


A Common General Access Structure Construction Approach in Secret Image Sharing

Xuehu Yan, National University of Defense Technology, Hefei, China

 <https://orcid.org/0000-0001-6388-1720>

Yuliang Lu, National University of Defense Technology, Hefei, China

Lintao Liu, National University of Defense Technology, Hefei, China

ABSTRACT

(k, n) threshold is a special case of the general access structure (GAS) in secret image sharing (SIS), therefore GAS is more extensive than (k, n) threshold. Most of conventional SIS, including visual secret sharing (VSS), polynomial-based SIS, linear congruence (LC)-based SIS, etc., were proposed with only (k, k) threshold or (k, n) threshold other than GAS. This article introduces a common GAS construction approach in SIS with on pixel expansion from existing (k, k) threshold or (k, n) threshold SIS. The authors input classic SIS methods to test the efficiency and feasibility of the proposed common GAS construction approach. Experiments are presented to indicate the efficiency of the approach by illustrations and analysis.

KEYWORDS

General Access Structure, Linear Congruence, Polynomial-Based Secret Image Sharing, Progressiveness, Secret Image Sharing, Visual Cryptography

1. INTRODUCTION

Secret image sharing (SIS) for (k, n) threshold splits a binary, grayscale or color secret image into n noisy shares (also called shadows or shadow images), and then assigns the shares among the owners. The secret can be revealed by collecting k or more authorized shares while less than k shares overall reveal nothing of the secret. Thus, we have n shares (stego-images) in SIS for (k, n) threshold with the feature of loss-tolerance, which is different from cryptology and steganography. SIS can be applied to watermarking, information hiding, authentication, transmitting passwords, access control, securely distributed computing and storage in cloud computing and big data application, etc. (Yan, Lu, Liu, Wan, Ding, & Liu, 2017b; Belazi & El-Latif, 2017). The typical SIS includes polynomial-based scheme (Shamir, 1979), visual secret sharing (VSS) (Naor & Shamir, 1995; Wang, Liu, & Yan, 2016) called visual cryptography (VC) as well, linear congruence (LC)-based method (Liu, Lu, Yan, & Wan, 2016; Yan, Lu, Liu & Wang, 2018) and so on (Yan, Ding & Dongxu, 2000; Yan, Lu, Liu, Wan, Ding, & Liu, 2017a) in SIS research domain.

DOI: 10.4018/IJDCF.2020070107

This article, originally published under IGI Global's copyright on July 1, 2020 will proceed with publication as an Open Access article starting on January 27, 2021 in the gold Open Access journal, International Journal of Digital Crime and Forensics (converted to gold Open Access January 1, 2021), and will be distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

In Shamir's first polynomial-based SIS (Shamir, 1979) for (k, n) threshold, the secret image is generated into the constant coefficient for a constructed random $(k - 1)$ -degree polynomial to get n shares, which are then also assigned to n owners. The secret image can be revealed with high-resolution, i.e., almost lossless recovery, by Lagrange's interpolation when collecting any k or more shares. While less than k shares reveal nothing of the secret. This is so-called "all-or- nothing." Following Shamir's scheme, some other polynomial-based SIS schemes were extended to achieve different features (Yang & Ciou, 2010; Li, Yang, & Kong, 2016). The strength of polynomial- based SIS lies in the secret can be revealed with high quality. Although polynomial-based SIS only utilizes k shares for revealing the distortion-less image, it needs known order of shares, complicated computations for recovery, and no general access structure (GAS). In SIS for GAS (Wu & Sun, 2012; Yan & Lu, 2017), the user may appoint the qualified owners combinations which can recover the secret, i.e., a specification of all qualified subsets of owners may be allocated by the user. Therefore, GAS is more extensive than (k, n) threshold and (k, k) threshold.

In VSS (Weir & Yan, 2010; Yan, Wang & Niu, 2014; Wang, Zhang, Ma, & Li, 2007; Wang, Arce & Di Crescenzo, 2009; Yan, Wang, Niu & Yang, 2015b) for (k, n) threshold, the obtained n shares are first printed onto transparencies and then assigned to n owners. The merit of VSS is, the secret image can be revealed by superposing any k or more shares and human eyes with no cryptographic computation. Collecting less than k shares will in general gives no clue about the secret image even one owns infinite computation power. Unfortunately, original VSS suffers from pixel expansion problem, codebook design and no GAS. As an important VSS research branch, many other researchers took into account of random grid (RG)-based VSS (RGVSS) (Fu & Yu, 2014; Guo, Liu, & Wu, 2013; Yan, Liu, & Yang, 2015a) because RGVSS has neither pixel expansion problem nor codebook design. Kafri and Keren (Kafri & Keren, 1987) first proposed RG-based encryption for binary secret image, split into two random RGs (i.e., shares) with the same size as secret image. The revealed method is superimposing too. Although some VSS schemes for GAS (Ateniese, Blundo, De Santis, & Stinson, 1996; Wu & Sun, 2012) were proposed, most of VSS schemes suffer from no GAS as well.

Besides the above mentioned two primary approaches, some other SIS schemes (Liu, Lu, Yan, & Wan, 2016) were given as well to obtain different features. In (Liu, Lu, Yan, & Wan, 2016), Liu et al. presented a threshold SIS utilizing LC for grayscale secret image according to only addition and module operations, which achieves the advantages of lossless recovery and no pixel expansion by collecting all the n shares etc. However, it is for (k, k) threshold other than GAS. SIS for GAS is more extensive than (k, n) threshold and (k, k) threshold. In this paper, our contribution is that we introduce a common GAS construction approach in SIS with on pixel expansion from existing (k, k) threshold SIS rather than packaging the existing methods. Based on our GAS construction approach, different SIS for GAS algorithms can be derived from different classic SIS methods with (k, k) threshold, respectively. The output SIS by our common GAS construction approach gains GAS, which may be not achieved by previous researches. Experiments are provided to exhibit the efficiency of our method by illustrations and analysis.

The rest of the paper is prepared as follows. Section 2 described some basic requirements and related works. In Section 3, our common GAS construction approach in SIS is given in detail. Section 4 presents experiments. Finally, Section 5 concludes this paper.

2. PRELIMINARIES

In this section, we exhibit some preliminaries for our work. In a (k, n) threshold SIS, the secret image S with size of $W \times H$ is encrypted into total n shares SC_1, SC_2, \dots, SC_n , while the revealed secret image S' is revealed from t ($k \leq t \leq n, t \in \mathbb{Z}^+$) shares. $S(i, j) \in [0, P - 1]$, where $[0, P - 1]$ means the pixel value range and P denotes the maximum pixel value, such as, for VSS $P = 2$ and $P = 251, 256$ or a suitable prime number for grayscale image or colour image sharing.

In the following, \otimes and \oplus indicate Boolean OR and XOR operations, respectively.

2.1. Polynomial-Based (k, n) Threshold SIS

We assume the now processing grayscale secret image pixel value is s , and then to encode s into n pixels assigned to n corresponding shares by Shamir's first polynomial-based SIS scheme. The following Steps are repeated until processing all the secret pixels.

Step 1: For the now processing pixel value $s = S(i, j)$, in order to split s into shared pixels sc_i , we construct a $k - 1$ degree polynomial:

$$g(x) = (a_0 + a_1x + \dots + a_{k-1}x_{k-1}) \bmod P \quad (1)$$

where:

$a_0 = s$, a_i is random for $i = 1, 2, \dots, k - 1$ and $P = 251$

Step 2: SET

$$sc_1 = g(1), \dots, sc_i = g(i), \dots, sc_n = g(n) \quad (2)$$

In the recovery of polynomial-based SIS, for any given k pairs of n pairs $\left\{ \left(i, sc_i \right) \right\}_{i=1}^n$, where i may be served as an order label of the i^{th} owner, we can obtain the coefficients of $g(x)$ based on Lagrange's interpolation, and then get $s = g(0)$. The processing repeats until all pixels of the secret image are processed. And the secret image S cannot be overall revealed with less than k shares.

Since (k, k) threshold is a specific case of (k, n) threshold, (k, n) threshold is also suitable for our common GAS construction approach, where we can set $k = n$.

2.2. (k, k) Threshold VSS

In RGVSS (Kafri & Keren, 1987), 1 indicates black pixel and 0 denotes white pixel. The generation steps and revealing phase of one popular original $(2, 2)$ RGVSS are described as follows:

Step 1: Construct 1 RG SC_1 randomly. Step 2: Compute SC_2 as in Equation (3).

Revealing phase: $S' = SC_1 \otimes SC_2$ from Equation (4). If the secret pixel $s = S(i, j)$ is 1, the recovery bit.

$sc_1 \otimes sc_2 = 1$ is black. If the certain secret pixel is 0, the recovery bit $sc_1 \otimes sc_2 = SC_1(i, j) \otimes SC_2(i, j)$ has half chance to be black or white because sc_1 is generated randomly:

$$SC_2(i, j) = \begin{cases} SC_1(i, j) & \text{if } S(i, j) = 0 \\ \overline{SC_1(i, j)} & \text{if } S(i, j) = 1 \end{cases} \quad (3)$$

$$S'(i, j) = SC_1(i, j) \otimes SC_2(i, j) = \begin{cases} SC_1(i, j) \otimes SC_1(i, j) & \text{if } S(i, j) = 0 \\ SC_1(i, j) \otimes \overline{SC_1(i, j)} = 1 & \text{if } S(i, j) = 1 \end{cases} \quad (4)$$

We remark that, Equation (3) is equal to $sc_2 = sc_1 \otimes s$. Due to if $s = 0 \Rightarrow sc_2 = sc_1 \otimes 0 \Rightarrow sc_2 = sc_1$, and if $s = 1 \Rightarrow sc_2 = sc_1 \otimes 1 \Rightarrow sc_2 = \overline{sc_1}$. Thus, the same equation can be extended to $s = sc_1 \otimes sc_2 \otimes \dots \otimes sc_k$ so that (k, k) threshold RGVSS is achieved.

2.3. (k, k) Threshold Linear Congruence-Based SIS

Equation (5) exhibits the primary equation for LC-based secret sharing, based on which (k, k) threshold secret sharing will be achieved, where P is a number larger than the biggest pixel value, sc_i and s indicate the i -th shared pixel and secret pixel, respectively. Aiming to share a grayscale secret image, in general we set $P = 256$:

$$(sc_1 + sc_2 + \dots + sc_k) \bmod P = s \quad (5)$$

2.4. General Access Structure

The definition (Ateniese, Blundo, De Santis & Stinson, 1996) of GAS is described as follows.

2.4.1. Definition 1 (GAS)

$\{\Gamma_{Qual}, \Gamma_{Forb}\}$ is known as a GAS, which is a specification of all qualified and forbidden subsets (Γ_{Qual} and Γ_{Forb}) of owners $P = \{1, 2, \dots, n\}$, where $i \in [1, n]$ means an owner with the order number of “ i ”. Any set $X = \{i_1, i_2, \dots, i_r\} \in \Gamma_{Qual}$, where owners $i_1, i_2, \dots, i_r \in P$, can reveal the secret image while any set $X \in \Gamma_{Forb}$ reveals nothing of the secret, which is the security of SIS for GAS. Here, Γ_{Qual} and Γ_{Forb} exhibit non-empty subsets of owners set P , where $\Gamma_{Qual} \subseteq 2^P$, $\Gamma_{Forb} \subseteq 2^P$ and $\Gamma_{Qual} \cap \Gamma_{Forb} = \emptyset$.

Let Γ_0 denote a set consisting of the minimum qualified sets, as follows:

$$\Gamma_0 = \{Q \in \Gamma_{Qual} \mid Q' \notin \Gamma_{Qual}, \forall Q' \subset Q\} \quad (6)$$

where the element of Γ_0 is one minimum qualified set, i.e., there is not any qualified set less than the element of Γ_0 . For any $A \in \Gamma_0$, there exists $B \in \Gamma_{Qual}$ satisfying $A \subseteq B$.

Owner $p \in P$ is called an essential owner if $\{A \mid A \cup \{p\} \in \Gamma_{Qual}, A \notin \Gamma_{Qual}\} \neq \emptyset$, where A indicates any subset of P . $p \in P$ is an essential owner tells that at least one subset of P needs to contain p to be a qualified set.

The GAS is strong and Γ_0 is a basis if Γ_{Qual} is monotone increasing and Γ_{Forb} is monotone decreasing.

In this paper, we assume that all the owners are essential and the GAS is strong.

In definition 1, the revealed secret image may be lossy in GAS, which will be considered in the next Section 2.5.

2.5. Quality Evaluation Metrics of the Revealed Secret Image

In VSS, the visual quality of the revealed secret image S' will decide how well human eyes can recognize the revealed image, which can be evaluated by contrast as follows (Yan, Liu & Yang, 2015a).

2.5.1. Definition 2 (Contrast)

$$\alpha = \frac{P_0 - P_1}{1 + P_1} = \frac{P(S'[AS0] = 0) - P(S'[AS1] = 0)}{1 + P(S'[AS1] = 0)} \quad (7)$$

where α is contrast, P_0 (resp., P_1) demonstrates the appearance probability of white pixels in the revealed image S' for the corresponding white (resp., black) area of secret image S , that is, P_0 is

the correctly decrypted probability corresponding to the white area in secret image S , and P_1 is the wrongly decrypted probability corresponding to the black area in secret image S . $AS0$ (resp., $AS1$) indicates the white (resp., black) area of secret image S .

Due to lossless recovery or nothing, classic SIS for grayscale image omits to consider the quality evaluation of the revealed secret image. The revealed secret image may be lossy in GAS, therefore we need to consider the quality evaluation of the revealed grayscale secret image. The following objective metrics may be adopted to evaluate the image quality between S' and S .

1. Peak signal-to-noise-ratio ($PSNR$): $PSNR$, in Equation (8) between S and S' , is used to measure image similarity, where MSE indicates the mean square error, as in Equation (9):

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) dB \quad (8)$$

$$MSE = \frac{1}{W \times H} \sum_{i=1}^W \sum_{j=1}^H [S'(i, j) - S(i, j)]^2 \quad (9)$$

2. Structural similarity index measure (SSIM) (Wang, Bovik, Sheikh & Simoncelli, 2004) is used to evaluate the visual impact of three characteristics for an image, i.e., luminance, contrast and structure, which obtains a multiplicative combination of the above three characteristics, as exhibited in Equation (10). SSIM is in -1 and 1. The larger SSIM indicates higher image similarity:

$$SSIM(x, y) = [I(x, y)]^\alpha [C(x, y)]^\beta [S(x, y)]^\gamma \quad (10)$$

where μ_x , μ_y , σ_x , σ_y , and σ_{xy} are the local means, standard deviations, and cross-covariance for images x , y . In this paper, we assume $C_3 = \frac{C_2}{2}$, $\alpha = \beta = \gamma = 1$.

3. A COMMON GAS CONSTRUCTION APPROACH IN SIS

Here, we will introduce a common GAS construction approach in SIS with on pixel expansion from existing SIS for only (k, k) threshold.

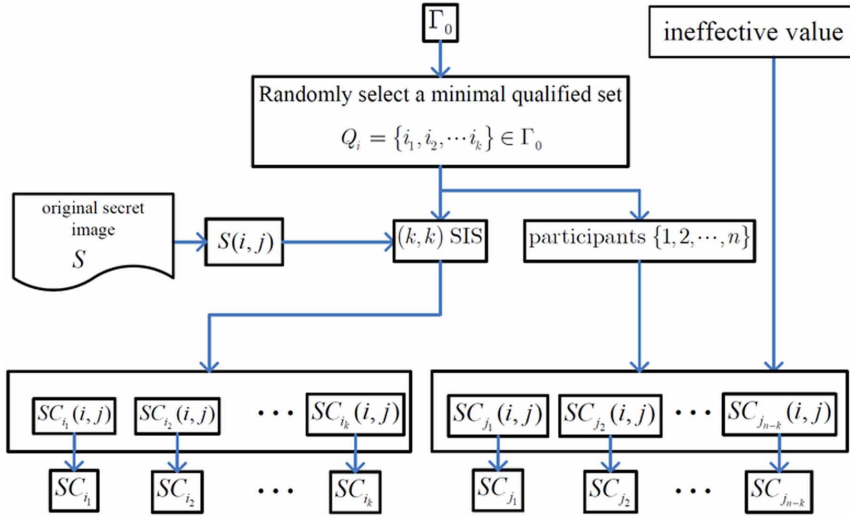
3.1. Our Method

The introduced common GAS construction approach is presented in Algorithm 1, whose diagrammatic design concept is shown in Figure 1.

In Algorithm 1, we remark that:

1. The GAS and existing (k, k) threshold SIS are input or selected by the user other than our common GAS construction approach, based on which our approach can derive specific SIS for GAS;
2. Here we input existing (k, k) threshold SIS, where $2 \leq k \leq n$;
3. For each position $(h, w) \in \{(h, w) | 1 \leq h \leq H, 1 \leq w \leq W\}$, k and shares orders are determined by $\{i_1, i_2, \dots, i_k\}$ corresponding to selected A in Step 2;
4. In Step 2, if one minimum qualified set is selected, say A , the participants in A can recover only a portion of the whole image. The portion will decrease as the number of participants increases.

Figure 1. The design concept of our introduced common GAS construction approach from existing SIS for (k, k) threshold



Algorithm 1. The introduced common GAS construction approach from existing SIS for (k, k) threshold

Input: (1) a $W \times H$ secret image: S , (2) the strong general access structure $\{\Gamma_{Qual}, \Gamma_{Forb}\}$, (3) (k, k) threshold SIS.

Output: n shares SC_1, SC_2, \dots, SC_n .

Step 1: From the input GAS $\{\Gamma_{Qual}, \Gamma_{Forb}\}$, obtain its basis Γ_0 . For each position $(h, w) \in \{(h, w) | 1 \leq h \leq H, 1 \leq w \leq W\}$, repeat Steps 2-5.

Step 2: Randomly select one minimum qualified set $A = \{i_1, i_2, \dots, i_k\} \in \Gamma_0$.

Step 3: For the current secret pixel $s = S(h, w)$ and $\{i_1, i_2, \dots, i_k\}$, use (k, k) threshold SIS to split s into k shared pixels assigned to k shadow pixels $SC_{i_1}, SC_{i_2}, \dots, SC_{i_k}$, respectively.

Step 4: If $k < n$, then go to Step 5.

Step 5: Set all the last $n - k$ shared pixels to be ineffective value in the revealed phase of existing SIS for (k, k) threshold.

Step 6: Output n shares SC_1, SC_2, \dots, SC_n .

Thus, our construction approach is a progressive one as t increases with the same minimum qualified set;

5. Ineffective value is decided by the recovery method of existing SIS:
 - a. In polynomial-based SIS, the modular 251 operation is applied to the recovery phase, therefore ineffective value can be any integer in $[251, 255]$. Here, the ineffective value can be viewed as a flag, whose corresponding shadow pixel will not join in the recovery;
 - b. In VSS, the recovery method is stacking, thus ineffective value is 0 (white). (c) For LC-based SIS, since additive recovery, ineffective value is 0 (black).

3.2. GAS Construction Proof and Analysis

Here, we only perform general performance analysis due to detail performance analysis can be given according to specific existing SIS. Without losing of generality, in the analysis, we assume that sc_1 ,

sc_2, \dots, sc_k are generated based on the secret pixel s and existing (k, k) threshold SIS in Step 3 of the proposed approach and the other $n - k$ pixels $sc_{k+1}, sc_{k+2}, \dots, sc_n$ are obtained in Step 5, respectively.

In Steps 2-3, for every secret pixel, A is randomly selected from Γ_0 , as a result its (k, k) thresh- old mechanism will be achieved in Step 3 for GAS, where $|A| = k$. Since sc_1, sc_2, \dots, sc_k are ob- tained by the secret pixel s and existing (k, k) threshold SIS, we can reveal the secret s when collecting sc_1, sc_2, \dots, sc_k , i.e., sc_1, sc_2, \dots, sc_k are the really effective pixels covered the secret. The last $n - k$ share pixels are ineffective values. When we collect k shares, we will cover sc_1, sc_2, \dots, sc_k at a certain probability, therefore the secret will be revealed in a degree. When collecting more than k shadows, the probability of covering sc_1, sc_2, \dots, sc_k will be improved so that the GAS will be gained.

Any set $X = \{i_1, i_2, \dots, i_r\} \in \Gamma_{Qual}$, where owners $i_1, i_2, \dots, i_r \in P$, can reveal the secret image while any set $X \in \Gamma_{Forb}$ reveals nothing of the secret, which illustrates the security of SIS for GAS:

1. Every single share is secure. In Step 3 of our method, the first k shared pixels are generated from existing (k, k) threshold SIS, thus every single pixel of the first k shared pixels gives no clue about the secret s . Furthermore, the last $n - k$ shared pixels are set to be ineffective value, among which single one has no relation with the secret s . As a result, there will be no cross interference of the secret in every share, i.e. every single share could reveal nothing of the secret image;
2. The security of SIS for GAS. For any set $X \in \Gamma_{Forb}$, X cannot cover A , thus X cannot cover sc_1, sc_2, \dots, sc_k . As a result, any set $X \in \Gamma_{Forb}$ reveals nothing of the secret;
3. GAS construction. For any set $X = \{i_1, i_2, \dots, i_r\} \in \Gamma_{Qual}$, there exists $A \in X$ at a certain probability. Thus, X can cover sc_1, sc_2, \dots, sc_k at a certain probability. Finally, any set $X = \{i_1, i_2, \dots, i_r\} \in \Gamma_{Qual}$ can reveal the secret image in a degree.

4. EXPERIMENTAL RESULTS AND ANALYSES

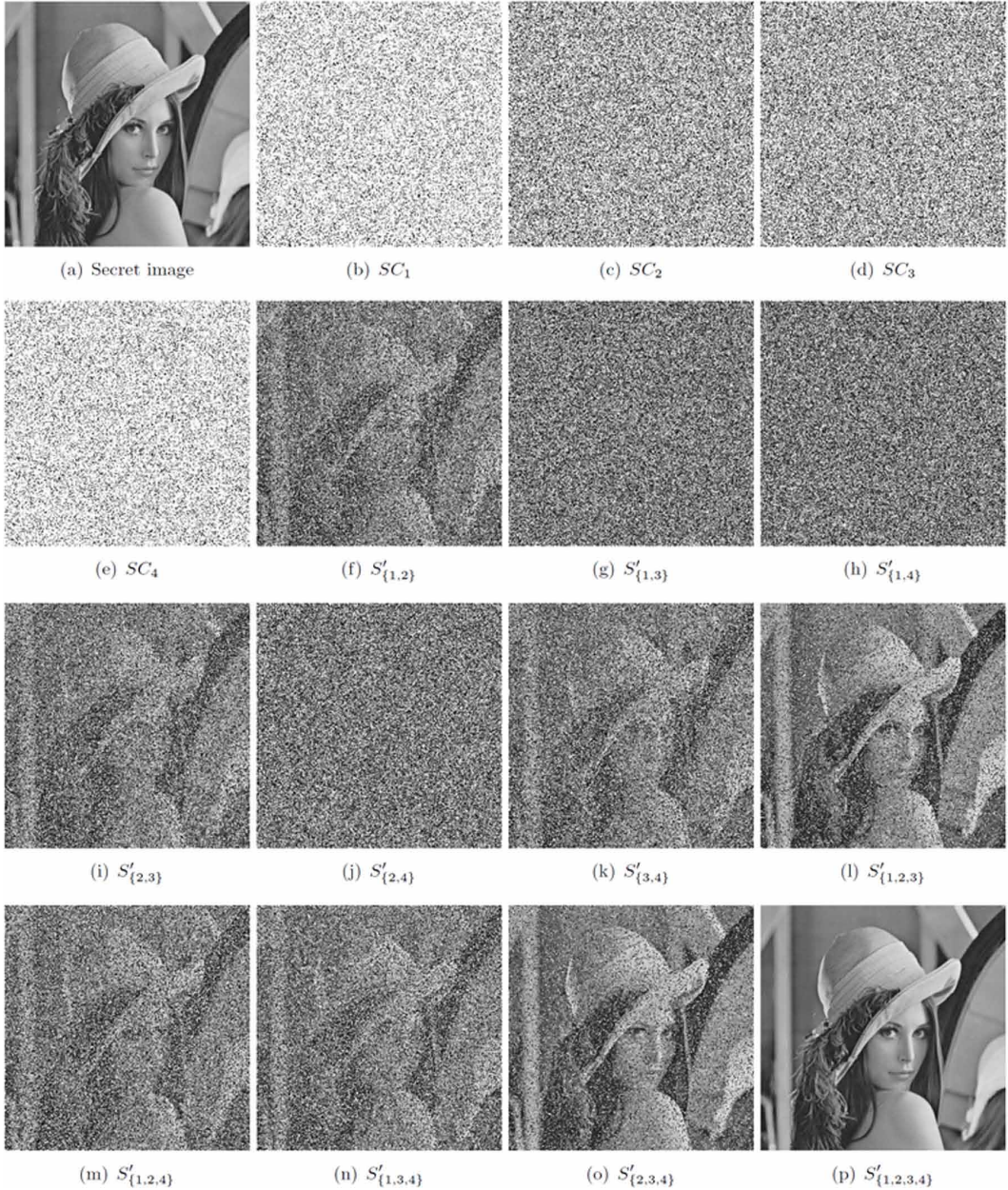
In this Section, we will input classic SIS methods to test the efficiency and feasibility of the proposed common GAS construction approach. Experimental results and analysis will be realized to illustrate the effectiveness of the derived GAS construction algorithms gained by our introduced common GAS construction approach in SIS. In addition, some discussions are further provided.

4.1. Image Illustration and Quality

Figure 2 denotes the experimental results of the constructed SIS for GAS from (k, k) threshold polynomial-based SIS by our introduced common GAS construction approach, where $\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$ based on Lagrange's interpolation decryption and the grayscale secret image is in Figure 2(a). Figure 2(b-e) give the 4 shares, which are noisy. Figure 2(g-p) display the revealed grayscale secret image when collecting any t ($2 \leq t \leq 4$) shares by Lagrange's interpolations. The revealed images by the qualified sets can reveal the secret image but reveal nothing by the forbidden sets. When the qualified sets with the same minimum set and more owners are employed, better revealed secret image is obtained. When all the owners are collected, the revealed secret image is high-resolution due to our approach and existing (k, k) threshold polynomial-based SIS.

Figure 3 demonstrates the results of the constructed SIS for GAS from (k, k) threshold RGVS by our introduced common GAS construction approach, where $\Gamma_0 = \{\{1, 2, 3\}, \{1, 4\}, \{3, 4\}\}$ based on stacking decryption and the binary secret image is given in Figure 3(a). Figure 3(b-e) displays the 4 shares SC_1, SC_2, SC_3 , and SC_4 , which are noisy as well. Figure 3(f-p) are the revealed secret images when collecting any 2 or more shares based on stacking recovery, from which the secret image by the qualified sets could be recognized based on superposition while nothing by the forbidden sets. When the qualified sets with the same minimum set and more owners are employed, better revealed

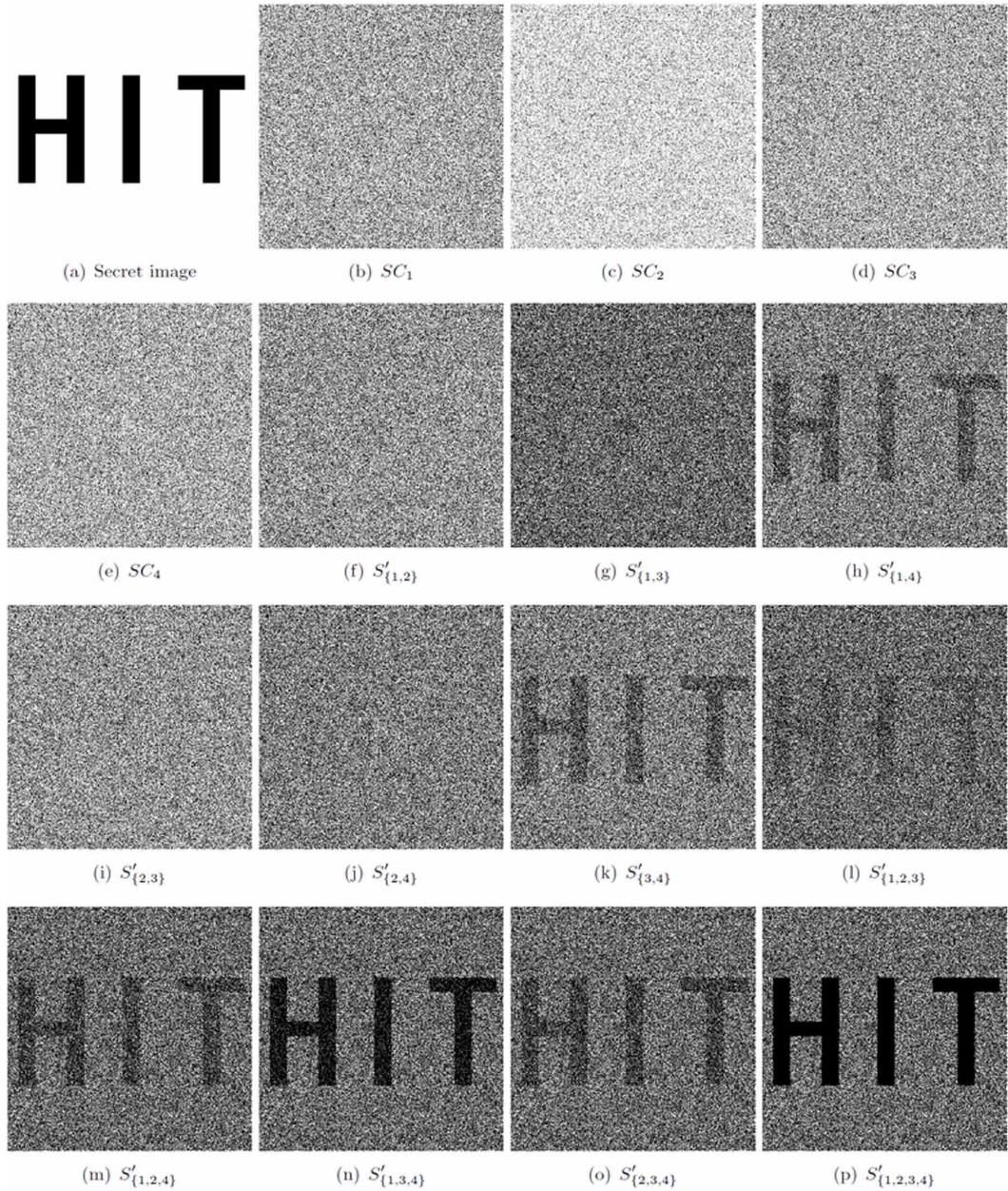
Figure 2. Simulation results of the constructed SIS for GAS from (k, k) threshold polynomial-based SIS by our introduced common GAS construction approach, where $\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$ based on Lagrange's interpolation decryption. (a) The grayscale secret image; (b) -- (e) four shares SC_1 , SC_2 , SC_3 and SC_4 ; (f)–(p) revealed results by different shares.



secret image is obtained as well. When all the owners are collected, the visual quality of the revealed secret image is the best.

Figure 4 is an example for the constructed SIS for GAS from (k, k) threshold LC-based SIS by our introduced common GAS construction approach, where $\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$ based on additive decryption and the input grayscale secret image is in Figure 4(a). Figure 4(b) – (e) are the

Figure 3. Simulation results of the constructed SIS for GAS from (k, k) threshold RGVS by our introduced common GAS construction approach, where $\Gamma_0 = \{\{1, 2, 3\}, \{1, 4\}, \{3, 4\}\}$ based on stacking decryption. (a) The binary secret image; (b) - (e) four shares SC1, SC2, SC3, and SC4; (f)-(p) revealed results by different shares.

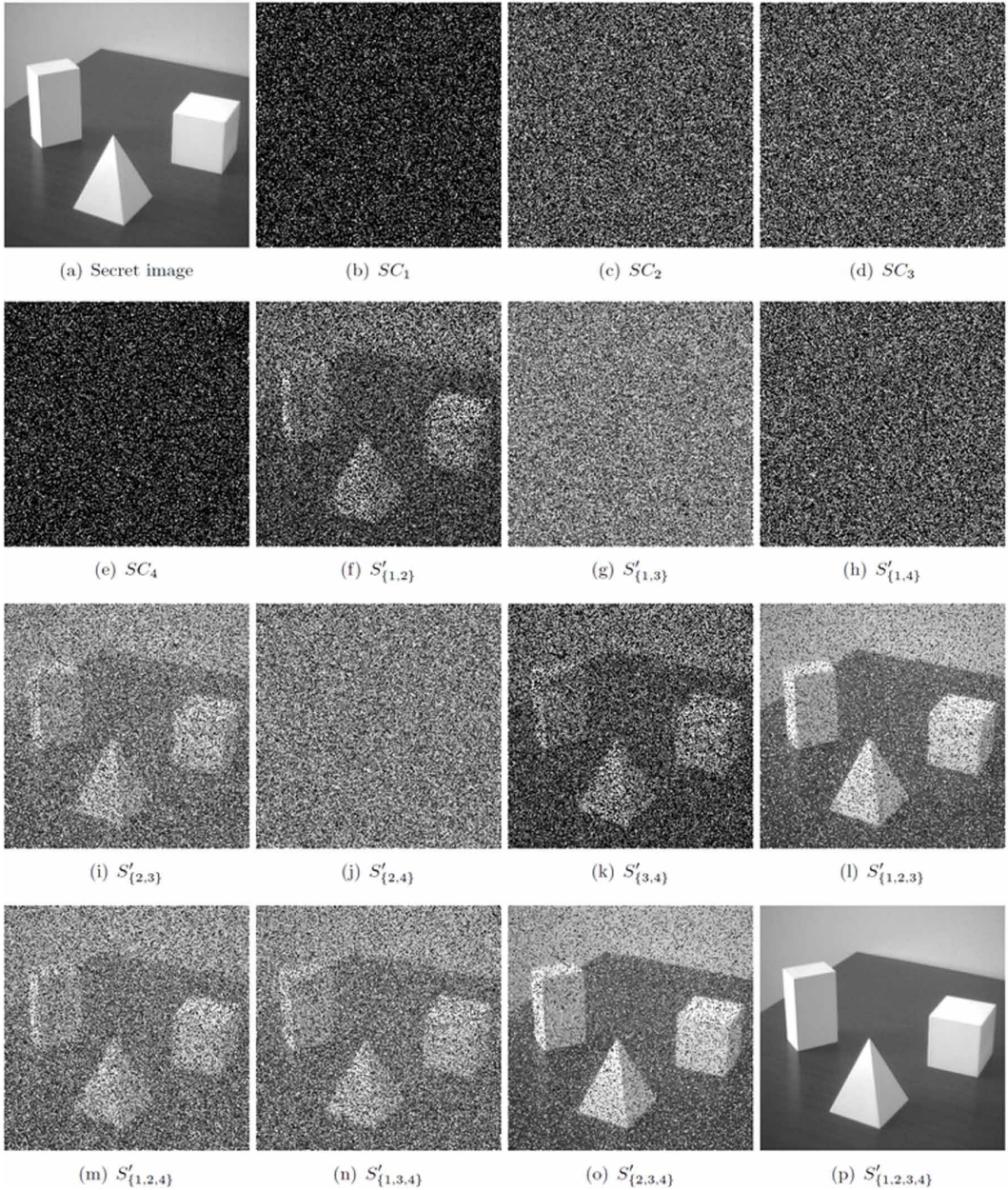


4 generated shares, which are noisy as well. Figure 4(f) – (p) demonstrate the revealed images with different orders of shares. Similar conclusion as the above results will be obtained.

For the above experiments, their corresponding quality metrics of the revealed secret image are given in Table 1. From Table 1, based on our GAS construction approach, the derived different SIS for GAS algorithms achieve GAS as well as progressive feature when more shares are collected.

By the above results we can find that:

Figure 4. Simulation results of the constructed SIS for GAS from (k, k) threshold LC-based SIS by our introduced common GAS construction approach, where $\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$ based on additive decryption. (a) The grayscale secret image; (b)- (e) four shares SC1, SC2, SC3, and SC4; (f)-(p) revealed results by different shares.



1. The shares are noisy, therefore there is no cross interference of secret image in each share;
2. When shadow images in the forbidden sets are inspected, there is no information of the secret image can be leaked showing the security of our method;
3. When we collect shadow images in the qualified sets, the secret image could be revealed;
4. When all the owners are collected, the best quality of the revealed secret image is obtained since our approach and existing (k, k) threshold SIS;

Table 1. The quality metrics of the revealed secret image

Basis Γ_0	Quality Metrics
Figure 2 for $\Gamma_0 = \{\{1,2\}, \{2,3\}, \{3,4\}\}$ of the constructed SIS for GAS from (k, k) threshold polynomial- based SIS	$PSNR_{(1,2)} = 10.5935, PSNR_{(2,3)} = 10.6352, PSNR_{(3,4)} = 10.6244, PSNR_{(1,2,3)} = 13.5586, PSNR_{(1,2,4)} = 10.6179, PSNR_{(1,3,4)} = 10.6412, PSNR_{(2,3,4)} = 13.6972, PSNR_{(1,2,3,4)} = +\infty$
Figure 2 for $\Gamma_0 = \{\{1,2\}, \{2,3\}, \{3,4\}\}$ of the constructed SIS for GAS from (k, k) threshold polynomial- based SIS	$SSI M_{(1,2)} = 0.0558, SSI M_{(2,3)} = 0.0584, SSI M_{(3,4)} = 0.0565, SSI M_{(1,2,3)} = 0.1523, SSI M_{(1,2,4)} = 0.0587, SSI M_{(1,3,4)} = 0.0562, SSI M_{(2,3,4)} = 0.1549, SSI M_{(1,2,3,4)} = 1$
Figure 3 for $\Gamma_0 = \{\{1,2,3\}, \{1,4\}, \{3,4\}\}$ of the constructed SIS for GAS from (k, k) threshold RGVSS	$\alpha_{(1,4)} = 0.1231, \alpha_{(3,4)} = 0.1250, \alpha_{(1,2,3)} = 0.0583, \alpha_{(1,2,4)} = 0.1322, \alpha_{(1,3,4)} = 0.3048, \alpha_{(2,3,4)} = 0.1344, \alpha_{(1,2,3,4)} = 0.4152$
Figure 4 for $\Gamma_0 = \{\{1,2\}, \{2,3\}, \{3,4\}\}$ of the constructed SIS for GAS from (k, k) threshold LC-based SIS	$PSNR_{(1,2)} = 8.1156, PSNR_{(2,3)} = 10.4125, PSNR_{(3,4)} = 8.1317, PSNR_{(1,2,3)} = 13.4090, PSNR_{(1,2,4)} = 10.4129, PSNR_{(1,3,4)} = 10.4271, PSNR_{(2,3,4)} = 13.4367, PSNR_{(1,2,3,4)} = +\infty$
Figure 4 for $\Gamma_0 = \{\{1,2\}, \{2,3\}, \{3,4\}\}$ of the constructed SIS for GAS from (k, k) threshold LC-based SIS	$SSI M_{(1,2)} = 0.0188, SSI M_{(2,3)} = 0.0272, SSI M_{(3,4)} = 0.0200, SSI M_{(1,2,3)} = 0.0666, SSI M_{(1,2,4)} = 0.0272, SSI M_{(1,3,4)} = 0.0292, SSI M_{(2,3,4)} = 0.0680, SSI M_{(1,2,3,4)} = 1$

- When the qualified sets with the same minimum set and more owners are employed, better image quality will be gained. Thus, the derived SIS algorithms are progressive, for the same minimum qualified set;
- We obtain a common GAS construction approach.

4.2. Comparisons With Relative Schemes

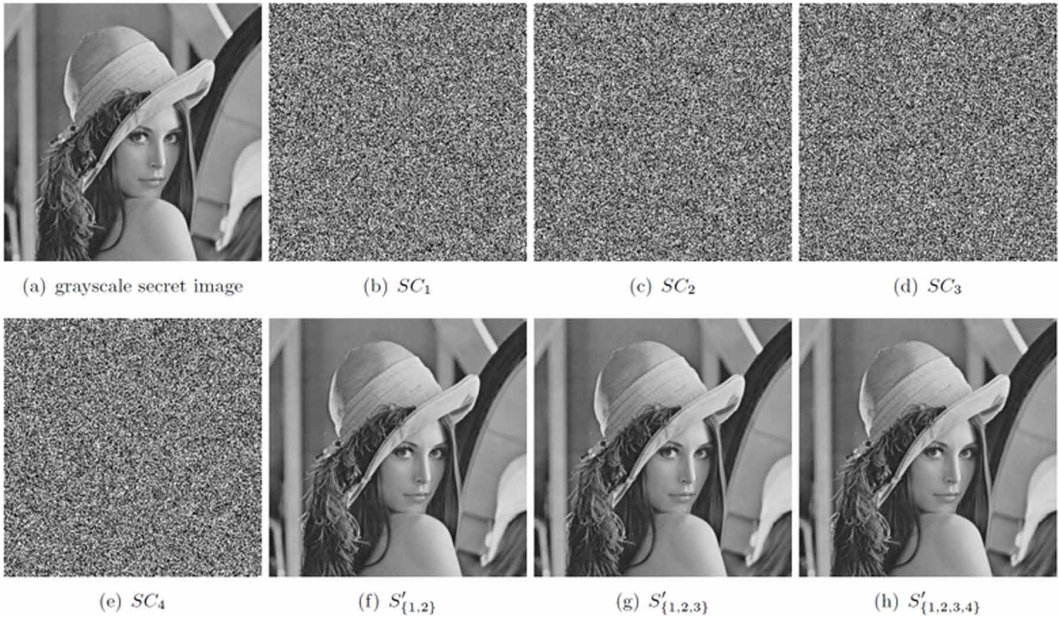
We will first compare the constructed GAS from polynomial-based SIS with existing polynomial-based (k, n) threshold SIS (Li, Yang & Kong, 2016), where only the first coefficient is utilized to cover the secret. Then analysis will be performed.

As comparison, Figure 5 displays the experimental results for existing polynomial-based (k, n) threshold SIS, where $k = 2, n = 4$ and the grayscale secret image is shown in Figure 5(a). Figure 5(b-e) show the 4 shares, which are also noisy. Figure 5(f-h) indicate the revealed grayscale secret image with any t ($2 \leq t \leq 4$) shares by Lagrange's interpolations. We can find existing polynomial-based (k, n) threshold SIS has neither GAS nor progressiveness.

According to Figure 2 and Figure 5, the constructed GAS is progressive when the same minimum set is used. Pre-existed polynomial-based (k, n) threshold SIS has no GAS.

In addition, comparing functionalities with relative GAS (Ateniese, Blundo, De Santis & Stinson, 1996; Wu & Sun, 2012; Yan & Lu, 2017), our features lie in:

Figure 5. Experimental example of existing polynomial-based (k, n) threshold SIS (Li, Yang & Kong, 2016), where $k = 2$, $n = 4$. (a) The grayscale secret image; (b) - (e) four shares SC_1 , SC_2 , SC_3 , and SC_4 ; (f) - (h) revealed results by t shares, where $t = 2, 3$, and 4, respectively.



1. Our introduced method belongs to a common GAS construction approach in SIS from existing SIS for only (k, k) threshold other than detail GAS algorithm;
2. Some existing SIS schemes are employed in our method resulting in effective GAS, which illustrates the feasibility of the introduced common GAS construction approach in SIS;
3. For any given new SIS, based on our common GAS construction approach in SIS, a new GAS may be derived with special characteristic;
4. For detail GAS algorithmic comparisons, we need refer to special input existing SIS, thus which is omitted in this paper.

4.3. Extensions and Discussion

According to the above results and analysis, our approach may be extended as follows:

1. Our approach may be suitable for SIS with pixel expansion;
2. Based on color decomposition and color composition, our approach can share color secret image;
3. Some other ideas may be further utilized in our approach to enhance the image quality (Yan, Liu & Yang, 2015a; Yan, Wang & Niu, 2014).

5. CONCLUSION

In this paper, we introduced a common general access structure (GAS) construction approach in secret image sharing (SIS) from input existing SIS for only (k, k) threshold. Based on our GAS construction approach, then different SIS algorithms for GAS were derived from existing SIS for (k, k) threshold, respectively, which indicates the efficiency and feasibility of the proposed common GAS construction approach in terms of analysis and experimental results. Extending GAS construction approach owning better features are our future work.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China (Grant Number: 61602491) and the Key Program of the National University of Defense Technology (Grant Number: ZK-17-02-07). Dr. Xuehu Yan, affiliated with National University of Defense Technology, Hefei, China (publictiger@126.com) aided this project by serving as the corresponding author.

REFERENCES

- Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (1996). Visual cryptography for general access structures. *Information and Computation*, 129(2), 86–106. doi:10.1006/inco.1996.0076
- Belazi, A., & El-Latif, A. A. A. (2017). A simple yet efficient s-box method based on chaotic sine map. *Optik - International Journal for Light and Electron Optics*, 130, 1438–1444. doi:10.1016/j.ijleo.2016.11.152
- Fu, Z.-x., & Yu, B. (2014). Visual cryptography and random grids schemes. In *Digital-Forensics and Watermarking* (pp. 109–122). Springer.
- Guo, T., Liu, F., & Wu, C. (2013). Threshold visual secret sharing by random grids with improved contrast. *Journal of Systems and Software*, 86(8), 2094–2109. doi:10.1016/j.jss.2013.03.062
- Kafri, O., & Keren, E. (1987). Encryption of pictures and shapes by random grids. *Optics Letters*, 12(6), 377–379. doi:10.1364/OL.12.000377 PMID:19741737
- Li, P., Yang, C.-N., & Kong, Q. (2016). A novel two-in-one image secret sharing scheme based on perfect black visual cryptography. *Journal of Real-Time Image Processing*, 1–10.
- Liu, L., Lu, Y., Yan, X., & Wan, S. (2016). A progressive threshold secret image sharing with meaningful shares for gray-scale image. In *Proceedings of the 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)* (pp. 380–385). IEEE. doi:10.1109/MSN.2016.069
- Naor, M., & Shamir, A. (1995). Visual cryptography. In *Advances in CryptologyEUROCRYPT'94*. Springer. doi:10.1007/BFb0053419
- Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11), 612–613. doi:10.1145/359168.359176
- Wang, D., Zhang, L., Ma, N., & Li, X. (2007). Two secret sharing schemes based on Boolean operations. *Pattern Recognition*, 40(10), 2776–2785. doi:10.1016/j.patcog.2006.11.018
- Wang, G., Liu, F., & Yan, W. Q. (2016). Basic visual cryptography using braille. *International Journal of Digital Crime and Forensics*, 8(3), 85–93. doi:10.4018/IJDCF.2016070106
- Wang, Z., Arce, G. R., & Di Crescenzo, G. (2009). Halftone visual cryptography via error diffusion. *IEEE Transactions on Information Forensics and Security*, 4(3), 383–396. doi:10.1109/TIFS.2009.2024721
- Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4), 600–612. doi:10.1109/TIP.2003.819861 PMID:15376593
- Weir, J., & Yan, W. (2010). A comprehensive study of visual cryptography. In *Transactions on DHMS V* (pp. 70–105). Springer.
- Wu, X., & Sun, W. (2012). Visual secret sharing for general access structures by random grids. *IET Information Security*, 6(4), 299–309. doi:10.1049/iet-ifs.2012.0046
- Yan, W., Ding, W., & Dongxu, Q. (2000). Image sharing based on Chinese remainder theorem. *J. of the North China Univ. of Tech.*, 12, 6–9.
- Yan, X., Liu, X., & Yang, C.-N. (2015a). An enhanced threshold visual secret sharing based on random grids. *Journal of Real-Time Image Processing*. doi:10.1007/s11554-015-0540-4
- Yan, X., & Lu, Y. (2017). Progressive visual secret sharing for general access structure with multiple decryptions. *Multimedia Tools and Applications*, 1–20.
- Yan, X., Lu, Y., Liu, L., Wan, S., Ding, W., & Liu, H. (2017a). Chinese remainder theorem- based secret image sharing for (k, n) threshold. In X. Sun, H.-C. Chao, X. You, & E. Bertino (Eds.), *Cloud Computing and Security: Third International Conference, ICCCS 2017, Revised Selected Papers, Part II* (pp. 433–440). Cham: Springer. doi:10.1007/978-3-319-68542-7_36
- Yan, X., Lu, Y., Liu, L., Wan, S., Ding, W., & Liu, H. (2017b). Exploiting the homomorphic property of visual cryptography. *International Journal of Digital Crime and Forensics*, 9(2), 45–56. doi:10.4018/IJDCF.2017040105

Yan, X., Lu, Y., Liu, L., & Wang, S. (2018). Partial secret image sharing for (k,n) threshold based on image inpainting. *Journal of Visual Communication and Image Representation*, 50, 135–144. doi:10.1016/j.jvcir.2017.11.012

Yan, X., Wang, S., & Niu, X. (2014). Threshold construction from specific cases in visual cryptography without the pixel expansion. *Signal Processing*, 105, 389–398. doi:10.1016/j.sigpro.2014.06.011

Yan, X., Wang, S., Niu, X., & Yang, C.-N. (2015b). Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. *Digital Signal Processing*, 38, 53–65. doi:10.1016/j.dsp.2014.12.002

Yang, C.-N., & Ciou, C.-B. (2010). Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. *Image and Vision Computing*, 28(12), 1600–1610. doi:10.1016/j.imavis.2010.04.003

Xuehu Yan was born in February 1984, in China, and received a B.Sc. degree with honor rank in Science in Information & Calculate Science, China in 2006, an M.Sc. degree in Computational Mathematics in 2008, and a doctoral degree in Computer Science and Technology in 2015 from the Harbin Institute of Technology. He is now a lecturer at the National University of Defense Technology, Hefei, P. R. China. His areas of interests are visual cryptography, cryptography, and multimedia security.

Yuliang Lu was born in 1964, in China, and received a B.Sc. degree with honor rank in Computer Application, in 1985 and an M.Sc. degree in Computer Application in 1988 from Southeast University. He is now a professor at the National University of Defense Technology, Hefei, P. R. China. His areas of interests are computer applications and information processing.

Lintao Liu was born in December 1989, in China, and received a B.Sc. degree with honor rank in Computer Application, in 2012, an M.Sc. degree in Information Security in 2015 from the National University of Defense Technology. He is now a PhD candidate at the National University of Defense Technology, Hefei, P. R. China. His areas of interests are cryptography, multimedia security, and biometrics.