Multimed Tools Appl (2017) 76:1–11
DOI 10.1007/s11042-015-3011-9

Selective scalable secret image sharing with verification

Jung-San Lee[1] · You-Ren Chen[1]

Received: 30 November 2014 / Revised: 26 August 2015 / Accepted: 19 October 2015 /
Published online: 24 October 2015

Abstract Scalable secret image sharing (SSIS) is a new secret image sharing technique. The feature of scalability refers to the fact that the revealed secret information is proportional to the number of gathered shadows. Once all of the valid shadows are collected, the complete secret can be revealed easily. The kernel of secret information, however, may be leaked out with a few shadows collected in the existing SSIS mechanisms. This is because researchers seldom concerned about secret distribution. Thus, we introduce the Salient map to develop a new method, in which the ROIs (region of interesting) of secret image can be revealed progressively. Additionally, we introduce the concepts of meaningful shadow and verification to SSIS. To the best of our knowledge, this is the first SSIS that employs a meaningful shadow. The leading adoption can greatly help reduce the attention of attackers in order to enhance the security, while the second concept can avoid malicious behaviors from outside attackers or dishonest members.

Keywords Scalable secret image sharing · Salient map · Meaningful shadow · Verification · ROI

1 Introduction

In conventional cryptosystems, it is common to employ a single node to protect the secret data in an insecure network due to the advantage of easy supervision. The performance of the single node, however, is always the bottleneck of the whole security system. In 1979, Shamir first proposed the concept of (t,n) threshold secret sharing to mitigate this problem [9]. Given a set of n participants, a dealer issues each of them an individual shadow constructed from the secret data S. That is, the responsibility for protecting the secret data is distributed to a set of authorized members. Later, any t members can cooperate to reveal S by providing their secret shadows. More precisely, involved participants who possess fewer than t shadows have no

✉ Jung-San Lee
leejs@fcu.edu.tw

[1] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724 Taiwan, Republic of China

more knowledge of the secret than the one with nothing. This can effectively enhance the security of secret information in an insecure network.

Thien and Lin later extended this concept to protect confidential images [10]. Due to its practicability, the secret image sharing version has been widely applied to the e-commerce, communications, and medical fields. In Thien and Lin's (t, n) threshold method, a dealer has to generate n distinct shadows from a secret image and issue them to authorized participants. Hereafter, any t participants can cooperate to reveal the secret image. Based on this method, Zhao et al. introduced the concept of cheater identification into the secret image sharing mechanism [2, 4–6, 14]. Their method allows authorized members to confirm the validity of the shadows. If a dishonest participant provides a fake shadow for this cooperation, legal users can become aware of this attempt. Nevertheless, neither [10] nor [6] can provide a meaningful shadow image. Delivering meaningless shadow images over an insecure channel may attract attackers' attention to the secret information.

Lin and Tsai offered a version, in which each shadow is meaningful [7]. The meaningfulness of the shadow can decrease the potential risk. In 2007, Wang and Shyu created the scalable secret image sharing (SSIS) mechanism for sharing a secret image to a group of participants [12]. The feature of scalability refers to the fact that the revealed secret information is proportional to the number of collected shadows. That is, the secret is disclosed gradually. Yang and Huang extended SSIS to a t-out-of-n version in 2010 [11, 13, 15, 17], where a qualified group of participants includes t participants and $2 \leq t \leq n$. Inheriting the properties from previous SSIS schemes, Yang and Chu provided a new SSIS mechanism [16], in which the essential of smooth scalability must be confirmed. Specifically, the secret information can be exposed smoothly proportional to the number of gathered shadows.

So far, SSIS schemes cannot offer involved participants meaningful shadows to enhance security. In particular, the revealed parts of the secret are randomly distributed. This may violate the principle of scalable secret sharing: the more shadows we collect, the more secrets we get. That is to say, the key secret may be disclosed even by stacking two shadows. Without loss of generality, the most important information of an image shall be revealed at the final stage. Inspired by this, we aim to design a brand-new SSIS scheme based on the Saliency map and Aryabhata remainder theorem (ART), in which the ROIs of secret image can be revealed selectively [3, 8]. That means the main secret can only be exhibited when all shadows are gathered. Aside from preserving the property of smooth scalability, the new scheme can further provide meaningful shadows for each participant in order to reduce the attention of malicious intruders and allow legal users to verify if the gathered shadow is tampered [1].

The rest of this article is organized as follows. We introduce ART and Shamir's secret sharing technique in Section 2. The proposed new mechanism is described in Section 3, followed by experimental results in Section 4. We finally make conclusions in Section 5.

2 Related work

2.1 Shamir's secret sharing

The (t, n) threshold mechanism was firstly proposed by Shamir [9] in 1979. A dealer has to construct n shadows $(S_1, S_2, \ldots, S_n)$ from the secret data S. Without t or more shadows, no one can restore the secret data S. To divide S into n shadows, the dealer chooses a prime m and generates a $(t-1)$-degree polynomial

$$F(x) = \left(a_o + a_1 x + \ldots + a_{t-1} x^{t-1}\right) \bmod m,$$

where a_0=S and coefficients $a_1,a_2,\ldots,a_{t-1}$ are randomly decided from the integers within [0, $m-1$]. The dealer then computes

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

Finally, the dealer sends secret shadows y_i's to involved participants.

Given any t pairs of $\{(i,y_i)\}_{i=1}^{n}$, involved participants can reconstruct $F(x)$ by the Lagrange interpolation polynomial [13]. Hence, they can recover all coefficients $a_0,a_1,\ldots,a_{t-1}$ of $F(x)$ to learn the secret data S.

2.2 Aryabhata remainder theorem (ART)

Let m_1 and m_2 be two coprime moduli and M=m_1m_2. The congruence system,

$$\begin{aligned} x &\equiv b_1 (\text{mod } m_1), \\ x &\equiv b_2 (\text{mod } m_2), \end{aligned}$$

has a unique solution under modulus M, and the solution can be given by

$$\begin{aligned} x &= \mathcal{ART}(b_1, b_2; m_1, m_2; M) \\ &= \mathcal{ART}(0, c; m_1, m_2; M) + b_1 \\ &= m_1\left(\left(c \cdot m_1^{-1}\right) \text{mod } m_2\right) + b_1, \end{aligned} \tag{1}$$

where c=(b_2-b_1)mod m_2.

Example Find x such that $x\equiv 2$ (mod 3), $x\equiv 3$ (mod 5), and $x\equiv 2$(mod 7).

Solution x can be obtained by the ART twice:

Step 1: Solve $x_1 = \mathcal{ART}(2,\ 3;\ 3,\ 5;\ 15)$

$$\begin{aligned} x_1 &= \mathcal{ART}(2,\ 3;\ 3,\ 5;\ 15) \\ &= \mathcal{ART}(0,\ 1;\ 3,\ 5;\ 15) + 2 \\ &= 3 \cdot \left(\left(1 \cdot 3^{-1}\right)\ \text{mod } 5\right) + 2 \\ &= 3 \cdot 2 + 2 = 8 \end{aligned}$$

Step 2: Compute

$$\begin{aligned} x &= \mathcal{ART}(x_1, 2; 15, 7; 105) \\ &= \mathcal{ART}(8, 2; 15, 7; 105) \\ &= \mathcal{ART}(0, 1; 15, 7; 105) + 8 \\ &= 15 \cdot \left(\left(1 \cdot 15^{-1}\right) \text{mod } 7\right) + 8 \\ &= 15 \cdot 1 + 8 = 23 \end{aligned}$$

Utilizing the iterative method as the solution procedure mentioned above, it is easy to extend ART to the case of t moduli. Here, we omit the algorithm for the t moduli case and the proof of ART; for details, refer to [8].

3 The proposed method

The proposed (t, n)-SSIS scheme can be divided into two phases: sharing and decrypting. Notations used are listed below.
Notations:

I	The selected secret image with size $\|I\|$.
$P(.)$	The partition function, which is used to divide the secret image into n equal sub-images according to Saliency map [3].
$E_{t,n}(.)$	Encoding function of a polynomial-based (t, n)-SIS scheme [17].
$D_{t,n}(.)$	Decoding function used to reverse $E_{t,n}(.)$ processing [17].
I_j	The jth sub-image with size $I_j=\|I\|/n$, where $j\in(1,n)$.
$\overline{I_j}$	The outcome of stacking j shadows, where $k\leq j\leq n$.
$\overline{I^i_j}$	The ith sub-shadow of jth sub-image, where $i\in[1,n]$ and $j\in[k,n]$.
O_j	The jth occupancy map with size $2n\times 2n$ bits, where $j\in[1,n]$.
$\overline{O^i_j}$	The ith sub-shadow of jth occupancy map, where $i\in[1,n]$ and $j\in[k,n]$.
SP^{ij}_s	The shared pixel in the position (i,j) of the sth cover image, where $s\in[1,n]$.
B^{ij}_s	The four-pixel block with position (i,j) within the sth cover image, where $s\in[1,n]$.
$\overline{B^{ij}_s}$	The four-pixel block with position (i,j) in the sth stego image, where $s\in[1,n]$.
$\overline{X^{ij}_s}, \overline{V^{ij}_s}, \overline{W^{ij}_s}, \overline{Z^{ij}_s}$	The four pixel values in the block with position (i,j) in the sth stego image, where $s\in[1,n]$.
PC_{ij}	The pixel collection of the t pixels in the secret image with the position (i,j).

3.1 The sharing phase

The flowchart of this phase is illustrated in Fig. 1. The Saliency map of secret image I is first retrieved according to [3], and I is partitioned into $2n\times 2n$ grids. Afterward, the saliency map, i.e., the ROIs, is used to guide the selection of grids to generate both the sub-images and occupancy maps. Then, t sub-shadows are derived from each of the sub-images using the (t, n) polynomial-based SIS scheme. By combining these sub-shadows, the remaining (n-t) shadows are obtained. Finally, we embed the shadows into the selected cover image and insert the authentication watermark to protect the integrity of the stego images.

Step 1. The secret image is partitioned into $(n-t+1)$ sub-images and counterparts of occupancy maps by $P(.)$ [3]. The size of one sub-image is $(t\times|I|)/n$, in which the number of selected grids is $t\times 2n\times 2n/n$, and other $n-t$ sub-images are sized of $(|I|)/n$ with $2n\times 2n/n$ grids. The location of selected grids is recorded as the occupancy map.

Step 2. As the modulus used in the polynomial $E_{t,n}(.)$ is set to GF(2^8), such that the 8-bit pixel can be encrypted lossless and without additional pixels. Every t pixels of the sub-images and occupancy maps can form a pixel collection. Furthermore, PC_{ij} can be applied to generate n shared pixels $SP^{ij}_1, SP^{ij}_2, \ldots, SP^{ij}_n$ to be embedded into the blocks $B^{ij}_1, B^{ij}_2, \ldots, B^{ij}_n$, respectively, within the n cover images. The PC_{ij} is hidden in the coefficients $a_0, a_1, \ldots, a_{t-1}$ in the polynomial function. Input the decimal value of the five MSBs of the pixel into the polynomial function to generate the shared pixel SP^{ij}_s. Consequently, we employ the function $E_{t,n}(.)$ to encrypt the occupancy map

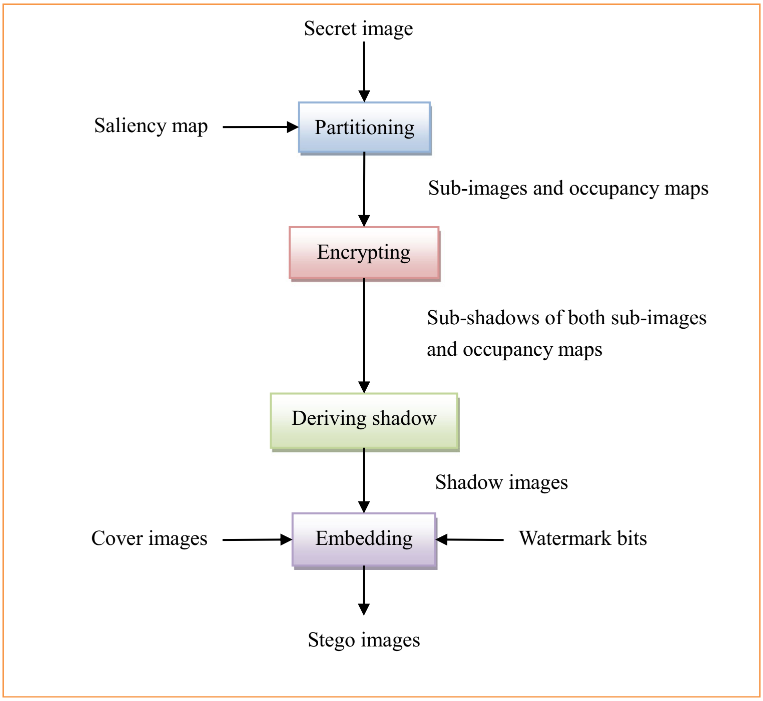


Fig. 1 The flowchart of sharing phase

with the size of $2n\times 2n$ to generate sub-shadows of occupancy maps $O_1^1, O_2^1, \ldots, O_n^1$ and the sub-image with the size of $(t\times|I|)/n$ to generate sub-shadows of sub-images $I_1^1, I_2^1, \ldots, I_n^1$. Similarly, we encrypt other occupancy maps and sub-images by $E_{t+1,n}(.)$, $E_{t+2,n}(.), \ldots,$ $E_{n,n}(.)$, respectively.

Step 3. We then combine the sub-shadows progressively to generate the shadows $S_1, S_2, \ldots, S_n$.

Step 4. The binary bits of the shared pixel $SP_s^{ij}(s_1, s_2, \ldots s_8)$ is embedded into the block by replacing the eight bits $x_6x_7v_6v_7w_6w_7z_6z_7$.

Step 5. To prevent malicious faking, we employ the ART-based authentication method to protect the integrity of the stego images. First, we retrieve the former seven bits of the four pixels within $\overline{B_s^{ij}}$ to form four new values as $A_{ij1}^s, A_{ij2}^s, A_{ij3}^s, A_{ij4}^s$. Let $A_{ij5}^s = i$, $A_{ij6}^s = j$. Next, the six moduli that are relatively primes $m_{ij1}^S, m_{ij2}^S, \ldots, m_{ij6}^S$ are determined, where each modulus is the prime number greater than A_{ija}^s and $1 \le a \le 6$. Finally, the integer Y_{ij}^s is computed by Eq. (1). The binary bits of Y_{ij}^s is shown as $(y_1y_2 \ldots y_e)$. Note that the number of these binary bits has to be a multiple of four. Then, the four authentication bits can be obtained as follows:

$$\begin{aligned}(c_1c_2c_3c_4) = {} & (y_1y_2y_3y_4)\oplus(y_5y_6y_7y_8)\\ & \oplus\cdots\oplus(y_{e-3}y_{e-2}y_{e-1}y_e)\end{aligned} \tag{2}$$

If the four watermark bits are t_1, t_2, t_3, t_4, the four check bits p_1, p_2, p_3, p_4 can be calculated as

$$(p_1p_2p_3p_4) = (c_1c_2c_3c_4)\oplus(t_1t_2t_3t_4) \tag{3}$$

Then, we replace the four LSBs $x_8v_8w_8z_8$ with the checked bits p_1,p_2,p_3,p_4. Here we have

$$X_s^{ij} = \ x_1x_2x_3x_4x_5s_1s_2p_1, \quad \overline{V_s^{ij}} = v_1v_2v_3v_4v_5s_3s_4p_2,$$
$$\overline{W_s^{ij}} = w_1w_2w_3w_4w_5s_5s_6p_3, \quad \overline{Z_s^{ij}} = z_1z_2z_3z_4z_5s_7s_8p_4.$$

Step 6. Repeat the sharing procedure until all pixels of the modified secret image have been processed. Next, the stego images are acquired and transmitted to the legal participants.

3.2 Decrypting phase

To ensure that the secret image can be reconstructed correctly, the stego images should be authenticated first. If the combined stego images are completed, then the secret image can be retrieved progressively by the (t, n)-based SSIS decryption method.

Step1. Each of the stego images is divided into a set of blocks with four pixels. We retrieve the former seven bits of the four pixels within $\overline{B_s^{ij}}$ to form four new values as $\overline{A_{ij1}^s}, \overline{A_{ij2}^s}, \overline{A_{ij3}^s}, \overline{A_{ij4}^s}$. Then, we set $\overline{A_{ij5}^s} = i$, $\overline{A_{ij6}^s} = j$ and employ Eq. (2) to gain the authentication bits. We apply the watermark bits together with the authentication bits to compute the check bits $\overline{p_1}, \overline{p_2}, \overline{p_3}, \overline{p_4}$. If the acquired check bits are identical to the hidden bits p_1,p_2,p_3,p_4, this block is verified successfully, and a shared pixel (s_1,s_2, …,s_8) is achieved. This authentication and revealing procedure is repeated progressively until the hidden shared pixels of the proposed stego images are gained.

Step2. We subsequently use the function $D_{t,n}$(.) to decrypt the t shadows S_1,S_2,…,S_t and obtain the progressive outcome $\overline{I_j}$.

Step3. We apply the function $E_{t+1,n}$(.) to decrypt the $\overline{I_j}$ and S_{t+1} based on the polynomial interpolation to obtain $\overline{I_{j+1}}$.

Step4. We repeat the above decryption process for all stego images to guarantee the integrity of the shadows and to reconstruct the secret image progressively and completely.

4 Experimental result and comparisons

We employed the Python to conduct all simulations using Intel 1.3GHz CPU. We first adopted the (3, 5)-polynomial based SSIS scheme as an example to demonstrate the secret sharing process of the proposed method. The generated five meaningful shadows are depicted as Fig. 2a through e. The stacking result of Fig. 2a through c is displayed as Fig. 2f, and the outcome of Fig. 2a through d is shown as Fig. 2g. The final effect of stacking all shadows is shown as Fig. 2h. According to human visual perception, the quality of these shadows is satisfactory. Thus, it is difficult for an intruder to be aware of any secret hidden in the images.

As for Fig. 2f through h, it is clear that the kernel of the secret can unfold progressively. This can prevent the selected important region of the secret from being exhibited unless all shadows are collected. In particular, the revealed secret is proportional to the number of collected shadows, which complies with the concept of scalability.

On the other hand, the stacking effects of [16, 17] are shown in Fig. 3. The first row displays the result of Yang and Huang's (3, 5)-polynomial based SSIS scheme. Figure 3a displays the

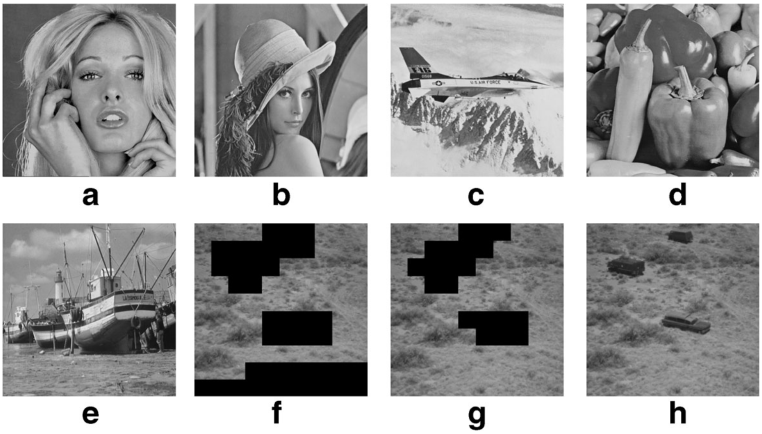


Fig. 2 **a**–**e** shadows, **f** outcome of three shadows, **g** outcome of four shadows; **h** outcome of five shadows

outcome of combing three meaningless shadows; Fig. 3b illustrates the result of four shadows; and Fig. 3c reveals a complete secret. It is clear that the stacking result can not comply with the essential of smooth scalability. The second row of Fig. 3 offers the result of Yang and Chu's (3, 5)-polynomial based SSIS scheme. Figure 3d displays the effect of stacking three meaningless shadows; Fig. 3e shows the result of four shadows; and Fig. 3f reveals a final secret. Although the revealed secret information is also proportional to the number of collected shadows, people can easily figure out the main content of secret by stacking four shadows. In fact, this has violated the principle of scalable secret image sharing. Recalling to the results of Fig. 2f, g, and h, the main secrets are recovered only under the situation that all the shadows are gathered. It is due to the help of Salient object detection technique. Without loss of generality, the detected ROIs are the representative features of a secret image. The more number of gathered shadows, the more ROIs can be revealed in the new method.

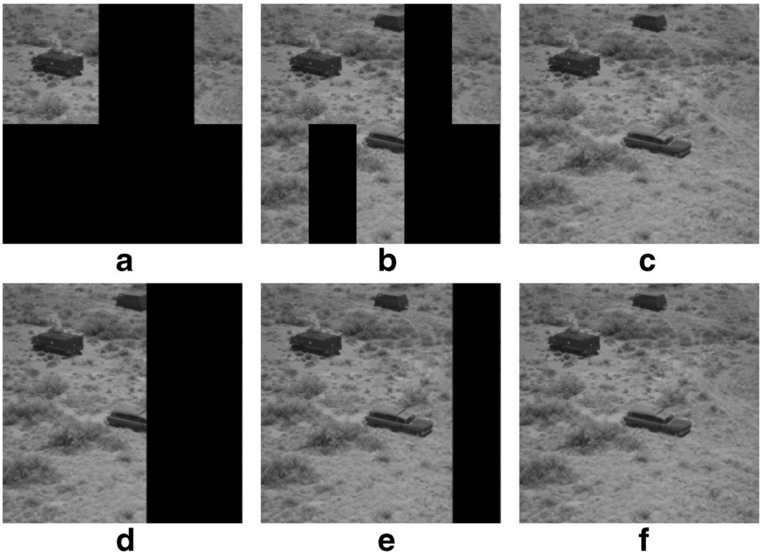
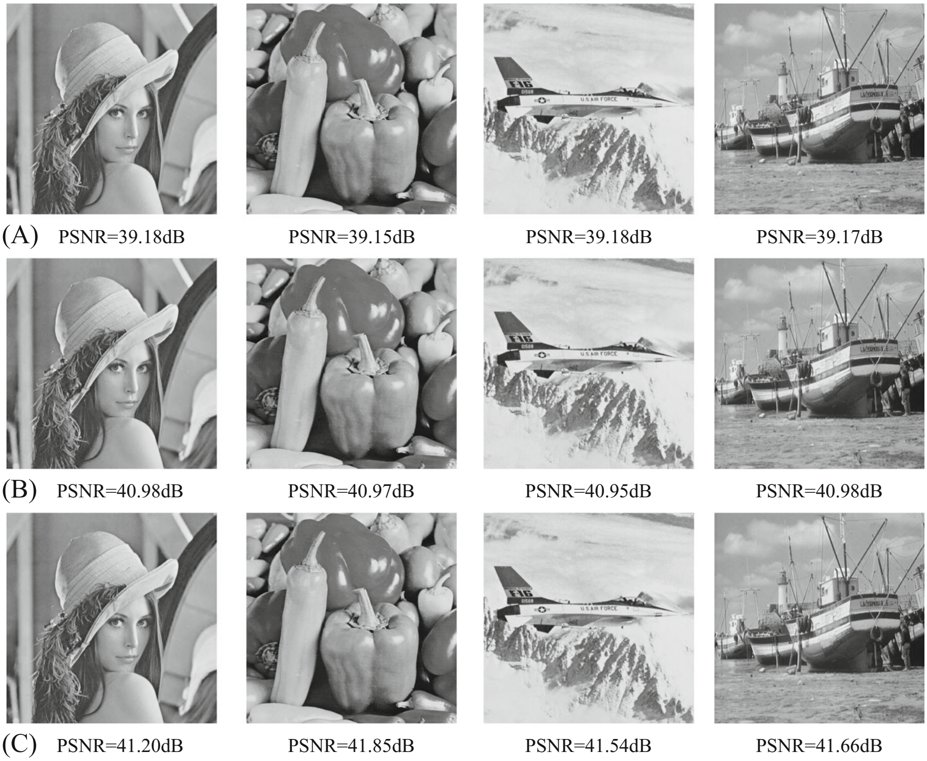


Fig. 3 Stacking results of [17] and [16]

To highlight the ability to mitigate the potential risk of attackers' consciousness, we conducted simulations of related state-of-the-art works [7, 15], which are (2, 4) scalable secret image sharing methods. These two methods are known for the excellent quality of the generated meaningful shadows. The result comparisons are shown in Fig. 4. The reason that we adopted the (2, 4) version is that it can offer the best performance of these two mechanisms. Undoubtedly, the quality of the meaningful shadows of the two related works and of the proposed mechanism is satisfactory according to human visual perception. Nevertheless, higher PSNR values are obtained from the proposed mechanism.

Verification of shadows is seldom concerned in the scalable secret image sharing schemes. With the explosive increase of network crimes, no one can guarantee that shadows will not be modified by outside attackers or dishonest participants. Thus, verifying the validity of shadows shall become an essential in designing a secret image sharing mechanism. With the adoption of ART, we can employ the watermark and authentication code to compute a check code in order to verify the integrity of the shadow. The verification evaluation is shown in Fig. 5. The left column contains three meaningful shadows, in which a small pumpkin is embedded in the corner. The verification results are listed in the right column. Obviously, the modified area can be marked out with a pumpkin shape.

To examine the verification ability of the proposed method in terms of digitalization, we employ the Verifying ratio of Shadow (*VoS*) in the tampered region to show its robustness. The *VoS* is defined as $VoS = \frac{NPV}{NPT}$, where *NPV* represents the number of pixels verified as



(A) PSNR=39.18dB PSNR=39.15dB PSNR=39.18dB PSNR=39.17dB

(B) PSNR=40.98dB PSNR=40.97dB PSNR=40.95dB PSNR=40.98dB

(C) PSNR=41.20dB PSNR=41.85dB PSNR=41.54dB PSNR=41.66dB

Fig. 4 Shadow evaluation for the (2, 4) secret image sharing schemes: **a** the shadows of [15]; **b** the shadows of [7]; **c** the shadows of the proposed scheme

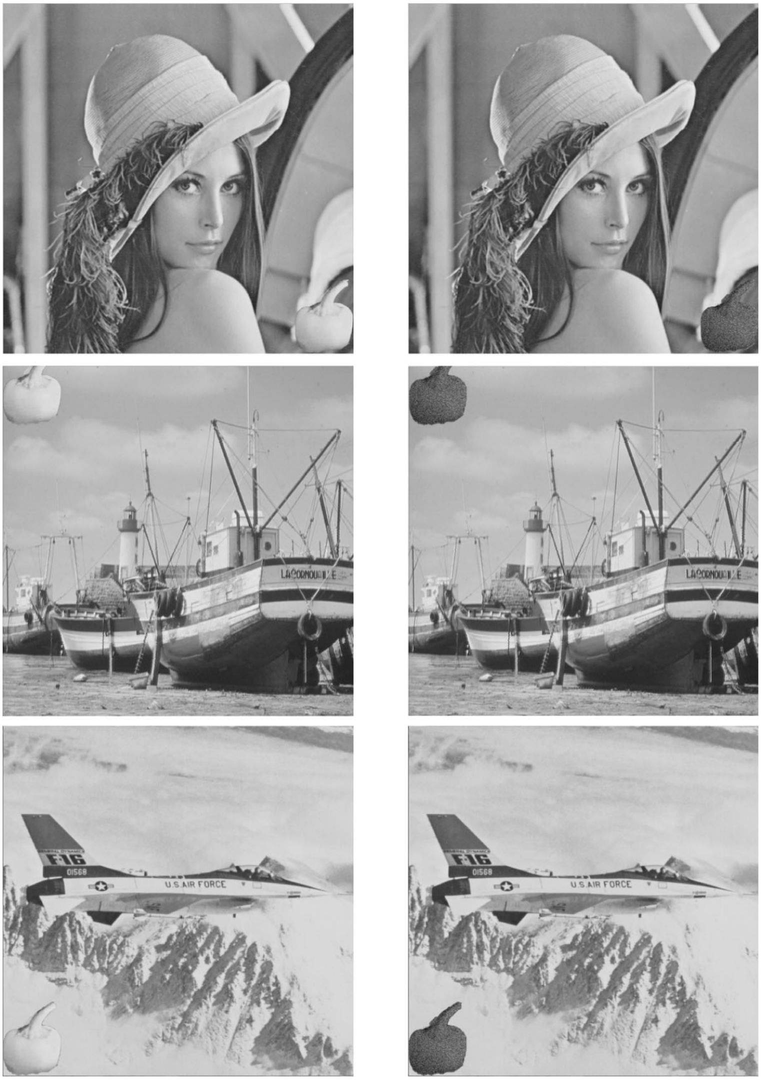


Fig. 5 Verification outcomes of the meaningful shadows

tampered, and *NPT* stands for the number of all tampered pixels. The results of the verification for different shadows are shown in the Table 1. Almost all modified pixels can be determined.

To emphasize the contribution of the proposed mechanism, we summarize the essentials of related schemes in Table 2. Aside from complying with scalability and smooth scalability, the

Table 1 VoS of the meaningful shadows

Image	VoS
Lena	0.98
Jet-F16	0.95
Steamship	0.98

Table 2 The functionality of related and proposed scheme

	[17]	[16]	Ours
Scalability	Yes	Yes	Yes
Smooth scalability	Yes	Yes	Yes
Meaningful shadow	No	No	Yes
Pixel expansion	No	No	No
Verification	No	No	Yes

new method can offer meaningful shadows without pixel expansion to reduce attention from malicious attackers. To the best of our knowledge, it is the first SSIS scheme with meaningful shadows. Furthermore, it is equipped with verification ability to enhance the robustness of shadows. This achievement can greatly help to avoid dishonest behavior in retrieving a secret. To underline the quality of meaningful shadows, we compare the result of related secret sharing schemes offering meaningful shadows with that of the proposed scheme. According to Fig. 4, we can conclude that the new method can provide better shadow quality than related works in terms of PSNR values and visual perception.

5 Conclusions

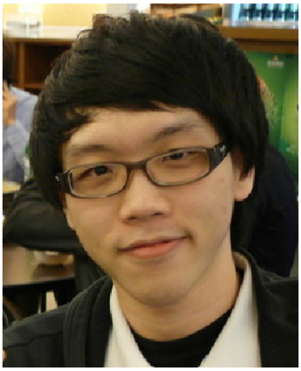
The innovation of this article can be highlighted in the following. 1) It is the first SSIS method providing meaningful shadow, which can effectively help to reduce attention from attackers. The quality of shadows is proven to be better than secret image sharing schemes according to the simulations. 2) It is the first SSIS method offering shadow verification, in which a dishonest or invalid shadow can be detected before stacking. 3) It is the first SSIS method concerning about the secret distribution of an image, in which the ROIs can be revealed gradually.

References

1. Chang CC, Hsieh YP, Lin CH (2008) Sharing secrets in stego images with authentication. Pattern Recogn 41(10):3130–3137
2. Hou YC, Wei SC, Lin CY (2014) Random-grid-based visual cryptography schemes. IEEE Trans Circuits Syst Video Technol 24:733–744
3. Jiang H, Wang J, Yuan Z, Wu Y, Zheng N, Li S (2013) Salient object detection: A discriminative regional feature integration approach. 2013 I.E. Conference on Computer Vision and Pattern Recognition (CVPR), pp. 2083–2090
4. Lin PY, Chan CS (2010) Invertible secret image sharing with steganography. Pattern Recogn Lett 31(13): 1887–1893
5. Lin PY, Chang CC (2011) Cheating resistance and reversibility oriented secret sharing mechanism. IET Inf Secur 5(2):81–92
6. Lin KS, Lin CH, Chen TH (2014) Distortionless visual multi-secret sharing based on random grid. Inf Sci 288:330–346
7. Lin CC, Tsai WH (2004) Secret image sharing with steganography and authentication. J Syst Softw 73(3): 405–414
8. Rao TRN, Yang CH (2006) Aryabhata remainder theorem: relevance to public-key crypto-algorithms. Circuits Syst Signal Process 25(1):1–15
9. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
10. Thien CC, Lin JC (2002) Secret image sharing. Comp Graph 26:765–770
11. Wang RZ, Chien YF, Lin YY (2010) Scalable user-friendly image sharing. J Vis Commun Image Represent 21(7):751–761

12. Wang RZ, Shyu SJ (2007) Scalable secret image sharing. Signal Process Image Commun 22(4):363–373
13. Wang RZ, Su CH (2006) Secret image sharing with smaller shadows. Pattern Recogn Lett 27:551–555
14. Wu X, Sun W (2013) Random grid-based visual secret sharing with abilities of OR and XOR decryptions. J Vis Commun Image Represent 24:48–62
15. Yang CN, Chen TS, Yu KH, Wang CC (2007) Improvements of image sharing with steganography and authentication. J Syst Softw 80(7):1070–1076
16. Yang CN, Chu YY (2011) A general (k, n) scalable secret image sharing scheme with the smooth scalability. J Syst Softw 84(10):1726–1733
17. Yang CN, Huang SM (2010) Constructions and properties of k out of n scalable secret image sharing. Opt Commun 283:1750–1762

Jung-San Lee received the BS degree in computer science and information engineering in 2002 and his Ph.D in computer science and information engineering in 2008, both from National Chung Cheng University, Chiayi, Taiwan. Since 2012, he has worked as an associate professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His current research interests include image processing, information security, watermarking, and mobile communications.



You-Ren Chen received his MS degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan in 2015. His current research interests include information security and watermarking.