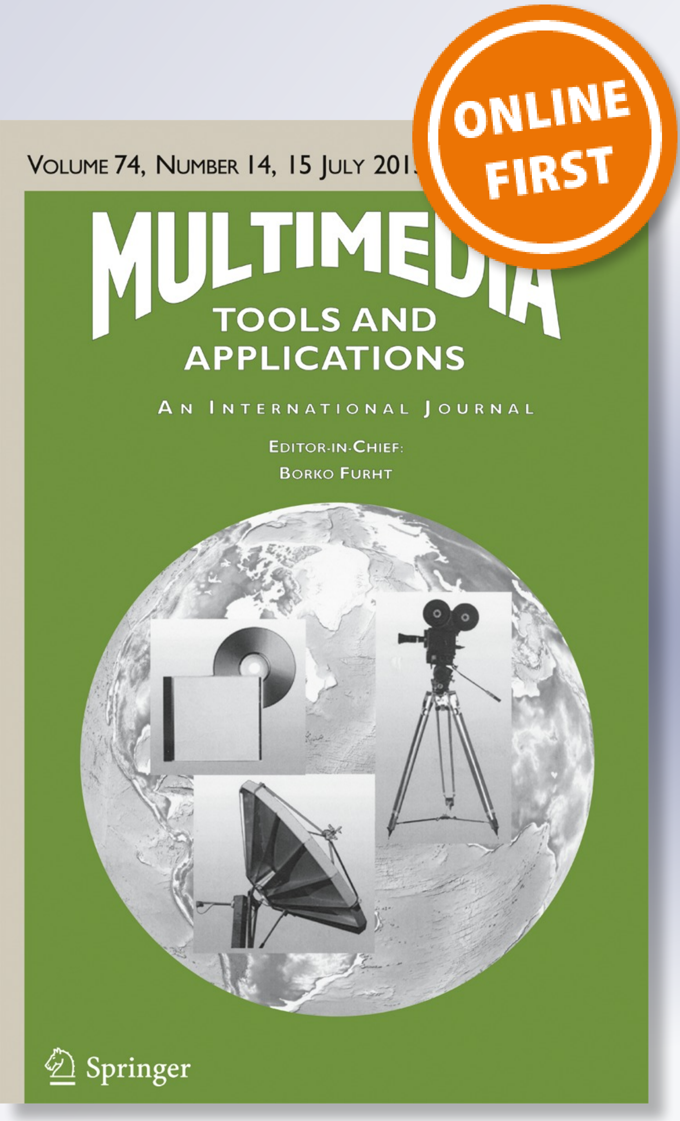
Secret image sharing with smaller shadow sizes for general access structures

Ying-Ru Chen, Ling-Hwei Chen & Shyong Jian Shyu

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501

Multimed Tools Appl
DOI 10.1007/s11042-015-2734-y



Springer

Multimed Tools Appl
DOI 10.1007/s11042-015-2734-y

Secret image sharing with smaller shadow sizes for general access structures

Ying-Ru Chen[1] · Ling-Hwei Chen[2] · Shyong Jian Shyu[3]

Received: 12 September 2014 / Revised: 1 May 2015 / Accepted: 4 June 2015

Abstract In the area of secret image sharing (SIS), most papers focused on the schemes for threshold or some special access structures. Regarding general access structures (GAS), few results have been found in the literature. Two SIS schemes for GAS were proposed in 2001 and 2010, both are based on qualified sets. However, one distorts the reconstructed secret image, and some extra information is needed in both schemes. Here, we propose three polynomial based SIS schemes for GAS. Considering either qualified or forbidden sets, these schemes can reconstruct the secret image perfectly without any extra information needed. Some proof and analysis on the shadow sizes of the three schemes are given to lead us to choose the one with the smallest size. In addition, we also give some comparisons with two existing schemes, and security issue is also addressed in conclusion.

Keywords Shadow size · Secret image sharing · General access structure

✉ Ling-Hwei Chen
lhchen@cc.nctu.edu.tw

Ying-Ru Chen
cyrchen@gmail.com

Shyong Jian Shyu
sjshyu@mail.mcu.edu.tw

[1] Institute of Computer Science and Engineering, National Chiao Tung University,
1001 Ta Hsueh Rd., Hsinchu, Taiwan 300, Republic of China

[2] Department of Computer Science, National Chiao Tung University,
1001 Ta Hsueh Rd., Hsinchu, Taiwan 300, Republic of China

[3] Department of Computer Science and Information Engineering, Ming Chuan University,
5 De Ming Rd., Gui Shan, Taoyuan 333 Taiwan, Republic of China

Published online: 09 July 2015

1 Introduction

Secret sharing (SS) safeguards the secret among a group of participants. It reduces the individual disloyal and has the fault tolerance ability. Shamir [11] and Blakley [3] proposed (k, n)-*threshold secret sharing* (TSS) schemes in 1979 independently. A secret s is encoded into n parts called shadows, which would be distributed to n participants, such that each group of k (or more) participants can recover s using their shadows, while any group of less than k ones cannot obtain any information about s. The decoding criterion is based on the number of participants and that is why k is called the threshold. The secret is protected by these n participants such that any disloyal group of less than k participants cannot recover it and a tolerance of $n - k$ damaged shares is allowed.

However, a TSS scheme cannot handle those sharing cases that the decoding does not depend on the number of participants. For instance, we might expect participants 1 and 2 as well as 2 and 3 can access the secret, but 1 and 3 cannot among the three participants. A *general access structure* (GAS), which predefines *qualified sets* and *forbidden sets*, can describe a wider range of participants' accessibility than the threshold one. A scheme with GAS can be applied to more situations in practical applications and a threshold structure is a special case of it.

Ito et al. [7] proposed a SS scheme for GAS in 1987, Benaloh and Leichter [2] proposed another in 1988. These two schemes are simple and will be explained later. The total shadow sizes of these two schemes are depended on the given access structure. Note that the shadow size is the major measurement to evaluate the effectiveness of a SS-GAS scheme. We prefer a scheme with a smaller total shadow size. Some extended researches [6, 8, 13] try to reduce the shadow size. The shadow size in [6] and [13] can be reduced in some special cases only. Horng's scheme [6] is effective when the cardinality of each minimal qualified set is near a constant, but the shadow size in the worst case is larger than that of Ito et al.'s scheme. Tochikubo's scheme [13] tries to merge some forbidden sets to reduce the shadow size; still, the worse case is the same as Ito et al.'s scheme. Iwamoto et al.'s scheme [8] minimizes the shadow size via setting conditions through integer programming. In 2013, Guo and Chang [5] proposed a SS scheme for GAS which is based on key-lock-pair mechanism. The number of shadows each participant holds is twice as many as the number of participants. Note that all the above schemes focus on sharing a secret number.

The study for sharing an image (instead of a number) is called *secret image sharing* (SIS). The demand of an SIS scheme with a smaller share size is even more critical than that of SS since the size of a secret image is much larger than that of a secret number. Thien and Lin [12] developed a (k, n)-SIS scheme in 2002. They modified Shamir's polynomial-based sharing approach straightforward on a gray-scale image with size N. The resultant shadow size is N/k. In 2014, Chang et al. [4] proposed a multi-image sharing scheme based on Chinese remainder theorem and Lagrange interpolation. All secret images have the same size. Each shadow of their scheme is a matrix of the same size as one secret image, but the value of each element in the matrix may be very large. The above-mentioned schemes only cope with the threshold structure.

Few SIS schemes are designed under GAS called SIS-GAS. In 2001, Tsai and Chang [14] presented a SIS-GAS scheme. In Tsai-Chang's scheme, a secret image S is first compressed into a sequence of indices I through vector quantization [10] with a certain selected codebook C. I is encrypted via an encryption-key K and put in public by the dealer. Then, Benaloh-Leich's SS-GAS scheme [2] is applied to codebook C and key K, respectively. The size of C is smaller than that of S, and each component of a codevector in C is regarded as a separate secret number. The size of each produced shadow is thus smaller than that of

S. However, the reconstructed secret image is a lossy version of S. In 2010, Lin et al. [9] proposed a scheme to share multiple secret images for GAS. For each secret image, each qualified set has a corresponding seed. Through this seed, the secret image is encrypted and put in public. And the seed is encoded into several shadows; each participant will own one shadow, such that participants in the qualified set can reconstruct the seed through the owned shadows and use the seed and the encrypted public image to reconstruct the secret image. Note that the encrypted image is put in public in above two schemes. Any storage accident or malicious damage on the encrypted image may destroy the whole sharing system.

The goal of this paper focuses on the design of SIS schemes under GAS such that a secret image can be perfectly (losslessly) reconstructed without any extra public information. In addition, the related researches for SIS-GAS only consider sharing secret for each qualified set in the encoding phase. We propose three SIS-GAS schemes by considering qualified and forbidden sets. The comparisons of their performances in terms of the shadow size are also provided. The rest of this paper is organized as follows. Section 2 surveys related works. Section 3 describes our proposed schemes. Section 4 analyzes the shadow sizes of our methods. Some concluding remarks are made in Section 5.

2 Related work

An SIS schemes devised by Thieh-Lin [12] and an extended SIS scheme based on Shamir [11] are described in Section 2.1, these two schemes are both threshold scheme. Section 2.2 gives the definitions regarding GAS. Then, we briefly introduce two SS schemes for GAS: Ito et al.'s multiple assignment scheme [7] in Section 2.3 and Benaloh and Leich's method [2] in Section 2.4.

2.1 Shamir's (k, n)-SIS scheme and Thieh-Lin's (k, n)-SIS scheme

Shamir's (k, n)-SIS scheme [12] is based on Shamir's (k, n)-TSS scheme [11]. Consider a gray-scale secret image S with size N and n predefined keys $x_1, x_2, \ldots, x_n$ for n participants 1, 2, ..., n. The secret image S is encoded into n shadow images for n participants by the following polynomial function with $k-1$ degrees:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \bmod q, \quad (1)$$

Here, $q = 251$, a_0 is the value of the j-th secret pixel and $a_1, a_2, \ldots, a_{k-1}$ are random numbers. The dealer determines n distinct random keys $x_1, x_2, \ldots, x_n$, constructs n shadows $d_1^j, d_2^j, \ldots, d_n^j$ and distributes (x_i, d_i^j) to participant i.

Thieh-Lin's (k, n)-SIS Scheme is similar to Shamir's (k, n)-SIS Scheme, except that S is permutated into S', and each set of k secret pixels in S' is assigned to the k coefficients in (1).

The dealer constructs the shadow image D_i by collecting all d_i^j and distributes (x_i, D_i) to participant i. The size of D_i is N for Shamir's (k, n)-SIS scheme and $\lceil N/k \rceil$ for Thieh-Lin's (k, n)-SIS Scheme.

2.2 General access structures in secret sharing

Let $P = \{1, 2, \ldots, n\}$ be a finite set of participants for sharing a secret s, and 2^P be the set of all subsets in P. According to [1, 7], some GAS related definition are given as follows:

Definition 1 Let $\Gamma_Q \subseteq 2^P$ and $\Gamma_F \subseteq 2^P$, where $\Gamma_Q \cap \Gamma_F = \emptyset$. The members of Γ_Q are referred as qualified sets and the members of Γ_F are called forbidden sets. $\mathbf{\Gamma} = (\Gamma_Q, \Gamma_F)$ is called a GAS of P.

Given $\mathbf{\Gamma} = (\Gamma_Q, \Gamma_F)$ of P with regard to s, a secret sharing scheme encodes s into shadows and distributes to participants such that all members of each $A \in \Gamma_{\mathrm{Q}}$ together can reconstruct s using their shadows, while those of any $B \in \Gamma_F$ cannot.

Definition 2 For each $A \in \Gamma_Q$ and any $B \in \Gamma_F$, if

$$A' \supseteq A \Rightarrow A' \in \Gamma_Q \; and \; B' \subseteq B \Rightarrow B' \in \Gamma_F,$$

then Γ_Q is monotone increasing and Γ_F is monotone decreasing. Consequently, $\mathbf{\Gamma} = (\Gamma_Q, \Gamma_F)$ is monotone.

Definition 3 If $\mathbf{\Gamma} = (\Gamma_Q, \Gamma_F)$ is monotone and $\Gamma_Q \cup \Gamma_F = 2^P$, then $\mathbf{\Gamma}$ is a $strong$ GAS.

Definition 4 Γ_0 is termed a basis of a strong GAS $\mathbf{\Gamma}$, if Γ_0 consists of all minimal qualified sets in $\mathbf{\Gamma}$. That is,

$$\Gamma_0 = \{A \in \Gamma_Q | B \notin \Gamma_Q for \; all \; B \subset A\}.$$

Definition 5 Z_M is defined as the collection of the maximal forbidden sets in $\mathbf{\Gamma}$. That is,

$$Z_M = \{B \in \Gamma_F \mid B \cup \{i\} \in \Gamma_Q for \; any \; i \in P \setminus B\}.$$

In the remainder parts of this paper, all mentioned GASs are strong GASs for short, and Γ_Q and Γ_F can be derivated by Γ_0 (or Z_M).

2.3 Ito-SS-FGAS scheme

Ito et al. [7] proposed an SS scheme for GAS in 1987, called Ito-SS-FGAS Scheme. Given $P = \{1, 2, \ldots, n\}$, s, and a $\mathbf{\Gamma} = (\Gamma_Q, \Gamma_F)$ with $Z_M = \{B_1, B_2, \ldots, B_m\}$, the encoding phase contains two steps:

1. Construct m pairs of keys and shadows (x_1, d_1), (x_2, d_2), $\ldots$, (x_m, d_m) for s by Shamir's (m, m)-TSS scheme.
2. Distribute each (x_f, d_f) to all participants who are not in B_f for $1 \leq f \leq m$.

In the decoding phase, since each qualified set $A \not\subset B_f$ for each $B_f \in Z_M$, at least a participant in A can receive (x_f, d_f) [7]. Thus, participants in A are able to reconstruct s by Shamir's (m, m)-TSS decoding scheme.

We can extend Ito-SS-FGAS Scheme to share an image. For a gray-scale secret image S, we simply treat each pixel in S as a separate secret and encode it using Ito-SS-FGAS Scheme. This scheme is called Ito-SIS-FGAS Scheme.

2.4 BL-SS-QGAS scheme

Benaloh and Leich [2] proposed an SS scheme for GAS in 1988, called BL-SS-QGAS Scheme. This scheme allows an access structure to be written as a $clause \; formula$

including AND and OR operators. Consider $P = \{1, 2, \ldots, n\}$, s, and a $\mathbf{\Gamma} = (\Gamma_Q, \Gamma_F)$ with $\Gamma_0 = \{A_1, A_2, \ldots, A_h\}$. This scheme translates Γ_0 to the following clause formula

$$\begin{aligned} F = &((i_{1_1} \wedge i_{1_2} \wedge \ldots \wedge i_{1_{m_1}}) \vee ((i_{2_1} \wedge i_{2_2} \wedge \ldots \wedge i_{2_{m_2}}) \\ &\vee \ldots \vee ((i_{h_1} \wedge i_{h_2} \wedge \ldots \wedge i_{h_{m_h}})) \end{aligned}$$

where $(i_{l_1} \wedge i_{l_2} \wedge \ldots \wedge i_{l_{m_l}})$ is clause l and stands for the participation of all members in A_l for $1 \leq l \leq h$, i_{l_u} is the u-th participant in A_l for $1 \leq u \leq m_l (= |A_l|)$ and $\wedge$ ($\vee$) denotes the AND (OR) operator. For instance, $\Gamma_0 = \{1, 2, 3, 4\}$ can be written as ((1$\wedge$ 2) $\vee$ (3 $\wedge$ 4)). The encoding phase contains two steps:

1. For each clause l, s ($\in [0, q - 1]$) is encoded into m_l shadows $s_{l_1}, s_{l_2}, \ldots, s_{l_{m_l}}$ with $s = (s_{l_1} + s_{l_2} + \ldots + s_{l_{m_l}}) \bmod q$.
2. The m_l shadows are distributed to the corresponding m_l participants in clause l for $1 \leq l \leq h$. The index l is attached to each shadow for decoding.

Regarding the decoding phase, the participants in qualified set A_l holding shadows s_{l_1}, $s_{l_2}, \ldots, s_{l_{m_l}}$ with the same index l can reconstruct s by simply computing $s = (s_{l_1} + s_{l_2} + \ldots + s_{l_{m_l}}) \bmod q$ for $1 \leq l \leq h$. This scheme is simple, but the total shadow size becomes large when the sum of $m_1, m_2, \ldots, m_l$ is large.

We can extend BL-SS-QGAS Scheme to share an image. For a gray-scale secret image S, we simply treat each pixel in S as a separate secret and encode it using BL-SS-QGAS Scheme. This scheme is called BL-SIS-QGAS Scheme.

3 Proposed methods

Consider a secret image S with size $H \times W$, a set of n participants $P = \{1, 2, \ldots, n\}$ and a GAS $\mathbf{\Gamma} = (\Gamma_Q, \Gamma_F)$ with $\Gamma_0 = \{A_1, A_2, \ldots, A_h\}$ and $Z_M = \{B_1, B_2, \ldots, B_m\}$. Here, we propose three SIS-GAS schemes in the following three sub-sections. The first one, referred to as Shamir-SIS-QGAS scheme, modifies BL-SIS-QGAS Scheme based on Shamir's (m, m)-SIS scheme. The second, referred to as TL-SIS-QGAS scheme, is based on Thien-Lin's (m, m)-SIS scheme and Γ_0, and the last, called TL-SIS-FGAS scheme, is based on Thien-Lin's (m, m)-SIS scheme and Z_M. The arithmetic operations apply GF(2^8) in these schemes.

3.1 Shamir-SIS-QGAS scheme

The Shamir-SIS-QGAS scheme is designed as follows.

1. Assign a unique key x_i for each participant $i \in P$, $1 \leq x_i \leq 255$.
2. For each minimal qualified set $A_l = \{i_{l_1}, i_{l_2}, \ldots, i_{l_{m_l}}\} \in \Gamma_0$, encode S into m_l shadow images $D_{l_1}, D_{l_2}, \ldots, D_{l_{m_l}}$ through Shamir's (m_l, m_l)-SIS scheme with keys $x_{i_{l_1}}, x_{i_{l_2}}, \ldots, x_{i_{l_{m_l}}}$. Each shadow image has the same size as S.
3. Assign shadow image D_{l_u} to participant i_{l_u} for $1 \leq u \leq m_l$. The index l with regard to A_l is distributed to participant i_{l_u}.
4. Distribute the height H and width W to each participant.
5. Merge all, say t_i, shadow images held by participant i into a shadow image UD_i. The size of UD_i is $t_i \times H \times W$. In addition, concatenate all indices corresponding to these t_i shadow images into an index-sequence UI_i with length t_i for participant i.

Note that participant i holds (a) a key x_i, (b) the height H and width W of the secret image, (c) a shadow image UD_i, and (d) an index-sequence UI_i.

In the decoding phase, each $A_l = \{i_{l_1}, i_{l_2}, \ldots, i_{l_{m_l}}\} \in \Gamma_0$ can reveal S by the steps below:

1. For each participant i_{l_u} in A_l where $1 \leq u \leq m_l$, extract H and W. Then, extract index l from $UI_{i_{l_u}}$ and shadow image D_{l_u} with size $H \times W$ from $UD_{i_{l_u}}$.
2. Recover S through Shamir's (m_l, m_l)-SIS decoding method by using the m_l shadows $D_{l_1}, D_{l_2}, \ldots, D_{l_{m_l}}$ with the same index l and the m_l corresponding keys $x_{i_{l_1}}, x_{i_{l_2}}, \ldots, x_{i_{l_{m_l}}}$ held by participants $i_{l_1}, i_{l_2}, \ldots, i_{l_{m_l}}$.

3.2 TL-SIS-QGAS scheme

TL-SIS-QGAS scheme is similar to Shamir-SIS-QGAS scheme, except two differences. The first is that the secret image is encoded into shadow images directly in Shamir-SIS-QGAS scheme, but in TL-SIS-QGAS scheme, the secret image must be transformed into a random image before encoding for each minimal qualified set. The second is that in the shadow image construction, Shamir-SIS-QGAS scheme uses Shamir's (m, m)-SIS scheme, but TL-SIS-QGAS scheme uses Thien-Lin's (m, m)-SIS scheme. The details of the scheme are described as follows.

1. Assign a key x_i to each participant i for $1 \leq i \leq n$, $1 \leq x_i \leq 255$.
2. Distribute the height H and width W to each participant.
3. Assign a seed e_l for each $A_l = \{i_{l_1}, i_{l_2}, \ldots, i_{l_{m_l}}\} \in \Gamma_Q$, where e_l is smaller than a prime q.
4. Generate a random sequence R_l with size $H \times W$ based on e_l.
5. Encode the secret image S into a random image S_l by

   $$S_l = S \oplus R_l,$$

   where $\oplus$ is XOR operator.
6. Encode S_l into shadow images $D_{l_1}, D_{l_2}, \ldots, D_{l_{m_l}}$ by Thien-Lin's (m_l, m_l)- SIS scheme, where m_l keys $x_{i_{l_1}}, x_{i_{l_2}}, \ldots, x_{i_{l_{m_l}}}$ are held by participants in A_l. The size of each shadow image D_{l_u} is $\lceil H \times W/m_l \rceil$.
7. Encode e_l into seed shadows $se_{l_1}, se_{l_2}, \ldots, se_{l_{m_l}}$ by Shamir's (m_l, m_l)-TSS scheme using the same m_l keys in Step 6. All seed shadows are smaller than q.
8. Distribute image D_{l_u} to participant i_{l_u} for $1 \leq u \leq m_l$. The index l, m_l, and seed shadow se_{l_u} with regard to A_l are distributed to participant i_{l_u}.
9. Merge all shadow images held by participant i into a shadow image UD_i. The size of UD_i is $\sum_{l \in \{k | i \in A_k\}} \lceil H \times W/m_l \rceil$. Concatenate all corresponding indice l, m_l and seed shadows into an index-sequence UI_i, number-sequence UN_i and seed-sequence UE_i, respectively.

To avoid forbidden set with e_l to guess the shapes of S, we shared e_l to increase the security in Step 7.

The decoding phase is similar to that of Shamir-SIS-QGAS scheme, except that Shamir's (k, n)-SIS scheme is replaced by Thien-Lin's (k, n)-SIS scheme and S_l is converted to S by XOR with sequence R_l which is generated from e_l. Let each participant i_{l_u} in $A_l = \{i_{l_1}, i_{l_2}, \ldots, i_{l_{m_l}}\} \in \Gamma_0$ have key $x_{i_{l_u}}$, shadow image $UD_{i_{l_u}}$, and three sequences $UI_{i_{l_u}}$, $UN_{i_{l_u}}$ and $UE_{i_{l_u}}$. The detail steps of the decoding phase are described as follows.

1. For each participant i_{l_u} in A_l, extract index l from $UI_{i_{l_u}}$, m_l from $UN_{i_{l_u}}$ and seed shadow se_{l_u} from $UE_{i_{l_u}}$. And extract shadow image D_{l_u} with size $\lceil H \times W/m_l \rceil$ from $UD_{i_{l_u}}$.
2. Reconstruct S_l by using all (m_l) extracted shadow images $D_{l_1}, D_{l_2}, \ldots, D_{l_{m_l}}$ and keys $x_{i_{l_1}}, x_{i_{l_2}}, \ldots, x_{i_{l_{m_l}}}$ through Thien-Lin's (m_l, m_l)-SIS scheme.
3. Reconstruct e_l by using all (m_l) extracted seed shadows $se_{l_1}, se_{l_2}, \ldots, se_{l_{m_l}}$, and the same keys in Step 2 via Shamir's (m_l, m_l)-TSS decoding method.
4. Generate a random sequence R_l with size $|S_l|(= H \times W)$ through e_l.
5. Reconstruct S by applying XOR operator to S_l and R_l,

$$S = S_l \oplus R_l.$$

3.3 TL-SIS-FGAS scheme

TL-SIS-FGAS scheme is similar to Ito-SIS-FGAS scheme, except two differences. The first is that the secret image is encoded into shadow images directly in Ito-SIS-FGAS scheme, but in TL-SIS-FGAS scheme, the secret image must be transformed into a random image before encoding. The second is that in the shadow image construction, Ito-SIS-FGAS scheme uses Shamir's (m, m)-SIS scheme, but TL-SIS-FGAS scheme uses Thien-Lin's (m, m)-SIS scheme. The detail steps are described as below.

1. Prepare a seed e and generate a random sequence R with size $H \times W$ according to e, where e is smaller than a prime q.
2. Encode the secret image S into a random image S' by

$$S' = S \oplus R.$$

3. Select $m(= |Z_M|)$ keys $x_1, x_2, \ldots, x_m$.
4. Encode e into seed shadows $se_1, se_2, \ldots, se_m$ through Shamir's (m, m)-TSS scheme and m keys $x_1, x_2, \ldots, x_m$. All seed shadows are smaller than q.
5. Encode S' into shadow images $D_1, D_2, \ldots, D_m$ through Thien-Lin's (m, m)-SIS scheme and m keys $x_1, x_2, \ldots, x_m$. The size of each shadow image is $\lceil H \times W/m \rceil$.
6. Distribute the height H and width W' ($= \lceil W/m \rceil$) to each participant.
7. For each maximum forbidden set B_f in Z_M, distribute key, seed shadow and shadow image (x_f, se_f, D_f) to each participant not in B_f.
8. Group all received shadow images of participant i into UD_i. The size of UD_i is $H \times W_i'$, where W_i' is the sum of all widths of shadow images that participant i holds. Then, group all keys corresponding to these shadow images in UD_i into a key-sequence UK_i, and group all corresponding seed shadows into a seed-sequence UE_i for participant i.

The decoding phase is similar to Shamir-SIS-FGAS scheme's except replacing Shamir's (k, n)-SIS scheme by Thien-Lin's (k, n)-SIS scheme, and converting the decoded image S' into the secret image S. The detail steps are as follows.

1. For each participant i_{l_u} belonging to $A_l = \{l_1, l_2, \ldots, l_{m_l}\}$, extract H, W', x_f, se_f and D_f with size $H \times W'$ from $UK_{i_{l_u}}$, $UE_{i_{l_u}}$, and $UD_{i_{l_u}}$ based on the same order.
2. Collect m different triples (x_f, se_f, D_f).

3. Reconstruct S' through Thien-Lin's (m, m)-SIS decoding method by using all x_1, $x_2, \ldots, x_m$ and $D_1, D_2, \ldots, D_m$. And reconstruct e via Shamir's (m, m)-TSS decoding method by using all $x_1, x_2, \ldots, x_m$ and $se_1, se_2, \ldots, se_m$.
4. Generate a random sequence R with size $|S'|$ through e.
5. Reconstruct S by applying XOR operator to S' and R.

4 Analysis of shadow sizes

To obtain the total shadow size for each of the aforementioned schemes, we have to find out the sizes of (a) shadow image (UD), (b) key/key-sequence (x/UK), (c) storage for height and width ($H\&W$), (d) index-sequence (UI), (e) number-sequence (UN) and (f) seed-sequence (UE) for each of them. The total shadow size is thus the summation of (a)-(f) correspondingly. Here, bit is the basic unit of total shadow size. We summarize the sizes of (a)–(f) for Ito-SIS-FGAS, BL-SIS-QGAS, and the proposed three schemes in Tables 1 and 2. Note that the sizes of (a), (c)-(f) between BL-SIS-QGAS and Shamir-SIS-QGAS are the same, but the size of (b) in BL-SIS-QGAS is 0.

The features of Ito-SIS-FGAS, BL-SIS-QGAS, and the proposed three schemes in terms of shadow sizes will be further analyzed in the following sub-sections. The qualified set based schemes, i.e., BL-SIS-QGAS, Shamir-SIS-QGAS and TL-SIS-QGAS, and the forbidden set based ones, i.e., Ito-SIS-FGAS and TL-SIS-FGAS will be compared, respectively, in Section 4.1. The two schemes with smaller sizes, i.e., TL-SIS-FGAS and TL-SIS-QGAS, will be further examined in Section 4.2.

4.1 Comparisons between Shamir based and TL based schemes

Based on the information in Tables 1 and 2, we shall further prove two significant findings:

(1) In qualified set based schemes, the total shadow size of Shamir-SIS-QGAS is larger than or equal to that of TL-SIS-QGAS if $8 \times H \times W \geq |P| \times (\lceil \log_2 P \rceil + \lceil \log_2 q \rceil)$.
(2) In forbidden set based schemes, the total shadow size of Ito-SIS-FGAS is larger than or equal to that of TL-SIS-FGAS if and only if $|Z_M| \geq 2$ and $H \times W \geq \lceil \log_2 q \rceil / 4$.

Let BLQ, ITF, SQ, TQ and TF denote the total shadow sizes of BL-SIS-QGAS, Ito-SIS-FGAS, Shamir-SIS-QGAS, TL-SIS-QGAS and TL-SIS-FGAS schemes, respectively. The aforementioned two findings are formally proved as two following theorems.

Theorem 1 *If* $8 \times H \times W \geq |P| \times (\lceil \log_2 P \rceil + \lceil \log_2 q \rceil)$, *then* $SQ \geq TQ$.

Table 1 Shadow size analysis for BL-SIS-QGAS, Shamir-SIS-QGAS and Ito-SIS-FGAS

Scheme	BL-SIS-QGAS	Shamir-SIS-QGAS	Ito-SIS-FGAS
(a) UD	$8 \times H \times W \times \sum_{l=1}^{\lvert\Gamma_0\rvert} \lvert A_l \rvert$	$8 \times H \times W \times \sum_{l=1}^{\lvert\Gamma_0\rvert} \lvert A_l \rvert$	$8 \times H \times W \times \sum_{f=1}^{\lvert Z_M \rvert} (\lvert P \rvert - \lvert B_f \rvert)$
(b) x/UK	0	$8 \times \lvert P \rvert$	$8 \times \sum_{f=1}^{\lvert Z_M \rvert} (\lvert P \rvert - \lvert B_f \rvert)$
(c) $H\&W$	$\lvert P \rvert \times (\lceil \log_2 H \rceil + \lceil \log_2 W \rceil)$	$\lvert P \rvert \times (\lceil \log_2 H \rceil + \lceil \log_2 W \rceil)$	$\lvert P \rvert \times (\lceil \log_2 H \rceil + \lceil \log_2 W \rceil)$
(d) UI	$\lceil \log_2 \lvert\Gamma_0\rvert \rceil \times \sum_{l=1}^{\lvert\Gamma_0\rvert} \lvert A_l \rvert$	$\lceil \log_2 \lvert\Gamma_0\rvert \rceil \times \sum_{l=1}^{\lvert\Gamma_0\rvert} \lvert A_l \rvert$	0
(e) UN	0	0	0
(f) UE	0	0	0

Table 2 Shadow size analysis for TL-SIS-QGAS and TL-SIS-FGAS

Scheme	TL-SIS-QGAS	TL-SIS-FGAS
(a) UD	$\sum_{l=1}^{\lvert\Gamma_0\rvert}\left(\lvert A_l\rvert\times\frac{8\times H\times W}{\lvert A_l\rvert}\right)$ $= 8\times H\times W\times\lvert\Gamma_0\rvert$	$\left\lceil\frac{8\times H\times W}{\lvert Z_M\rvert}\right\rceil\times\sum_{f=1}^{\lvert Z_M\rvert}(\lvert P\rvert-\lvert B_f\rvert)$
(b) x/UK	$8\times\lvert P\rvert$	$8\times\sum_{f=1}^{\lvert Z_M\rvert}(\lvert P\rvert-\lvert B_f\rvert)$
(c) $H\&W$	$\lvert P\rvert\times(\lceil\log_2 H\rceil+\lceil\log_2 W\rceil)$	$\lvert P\rvert\times\left(\lceil\log_2 H\rceil+\lceil\log_2\frac{W}{\lvert Z_M\rvert}\rceil\right)$
(d) UI	$\lceil\log_2\lvert\Gamma_0\rvert\rceil\times\sum_{l=1}^{\lvert\Gamma_0\rvert}\lvert A_l\rvert$	0
(e) UN	$\lceil\log_2 P\rceil\times\sum_{l=1}^{\lvert\Gamma_0\rvert}\lvert A_l\rvert$	0
(f)UE	$\lceil\log_2 q\rceil\times\sum_{l=1}^{\lvert\Gamma_0\rvert}\lvert A_l\rvert$	$\lceil\log_2 q\rceil\times\sum_{f=1}^{\lvert Z_M\rvert}(\lvert P\rvert-\lvert B_f\rvert)$

Proof From Tables 1 and 2, we have

$$\begin{aligned}
SQ &= 8\times H\times W\times\sum_{l=1}^{|\Gamma_0|}|A_l|+8\times|P|+|P|\times(\lceil\log_2 H\rceil+\lceil\log_2 W\rceil)\\
&\quad+\lceil\log_2|\Gamma_0|\rceil\times\sum_{l=1}^{|\Gamma_0|}|A_l|,\\
TQ &= 8\times H\times W\times|\Gamma_0|+8\times|P|+|P|\times(\lceil\log_2 H\rceil+\lceil\log_2 W\rceil)\\
&\quad+\lceil\log_2|\Gamma_0|\rceil\times\sum_{l=1}^{|\Gamma_0|}|A_l|+\lceil\log_2 P\rceil\times\sum_{l=1}^{|\Gamma_0|}|A_l|+\lceil\log_2 q\rceil\times\sum_{l=1}^{|\Gamma_0|}|A_l|.
\end{aligned}$$

After subtracting TQ from SQ, we obtain

$$\begin{aligned}
SQ-TQ &= 8\times H\times W\times\left(\left(\sum_{l=1}^{|\Gamma_0|}|A_l|\right)-|\Gamma_0|\right)\\
&\quad-(\lceil\log_2 P\rceil+\lceil\log_2 q\rceil)\times\sum_{l=1}^{|\Gamma_0|}|A_l|.
\end{aligned}\tag{2}$$

Since $|A_l|\geq 2$ for $1\leq l\leq|\Gamma_0|$. This implies

$$\sum_{l=1}^{|\Gamma_0|}|A_l|-|\Gamma_0|\geq 2\times|\Gamma_0|-|\Gamma_0|=|\Gamma_0|.\tag{3}$$

By (2) and (3), we have

$$SQ-TQ\geq(8\times H\times W\times|\Gamma_0|)-(\lceil\log_2 P\rceil+\lceil\log_2 q\rceil)\times\sum_{l=1}^{|\Gamma_0|}|A_l|.$$

Since $|\Gamma_0|=\sum_{l=1}^{|\Gamma_0|}1$, we obtain

$$\begin{aligned}
SQ-TQ &\geq\sum_{l=1}^{|\Gamma_0|}(8\times H\times W-(\lceil\log_2 P\rceil+\lceil\log_2 q\rceil)\times|A_l|)\\
&\geq\sum_{l=1}^{|\Gamma_0|}(8\times H\times W-(\lceil\log_2 P\rceil+\lceil\log_2 q\rceil)\times|P|).
\end{aligned}\tag{4}$$

If $8\times H\times W\geq|P|\times(\lceil\log_2 P\rceil+\lceil\log_2 q\rceil)$, by (4), we have $SQ-TQ\geq 0$. The proof is completed. □

Theorem 2 *If* $|Z_M| \geq 2$ *and* $H \times W \geq \lceil \log_2 q \rceil / 4$ *, then* $ITF \geq TF$.

Proof From Tables 1 and 2, we have

$$\begin{aligned} ITF &= 8 \times H \times W \times \sum_{f=1}^{|Z_M|} (|P| - |B_f|) + 8 \times \sum_{f=1}^{|Z_M|} (|P| - |B_f|) \\ &\quad + |P| \times (\lceil \log_2 H \rceil + \lceil \log_2 W \rceil), \\ TF &= \left\lceil \frac{8 \times H \times W}{|Z_M|} \right\rceil \times \sum_{f=1}^{|Z_M|} (|P| - |B_f|) + (8 + \lceil \log_2 q \rceil) \times \sum_{f=1}^{|Z_M|} (|P| - |B_f|) \\ &\quad + |P| \times \left(\lceil \log_2 H \rceil + \lceil \log_2 \frac{W}{|Z_M|} \rceil \right). \end{aligned}$$

Therefore

$$\begin{aligned} ITF - TF &= \left(8 \times H \times W - \left\lceil \frac{8 \times H \times W}{|Z_M|} \right\rceil - \lceil \log_2 q \rceil \right) \times \sum_{f=1}^{|Z_M|} (|P| - |B_f|) \\ &\quad + |P| \times \left(\lceil \log_2 W \rceil - \left\lceil \log_2 \frac{W}{|Z_M|} \right\rceil \right). \end{aligned} \tag{5}$$

If $|Z_M| \geq 2$ and $H \times W \geq \lceil \log_2 q \rceil / 4$, then

$$\begin{aligned} & 8 \times H \times W - \left\lceil \frac{8 \times H \times W}{|Z_M|} \right\rceil - \lceil \log_2 q \rceil \\ & \geq 4 \times H \times W - \lceil \log_2 q \rceil \geq 0 \end{aligned} \tag{6}$$

Note that

$$\lceil \log_2 W \rceil - \left\lceil \log_2 \frac{W}{|Z_M|} \right\rceil \geq 0, \tag{7}$$

$$|P| > 0, \tag{8}$$

and

$$\sum_{f=1}^{|Z_M|} (|P| - |B_f|) > 0. \tag{9}$$

By (5) to (9), we have $ITF - TF \geq 0$. The proof is completed. □

Note that in general, $H \times W$ (the size of the secret image) is much larger than $\lceil \log_2 q \rceil$ (the length of the seed) and $|P|$ (the number of participant), respectively. For example, to encrypt a 256×256 secret image among 16 participants by using seeds with 1024 bits, we have $8 \times H \times W (= 8 \times 256 \times 256) > |P| \times (\lceil \log_2 P \rceil + \lceil \log_2 q \rceil) (= 16 \times (4 + 1024))$. This indicates that the condition $8 \times H \times W \geq |P| \times (\lceil \log_2 P \rceil + \lceil \log_2 q \rceil)$ in Theorem 1 is easily satisfied in practical SIS. In addition, $H \times W (= 256 \times 256) \geq \lceil \log_2 q \rceil / 4 (= 1024/4)$, this implies that $H \times W \geq \lceil \log_2 q \rceil / 4$ in Theorem 2 is easily satisfied, too. Thus, according to Theorems 1 and 2, we realize that TL-SIS-FGAS and TL-SIS-QGAS will generate smaller shadow sizes for most circumstances among the five schemes.

4.2 Comparison between TL-SIS-QGAS and TL-SIS-FGAS

To explore the performances of TL-SIS-QGAS and TL-SIS-FGAS in terms of shadow size, we compare the sizes of their shadow images (UDs) in the beginning and then their total shadow sizes. From Table 1, we have

$$UD_{TQ} = 8 \times H \times W \times |\Gamma_0|$$

and

$$UD_{TF} = \left\lceil \frac{8 \times H \times W}{|Z_M|} \right\rceil \times \sum_{f=1}^{|Z_M|} (|P| - |B_f|).$$

To judge which is smaller, we simply compare $|\Gamma_0|$ against $\frac{1}{|Z_M|} \times \sum_{f=1}^{|Z_M|}(|P| - |B_f|)$. We start from examining the relationship between any $B_f(\in Z_M)$ and Γ_0 for $1 \leq f \leq |Z_M|$.

Lemma 1 *Given any pair $(B_f, a_{f,t})$ where $B_f \in Z_M$ and $a_{f,t} \in P \setminus B_f$ for $1 \leq f \leq |Z_M|$ and $1 \leq t \leq |P \setminus B_f|$, there exists $A_l \in \Gamma_0$ such that $A_l \subseteq B_f \cup \{a_{f,t}\}$ and $a_{f,t} \in A_l$ for $1 \leq l \leq |\Gamma_0|$.*

Proof By the definition of Z_M, we have $B_f \cup \{a_{f,t}\} \in \Gamma_Q$. Regarding the relationship between $B_f \cup \{a_{f,t}\}$ and Γ_0, there are two possibilities: $B_f \cup \{a_{f,t}\} \in \Gamma_0$ or $B_f \cup \{a_{f,t}\} \notin \Gamma_0$. If $B_f \cup \{a_{f,t}\} \in \Gamma_0$, the proof is completed. If $B_f \cup \{a_{f,t}\} \notin \Gamma_0$, by the definition of Γ_0 there must exist $A_l \in \Gamma_0$ such that $A_l \subset B_f \cup \{a_{f,t}\}$. Further, if $\{a_{f,t}\} \notin A_l$, then $A_l \subset B_f$, this implies A_l is a forbidden set and results in a contradiction (against $A_l \in \Gamma_0$). Therefore, $\{a_{f,t}\} \in A_l$. □

Example 1 shows what Lemma 1 means.

Example 1 For $P = \{1, 2, 3, 4\}$, consider the following GAS $\mathbf{\Gamma}_1$ specified by $\Gamma_0 = \{A_1, A_2, A_3\} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}\}$ and $Z_M = \{B_1, B_2\} = \{\{1\}, \{2, 3, 4\}\}$. Consider B_1, we have $P \setminus B_1 = \{a_{1,1}, a_{1,2}, a_{1,3}\} = \{2, 3, 4\}$. For pair $(B_1, a_{1,1})$, there exists $A_1 \subseteq B_1 \cup \{a_{1,1}\} = \{1, 2\}$. For $(B_1, a_{1,2})$ and $(B_1, a_{1,3})$, there exists $A_2 \subseteq B_1 \cup \{a_{1,2}\} = \{1, 3\}$, and $A_3 \subseteq B_1 \cup \{a_{1,3}\} = \{1, 4\}$, respectively. Consider B_2, we have $P \setminus B_2 = \{a_{2,1}\} = \{1\}$. For pair $(B_2, a_{2,1})$, there exists $A_1 \subseteq B_2 \cup \{a_{2,1}\} = \{1, 2, 3, 4\}$. Note that there also exist $A_2, A_3 \subseteq B_2 \cup \{a_{2,1}\} = \{1, 2, 3, 4\}$.

Lemma 2 *For two distinct pairs $(B_f, a_{f,t})$ and $(B_f, a_{f,t'})$ where $B_f \in Z_M$ and $a_{f,t}, a_{f,t'} \in P \setminus B_f$ for $1 \leq f \leq |Z_M|$ and $1 \leq t(t') \leq |P \setminus B_f|$, there exists $A_l \in \Gamma_0$ and $A_{l'} \in \Gamma_0$ such that $A_l \subseteq B_f \cup \{a_{f,t}\}$ and $A_{l'} \subseteq B_f \cup \{a_{f,t'}\}$ where $A_l \neq A_{l'}$.*

Proof By Lemma 1, there exists $A_l \in \Gamma_0$ for $(B_f, a_{f,t})$ such that $A_l \subseteq B_f \cup \{a_{f,t}\}$ and $a_{f,t} \in A_l$. Meanwhile, we also have $A_{l'} \in \Gamma_0$ for $(B_f, a_{f,t'})$ such that $A_{l'} \subseteq B_f \cup \{a_{f,t'}\}$ and $a_{f,t'} \in A_{l'}$. Suppose $a_{f,t'} \in A_l$, since $A_l \subseteq B_f \cup \{a_{f,t}\}$, $a_{f,t} \neq a_{f,t'}$ this implies $a_{f,t'} \in B_f$, a contradiction. This means $a_{f,t'} \notin A_l$ and $A_l \neq A_{l'}$. □

Lemma 2 addresses that distinct $A_l, A_{l'} \in \Gamma_0$ exist for distinct $(B_f, a_{f,t})$ and $(B_f, a_{f,t'})$ such that $A_l \subseteq B_f \cup \{a_{f,t}\}$ and $A_{l'} \subseteq B_f \cup \{a_{f,t'}\}$ for any $a_{f,t} \neq a_{f,t'} \in P \setminus B_f$. Below show some illustrating instances.

Example 2 Assume that $P = \{1, 2, 3, 4\}$, consider the following GAS $\mathbf{\Gamma}_2$ specified by $\Gamma_0 = \{A_1, A_2, A_3, A_4\} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3, 4\}\}$ and $Z_M = \{B_1, B_2, B_3, B_4\} = \{\{1\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$. Consider B_1, we have $P \setminus B_1 = \{a_{1,1}, a_{1,2}, a_{1,3}\} = \{2, 3, 4\}$. For $(B_1, a_{1,1})$ and $(B_1, a_{1,2})$, there exist $A_1 \subseteq B_1 \cup \{a_{1,1}\} = \{1, 2\}$ and $A_2 \subseteq B_1 \cup \{a_{1,2}\} = \{1, 3\}$ where $a_{1,1} \neq a_{1,2}$ and $A_1 \neq A_2$. For $(B_1, a_{1,3})$, these also exists $A_3 \subseteq B_1 \cup \{a_{1,3}\} = \{1, 4\}$ where $a_{1,3} \neq a_{1,1}(a_{1,3} \neq a_{1,2})$ and $A_3 \neq A_1(A_3 \neq A_2)$. Further, consider B_2, we have $P \setminus B_2 = \{a_{2,1}, a_{2,2}\} = \{1, 4\}$. For $(B_2, a_{2,1})$ and $(B_2, a_{2,2})$, there exist $A_1, A_2 \subseteq B_2 \cup \{a_{2,1}\} = \{1, 2, 3\}$ and $A_4 \subseteq B_2 \cup \{a_{2,2}\} = \{2, 3, 4\}$ where $a_{2,1} \neq a_{2,2}$ and $A_1(A_2) \neq A_4$. The similar results can be deduced from B_3 and B_4.

Theorem 3 *For each $B_f \in Z_M$, $|P| - |B_f| \leq |\Gamma_0|$.*

Proof For any given $B_f \in Z_M$, let m_f denote the number of elements in $P \setminus B_f$ and $P \setminus B_f = \{a_{f,1}, a_{f,2}, \ldots, a_{f,m_f}\}$. From Lemma 2, we know that there exists m_f distinct $A_{l_t} \in \Gamma_0$ such that $A_{l_t} \subseteq B_f \cup \{a_{f,t}\}$ and $a_{f,t} \in A_{l_t}$. This implies $m_f \leq |\Gamma_0|$, that is, $|P| - |B_f| \leq |\Gamma_0|$. □

Example 3 For $\mathbf{\Gamma}_1$ in Example 1, we have $|P| - |B_1| = 3 = |\Gamma_0|$ and $|P| - |B_2|(= 1) < |\Gamma_0|(= 3)$. Regarding $\mathbf{\Gamma}_2$ in Example 2, $|P| - |B_1|(= 3) < |\Gamma_0|(= 4), |P| - |B_2| = |P| - |B_3| = |P| - |B_4|(= 2) < |\Gamma_0|(= 4)$.

By Theorem 3, we can easily get Corollary 1.

Corollary 1 $\frac{1}{|Z_M|} \times \sum_{f=1}^{|Z_M|}(|P| - |B_f|) \leq |\Gamma_0|$.

In fact, $\frac{1}{|Z_M|} \times \sum_{f=1}^{|Z_M|}(|P| - |B_f|) = |\Gamma_0|$ holds if and only if $|P| - |B_f| = |\Gamma_0|$ for each $B_f \in Z_M$, otherwise, $\frac{1}{|Z_M|} \times \sum_{f=1}^{|Z_M|}(|P| - |B_f|) < |\Gamma_0|$. In the following, we shall further point out that $|P| - |B_f| = |\Gamma_0|$ for each $B_f \in Z_M$ is true only under rather strict condition. Consider only $B_f \in Z_M$ with $P \setminus B_f = \{a_{f,1}, a_{f,2}, \ldots, a_{f,m_f}\}$. Let

$$\Omega_{B_f} = \{B_f \cup \{a_{f,1}\}, B_f \cup \{a_{f,2}\}, \ldots, B_f \cup \{a_{f,m_f}\}\}$$

and

$$\Psi_{B_f} = \{A \in \Gamma_0 \mid A \subseteq B_f \cup \{a_{f,t}\} \; where \; a_{f,t} \in P \setminus B_f\}.$$

It is not hard to see $|\Omega_{B_f}| \leq |\Psi_{B_f}| \leq |\Gamma_0|$. Note that there may be more than one $A \in \Gamma_0$ satisfying $A \subseteq B_f \cup \{a_{f,t}\}$ for a given pair $(B_f, a_{f,t})$. The only condition for $|P| - |B_f| = |\Gamma_0|$ for each $B_f \in Z_M$ becomes

$$|\Psi_{B_f}| = |\Omega_{B_f}| = |\Gamma_0| = |P| - |B_f|,$$

this means $\Psi_{B_f} = \Gamma_0$ for each $B_f \in Z_M$. Corollary 2 is an immediate consequence from our discussion.

Corollary 2 *If $|\Psi_{B_f}| = |\Omega_{B_f}| = |\Gamma_0|$ for each $B_f \in Z_M$, $\frac{1}{|Z_M|} \times \sum_{f=1}^{|Z_M|}(|P| - |B_f|) = |\Gamma_0|$.*

Example 4 Assume that $P = \{1, 2, 3, 4, 5\}$ with a GAS $\mathbf{\Gamma_3}$ specified by $\Gamma_0 = \{A_1, A_2\} = \{\{1, 2, 3\}, \{4, 5\}\}$ and $Z_M = \{B_1, B_2, B_3, B_4, B_5, B_6\} = \{\{1, 2, 4\}, \{1, 2, 5\}, \{1, 3, 4\}, \{1, 3, 5\}, \{2, 3, 4\}, \{2, 3, 5\}\}$. We have $P \setminus B_1 = \{3, 5\}$ $(= \{a_{1,1}, a_{1,2}\})$, $\Omega_{B_1} = \{\{1, 2, 3, 4\}, \{1, 2, 4, 5\}\}$ and $\Psi_{B_1} = \{A_1, A_2\}$ such that $|\Omega_{B_1}| = |\Psi_{B_1}| = |\Gamma_0| = 2$. In addition,

$P \setminus B_2 = \{3, 4\} = (\{a_{2,1}, a_{2,2}\})$, $\Omega_{B_2} = \{\{1, 2, 3, 5\}, \{1, 2, 4, 5\}\}$ and $\Psi_{B_2} = \{A_1, A_2\}$ such that $|\Omega_{B_2}| = |\Psi_{B_2}| = |\Gamma_0| = 2$. The similar results can be deduced from B_3 to B_6.

Consider $\mathbf{\Gamma_1}$ again. We have $\Omega_{B_1} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}\}$ and $\Psi_{B_1} = \{A_1, A_2, A_3\}$ such that $|\Omega_{B_1}| = |\Psi_{B_1}| = |\Gamma_0| = 3$; and $\Omega_{B_2} = \{\{1, 2, 3, 4\}\}$ and $\Psi_{B_2} = \{A_1, A_2, A_3\}$ such that $|\Omega_{B_2}| (= 1) < |\Psi_{B_2}| = |\Gamma_0| (= 3)$.

Regarding $\mathbf{\Gamma_2}$, $\Omega_{B_1} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}\}$ and $\Psi_{B_1} = \{A_1, A_2, A_3\}$ such that $|\Omega_{B_1}| = |\Psi_{B_1}| (= 3) < |\Gamma_0| (= 4)$; and $\Omega_{B_2} = \{\{1, 2, 3\}, \{2, 3, 4\}\}$ and $\Psi_{B_2} = \{A_1, A_2, A_4\}$ such that $|\Omega_{B_2}| (= 2) < |\Psi_{B_2}| (= 3) < |\Gamma_0| (= 4)$; $\Omega_{B_3} = \{\{1, 2, 4\}, \{2, 3, 4\}\}$ and $\Psi_{B_3} = \{A_1, A_3, A_4\}$ such that $|\Omega_{B_3}| (= 2) < |\Psi_{B_2}| (= 3) < |\Gamma_0| (= 4)$; and $\Omega_{B_4} = \{\{1, 3, 4\}, \{2, 3, 4\}\}$, and $\Psi_{B_4} = \{A_2, A_3, A_4\}$ such that $|\Omega_{B_4}| (= 2) < |\Psi_{B_2}| (= 3) < |\Gamma_0| (= 4)$.

Corollary 3 *If all $A_i \cap A_i = \emptyset$ where $A_i, A_j \in \Gamma_0$, then $|\Omega_{B_f}| = |\Psi_{B_f}| = |\Gamma_0|$ for each $B_f \in Z_M$.*

Proof (a) To prove $|\Omega_{B_f}| = |\Psi_{B_f}|$: For any $B_f \in Z_M$ and $a_{f,t} \in P \setminus B_f$, suppose there exist $A_1 \neq A_2 \in \Gamma_0$ such that A_1 and $A_2 \subseteq B_f \cup a_{f,t}$. Since $a_{f,t} \in A_1$ and $a_{f,t} \in A_2$, this imply $A_1 \cap A_2 \neq \emptyset$, contradiction. This implies $|\Omega_{B_f}| = |\Psi_{B_f}|$.

(b) To prove $|\Gamma_0| \leq |\Psi_{B_f}|$: For any $C \in \Gamma_0$, , there exists $a_{f,t} \in P \setminus B_f$, such that $a_{f,t} \in C$. Let $A \in \Gamma_0$, $A \subseteq B_f \cup a_{f,t}$. Since $a_{f,t} \in C \cap A \neq \emptyset$, this implies $C = A$. Since $C \in \Psi_{B_f}$, this means $|\Gamma_0| \leq |\Psi_{B_f}|$.

By (a) and (b), the proof is complete. □

Finally, we compare the total shadow sizes of TL-SIS-QGAS and TL-SIS-FGAS schemes, which are denoted as TQ and TF, respectively.

Theorem 4 *$TF < TQ$ only if $(\lambda_1 = 0$ and $\lambda_2 > 0)$ or $(\lambda_1 > 0$ and $-\lambda_2 < \lambda_1 \times H \times W)$ where $\lambda_1 = 8 \times (|\Gamma_0| - \frac{1}{Z_M} \times \sum_{f=1}^{|Z_M|}(|P| - |B_f|))$ and $\lambda_2 = |P| \times (\lceil \log_2 W \rceil - \lceil \log_2 \frac{W}{|Z_M|} \rceil + 8) + (\lceil \log_2 |\Gamma_0| \rceil + \lceil \log_2 P \rceil + \lceil \log_2 q \rceil) \times \sum_{l=1}^{|\Gamma_0|} |A_l| - (8 + \lceil \log_2 q \rceil \times \sum_{f=1}^{|Z_M|}(|P| - |B_f|))$.*

Proof From Table 2, we have

$$\begin{aligned} TQ &= 8 \times H \times W \times |\Gamma_0| + |P| \times (\lceil \log_2 H \rceil + \lceil \log_2 W \rceil + 8) \\ &\quad + (\lceil \log_2 |\Gamma_0| \rceil + \lceil \log_2 P \rceil + \lceil \log_2 q \rceil) \times \sum_{l=1}^{|\Gamma_0|} |A_l|, \\ TF &= \left\lceil \frac{8 \times H \times W}{|Z_M|} \right\rceil \times \sum_{f=1}^{|Z_M|} (|P| - |B_f|) + (8 + \lceil \log_2 q \rceil) \times \sum_{f=1}^{|Z_M|} (|P| - |B_f|) \\ &\quad + |P| \times \left(\lceil \log_2 H \rceil + \left\lceil \log_2 \frac{W}{|Z_M|} \right\rceil \right). \end{aligned}$$

Then

$$\begin{aligned} TQ - TF &= 8 \times H \times W \times \left(|\Gamma_0| - \frac{1}{|Z_M|} \times \sum_{f=1}^{|Z_M|} (|P| - |B_f|) \right) \\ &\quad + |P| \times \left(\lceil \log_2 W \rceil - \left\lceil \log_2 \frac{W}{|Z_M|} \right\rceil + 8 \right) \end{aligned}$$

Table 3 The total shadow sizes of $\mathbf{\Gamma_1}$, $\mathbf{\Gamma_2}$ and $\mathbf{\Gamma_3}$ for our schemes

	BLQ	ITF	SQ	TQ	TF
$\mathbf{\Gamma_1}$	3145804	2097248	3145836	1579128	**1052764**
$\mathbf{\Gamma_2}$	4718674	4718728	4718706	2106500	**1188992**
$\mathbf{\Gamma_3}$	2621533	6291632	2621565	**1053836**	1061030

$$
\begin{aligned}
&+(\lceil\log_2|\Gamma_0|\rceil + \lceil\log_2 P\rceil + \lceil\log_2 q\rceil) \times \sum_{l=1}^{|\Gamma_0|}|A_l| \\
&-(8+\lceil\log_2 q\rceil) \times \sum_{f=1}^{|Z_M|}(|P|-|B_f|) \\
= {}& \lambda_1 \times H \times W + \lambda_2.
\end{aligned}
$$

By Corollary 1, we have $\lambda_1 = 8 \times (|\Gamma_0| - \frac{1}{Z_M} \times \sum_{f=1}^{|Z_M|}(|P|-|B_f|)) \geq 0$. There are two cases for $\lambda_1 \geq 0$: (1) $\lambda_1 = 0$ and (2) $\lambda_1 > 0$. If $\lambda_1 = 0$ and $\lambda_2 > 0$, $TQ - TF > 0$; otherwise, if $\lambda_1 > 0$ and $-\lambda_2 < \lambda_1 \times H \times W$, then $TQ - TF > 0$. The proof is completed. □

Now, we give an example to summarize the above Theorems and Corollaries.

Example 5 Consider the aforementioned access structures $\mathbf{\Gamma_1}$, $\mathbf{\Gamma_2}$ and $\mathbf{\Gamma_3}$ in Examples 1, 2, and 4, respectively. We share a 256 × 256 secret image (S) by using seeds with 1024 bits ($\lceil\log_2 q\rceil = 1024$) for five schemes. Let BLQ_i, ITF_i, SQ_i, TQ_i and TF_i denote the total shadow sizes of BL-SIS-QGAS, Ito-SIS-FGAS, Shamir-SIS-QGAS, TL-SIS-QGAS and TL-SIS-FGAS schemes for $\mathbf{\Gamma_i}$, respectively. We can use the formula in Tables 1 and 2 to calculate all total shadow sizes as shown in Table 3.

Take SQ_1 as an example. From Table 1, we have $SQ_1 = (8 \times H \times W \times \sum_{l=1}^{|\Gamma_0|}|A_l|) + (8 \times |P|) + (|P| \times (\lceil\log_2 H\rceil + \lceil\log_2 W\rceil)) + (\lceil\log_2|\Gamma_0|\rceil \times \sum_{l=1}^{|\Gamma_0|}|A_l|)$, and from Example 1, we have $|P| = 4$, $|\Gamma_0| = 3$, $\sum_{l=1}^{|\Gamma_0|}|A_l| = 6$. Thus, we can compute $SQ_1 = 3145728 + 32 + 64 + 12 = 3145836$.

First, we obtain $TQ_i < SQ_i$ from Table 3, which conforms with Theorem 1, for $1 \leq i \leq 3$, since the condition $8 \times H \times W > (\lceil\log_2 P\rceil + \lceil\log_2 q\rceil) \times |P|$ is satisfied. Second, we find out that $TF_i < ITF_i$ conforms with Theorem 2 owing to $|Z_M| \geq 2$ and $H \times W > \lceil\log_2 q\rceil/4$. Third, the relation between TF and TQ (i.e., $TF_1 < TQ_1$ and $TF_2 < TQ_2$; but $TF_3 > TQ_3$) also follows Theorem 4. Note that condition $\lambda_1 > 0$ and $-\lambda_2 < \lambda_1 \times H \times W$ are met for both $\mathbf{\Gamma_1}$ and $\mathbf{\Gamma_2}$, thus $TF_1 < TQ_1$ and $TF_2 < TQ_2$. For $\mathbf{\Gamma_3}$, $\lambda_1 = 0$ but $\lambda_2 < 0$, thus $TF_3 > TQ_3$.

5 Concluding remarks

In this paper, three schemes to deal with the SIS for GASs are designed. Compare with references [14] and [9], our proposed schemes have advantages of lossless result of reconstruction image, no public message needed in decoding phase, and both qualified and forbidden sets in access structure are considered in encoding phase. Some remarks of our schemes are: (a) The total shadow sizes of the proposed two schemes TL-SIS-QGAS and TL-SIS-FGAS are smaller than those of BL-SIS-QGAS, Shamir-SIS-QGAS, and Ito-SIS-FGAS in most of the access structures, since the conditions in Theorems 1 and 2 are easily satisfied; (b) UD in TL-SIS-FGAS scheme is smaller than that in TL-SIS-QGAS scheme; (c) The dealer may compute the sizes of these schemes in advance to choose the one producing the smallest shadow size.

As to the security of the three proposed schemes, we only need to prove that any forbidden set cannot reconstruct the secret image. In Shamir-SIS-QGAS Scheme and TL-SIS-QGAS Scheme, we apply Shamir's (m, m)-SIS (or Thien-Lin's (m, m)-SIS) scheme to each minimal qualified set to do secret sharing. Thus, the only way to reconstruct the secret image is using one of the minimal qualified sets. Since any forbidden set F cannot contain a minimal qualified set, this means that F cannot reconstruct the secret image. In TL-SIS-FGAS Scheme, if the number of the maximum forbidden sets is m, the secret image is encoded into m shadows by Thien-Lin's (m, m)-SIS scheme, then any participant in a maximum forbidden set will not own a certain shadow. Since any forbidden set F should be a subset of a certain maximum forbidden set, any participant in F will not own the corresponding shadow. This means that F cannot reconstruct the secret image.

Acknowledgments This work was supported in part by the National Science Council project under Grant NSC 103-2221-E-009-121-MY2.

References

1. Ateniese G, Blundo C, De Santis A, Stinson DR (1996) Visual cryptography for general access structures. Inf Comput 129(2):86–106
2. Benaloh J, Leichter J (1988) Generalized secret sharing and monotone functions. In: Advances in Cryptology-CRYPTO'88, LNCS 1988, vol 403, pp 27–36
3. Blakley GR (1979) Safeguarding cryptographic keys. In: Proceedings AFIPS 1979 National Computer Conference, 48, New York, USA, 4-7 June, pp 313–317
4. Chang CC, Huynh NT, Le HD (2014) Lossless and unlimited multi-image sharing based on Chinese remainder theorem and Lagrange interpolation. Signal Process 99:159–170
5. Guo C, Chang CC (2013) A construction for secret sharing scheme with general access structure. J Inf Hiding Multimed Signal Process 4(1):1–8
6. Horng G (2001) A new method for constructing multiple assignment schemes for generalized secret sharing. J Inf Sci Eng 17:959–65
7. Ito M, Saito A, Nishizeki T (1987) Secret sharing schemes realizing general access structure. In: Proc. IEEE Global Telecommunication Conf. (Globecom 87), pp 99–102
8. Iwamoto M, Yamamoto H, Ogawa H (2007) Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures. IEICE Trans Fundam 90-A(1):101–112
9. Lin YT, Juan JST, Wang YC (2010) A secure and efficient multi-use multi-secret images sharing scheme for general access structure. Proc. of 8th IEEE International Conference on Industrial Informatics (INDIN2010), Osaka University, Osaka, Japan, July 13-16, pp 437–442
10. Linde Y, Buzo A, Gray RM (1980) An algorithm for Vector Quantization design. IEEE Trans Commun 28:84–95
11. Shamir A (1979) How to share a secret. Communication of the ACM 22(11):612–613
12. Thien CC, Lin JC (2002) Secret image sharing. Comput Graph 26:765–70
13. Tochikubo K (2008) Efficient secret sharing schemes based on unauthorized subsets. IEICE Trans Fundam Electron Commun Comput Sci 2008 E91-A(10):2860–2867
14. Tsai CS, Chang CC (2001) A generalized secret image sharing and recovery scheme, Advanced in Multimedia Information Processing. Lect Notes Comput Sci 2195:963–968

Ying-Ru Chen was born in Taipei, Taiwan, Republic of China on February 16, 1983. She received the B.S. degree in Computer Science & Information Engineering from Ming Chuan University, Taoyuan, Taiwan in 2006, and M.S degree in Computer Science & Information Engineering from Ming Chuan University in 2008. She is now a Ph.D student of the Institute of Computer Science and Engineering at the National Chiao Tung University, Hsinchu, Taiwan. She current research interests include Information Security and Secret Sharing.

Ling-Hwei Chen was born in Changhua, Taiwan, Republic of China on February 18, 1954. She received the B.S. degree in Mathematics and the M.S. degree in Applied Mathematics from National Tsing Hua University, Hsinchu, Taiwan in 1975 and 1977, respectively, and the Ph.D. degree in Computer Engineering from National Chiao Tung University, Hsinchu, Taiwan in 1987.

From August 1977 to April 1979 she worked as a research assistant in the Chung-Shan Institute of Science and Technology, Taoyan, Taiwan, From May 1979 to February 1981 she worked as a research associate in the Electronic Research and Service Organization, Industry Technology Research Institute, Hsinchu, Taiwan. From March 1981 to August 1983 she worked as an engineer in the Institute of Information Industry, Taipei, Taiwan. She is now a Professor of the Department of Computer and Information Science at the National Chiao Tung University. Her current research interests include image processing, pattern recognition, document processing, image compression, image cryptography and distributed database system.

Shyong Jian Shyu received the B.S. degree in computer engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1985, and the M.S. degree in computer and decision sciences and the Ph.D. degree in computer science from National Tsing Hua University, Hsinchu, in 1987 and 1991, respectively. In 1994, he joined the Faculty of Ming Chuan University, Taoyuan, Taiwan, where he is currently a Professor with the Department of Computer Science and Information Engineering. He was a Researcher with the Academia Sinica Computer Center, Taipei, from 1993 to 1994. He was with the National Defense Management College, Taipei, serving in the army from 1991 to 1993. His current research interests include design and analysis of algorithms, visual cryptography, computational biology, and computational intelligence.