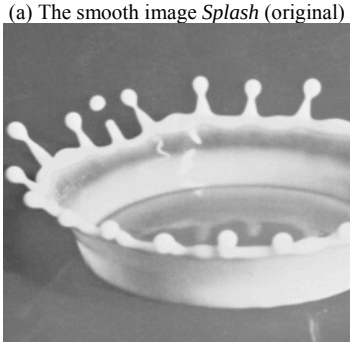
Figure 7. The results of *Lena*



(a) The smooth image *Splash* (original)

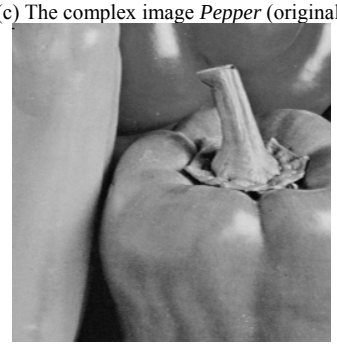
(b) The normal image *Lena* (original)

(c) The complex image *Pepper* (original)



(d) A shadow image from (a)

(e) A shadow image from (c)



(f) A shadow image from (e)

Figure 8. Enlarged partial area of different image types

Fig. 8 enlarges the shadow images in different types of host images to evaluate the visual quality of the shadow images. Figs. 8(a), 8(b), and 8(c) show the enlarged host image with smooth, normal, and complex types, respectively. The corresponding enlarged areas of the shadow images appear in Figs. 8(d), 8(e), and 8(f), respectively. From visual perception, the distortion of these areas is slight and imperceptible compared with the original one. Thus, the new scheme can efficiently camouflage the shadows in a host image and obtain a satisfactory quality of the shadow image.

To consider the underflow and overflow situations of the steganography approach, the proposed scheme camouflages the shadows into the pixel pair by Equation (6). Due to the camouflaged pixel pair is ranged within the sudoku block, the pixel values are limited in the grayscale boundary. It implies that the new scheme can prevent from underflow and overflow situations after the embedding process is performed.

In the (t, n)-threshold sharing scheme, we embed (t-1) secret digits into each host pair, the capacity of the embedded secret relates to the factor t. Therefore, the maximum capacity of the secret is $4\times(t\text{-}1)\times(H\times W)/2$ bits, which is equal to $(t\text{-}1)\times H\times W/4$ pixels. Note that the capacity of the embedded secret [12, 15, 16] is fixed to $H\times W/4$ pixels. Fig. 9 compares the capacity of the embedded secret for our scheme with those of [12, 15, 16]. For a test image with 512×512 pixels, the maximum shared capacities of the proposed scheme and the previous schemes [12, 15, 16] are 65,536 bytes while t = 2. However, the PSNRs of the schemes [12, 15, 16] are around 39 dB, 40 dB, and 41 dB, respectively. At the same situation, the new scheme can achieve higher PSNR approximately 44 dB. In the case of $t \geq 3$, the secret capacity of the new scheme is proportional to the increase of t. According to Fig. 9, the proposed scheme can share more secret capacity as compared with the related schemes.

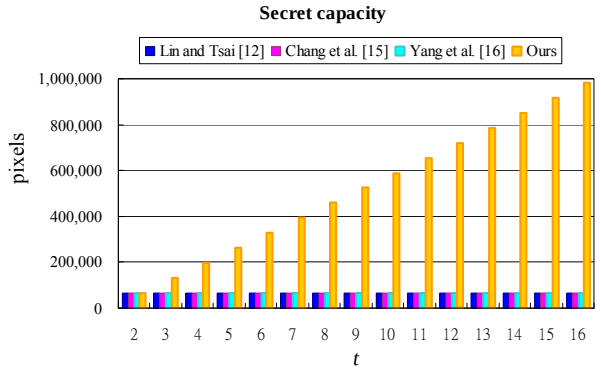


Figure 9. The secret capacity with different t

V. CONCLUSIONS

The revealed secret image inevitably is distorted due to the truncation of the grayscale secret image for common secret image sharing approaches. It is unacceptable for significant secret content even the distortion is slight. In this article, we propose a new secret image sharing scheme that can retrieve the lossless secret image and satisfy the related sharing essentials. Moreover, the proposed reversible scheme offers a large embedding capacity compared with related camouflage sharing schemes. After the secret image is revealed from any t of n shadow images, the authorized participants can restore the original host image from the shadow images. The reversibility of the new sharing scheme is a practical essential to preserve the valuable host images, such as military and medical images.

The participant in the sharing approach, however, may provide a fake shadow image and cheat other participants during the secret revealing procedure. The cheater who collects the genuine shadows thereby can reveal the secret image. Hence, how to detect the cheater during cooperation is an important issue in the sharing scheme. The further research aims to satisfy the requirements of cheating detection and cheater identification. The first allows the participants to detect whether a cheater exists or not during the cooperation. The second allows the involved participants to identify the cheater and locate the tampered areas of the fake shadow image. The secret image sharing scheme with reversibility and cheater defense can provide extensively practical in the really world.

REFERENCES

[1] G. R. Blakley, "Safeguarding cryptographic keys," *Proceedings of AFIPS National Computer Conference*, vol. 48, pp. 313-317, 1979.

[2] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[3] C. C. Chang and R. J. Hwang, "Efficient cheater identification method for threshold schemes," *IEE Proceedings - Computers and Digital Techniques*, vol. 144, no. 1, pp. 23-27, 1997.

[4] A. Beimel and B. Chor, "Secret sharing with public reconstruction," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1887-1896, 1998.

[5] C. C. Chang and R. J. Hwang, "Sharing secret images using shadow codebooks," *Information Sciences*, vol. 111, no. 1, pp. 335-345, 1998.

[6] T. S. Chen and C. C. Chang, "New method of secret image sharing based on vector quantization," *Journal of Electronic Imaging*, vol. 10, no. 4, pp. 988-997, 2001.

[7] J. B. Feng, H. C. Wu, C. S. Tsai and Y. P. Chu, "A new multi-secret images sharing scheme using Lagrange's Interpolation," *The Journal of Systems and Software*, vol. 76, no. 3, pp. 327-339, 2005.

[8] C. C. Chang, C. Y. Lin and C. S. Tseng, "Secret image hiding and sharing based on the (t, n)-threshold," *Fundamenta Informaticae*, vol. 76, no. 4, pp. 399-411, 2007.

[9] C. C. Thien and J. C. Lin, "Secret image sharing," *Computer & Graphics*, vol. 26, no. 1, pp. 765-770, 2002.

[10] R. Z. Wang and S. J. Shyu, "Scalable secret image sharing," *Signal Processing: Image Communication*, vol. 22, no. 4, pp. 363-373, 2007.

[11] C. S. Tsai, C. C. Chang and T. S. Chen, "Sharing multiple secrets in digital images," *The Journal of Systems and Software*, vol. 64, no. 2, pp. 163-170, 2002.
[12] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *The Journal of Systems and Software*, vol. 73, no. 3, pp. 405-414, 2004.
[13] Y. S. Wu, C. C. Thien and J. C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, no. 7, pp. 1377-1385, 2004.
[14] R. Zhao, J. J. Zhao, F. Dai and F. Q. Zhao, "A new image secret sharing scheme to identify cheaters," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 252-257, 2009.
[15] C. C. Chang, Y. P. Hsieh and C. H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130-3137, 2008.
[16] C. N. Yang, T. S. Chen, K. H. Yu and C. C. Wang, "Improvements of image sharing with steganography and authentication," *The Journal of Systems and Software*, vol. 80, no. 7, pp. 1070-1076, 2007.
[17] R. Z. Wang and C. H. Su, "Secret image sharing with smaller shadow images," *Pattern Recognition Letters*, vol. 27, no. 6, pp. 551-555, 2006.
[18] C. C. Chang, C. C. Lin, C. H. Lin and Y. H. Chen, "A novel secret image sharing scheme in color images using small shadow images," *Information Sciences*, vol. 178, no. 11, pp. 2433-2447, 2008.
[19] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003.
[20] C. C. Lin and N. L. Hsueh, "A lossless data hiding scheme based on three-pixel block differences," *Pattern Recognition*, vol. 41, no. 4, pp. 1415-1425, 2008.
[21] C. C. Chang and C. Y. Lin, "Reversible steganography for VQ-compressed images using side matching and relocation," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 4, pp. 493-501, 2006.
[22] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721-730, 2007.
[23] Z. Ni, Y. Q. Shi, N. Ansair, W. Su, Q. Sun and X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, no.4, pp. 497-509, 2008.
[24] *Mathematics of Sudoku*, Available at, http://en.wikipedia.org/wiki/Mathematics_of_Sudoku.
[25] B. Felgenhauer and F. Jarvis, "Mathematics of sudoku I," *Mathematical Spectrum*, vol. 39, no. 1, pp.15-22, 2006.
[26] E. Russell and F. Jarvis, "Mathematics of sudoku II," *Mathematical Spectrum*, vol. 39, no. 2, pp. 54-58, 2007.
[27] C. C. Chang, Y. C. Chou and T. D. Kieu, "An Information Hiding Scheme Using Sudoku," *Proceedings of the Third International Conference on Innovative Computing, Information and Control (ICICIC2008)*, pp. 17-1--17-5, Dalian, China, 2008.

Chin-Chen Chang received the B.S. degree in Applied Mathematics in 1977 and the M.S. degree in Computer and Decision Sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received the Ph.D. degree in Computer Engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years 1980–1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983 to 1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From 1989 to 2004, he was a Professor in the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. Since 2005, he has been a Professor in the Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan. His research interests include computer cryptography, data engineering, and image compression

Pei-Yu Lin received the M.S. and Ph.D. degrees in Computer Science and Information Engineering from National Chung Cheng University, Chiayi, Taiwan, in 2004 and 2009, respectively. Since 2009, she has been an Assistant Professor in the Department of Information Communication at Yuan Ze University, Chung-Li, Taiwan. Her current research interests include digital watermarking, image protection, data mining, and information security.

Zhi-Hui Wang received the BS degree in software engineering in 2004 from the North Eastern University, Shenyang, China, and the MS degree in software engineering in 2007 from the Dalian University of Technology, Dalian, China. She is currently pursuing her PhD degree in computer software and theory from the Dalian University of Technology, Dalian, China. Her research interests include data hiding, and image processing.

Ming-Chu Li received a Ph.D. degree from the University of Toronto (Toronto, Canada) in 1998. During 1997-2002, he worked as a system software Engineer in north america, where he helped in the design and implementation of algorithms and the structures of projects. In 2002, he was a Full Professor of Computer Science at Tianjin University (Tianjin, China). In 1993, he was a Full Associate Professor at the University of Science and Technology Beijing (Beijing, China). Prof. Li is currently a Full Professor of Computer Science at DaLian University of Technology (DLUT) (Dalian, China), where he has been since September 2004. He is also Vice Dean of School of Software of DLUT. His research interests include Hamiltonian Graph Theory, NP-Theory and Algorithms, Network and Information Security, Reputation Systems,and Grid computing and its applications. Prof. Li received several projects by National Nature Science Foundation of China, High-technology 863 plan of China and 973 plan of China since 2002, and have published more than 80 papers in journals and international academic conferences. He is the chair of 2007 International workshop on Graph Theory, Algorithm and its Applications, and 2008 workshop among Asia Information security labs.