Displays 39 (2015) 80–92

Contents lists available at ScienceDirect

Displays

journal homepage: www.elsevier.com/locate/displa

Visual multiple-secret sharing for flexible general access structure by random grids

Kai-Hsiang Tsao [a], Shyong-Jian Shyu [b], Chih-Hung Lin [c], Yao-Sheng Lee [a], Tzung-Her Chen [a,*]

[a] Dept. of Computer Science and Information Engineering, National Chiayi University, Chiayi 600, Taiwan, ROC
[b] Dept. of Computer Science & Information Engineering, Ming Chuan University, Taoyuan County 333, Taiwan, ROC
[c] Graduate Institute of Mathematics and Science Education, National Chiayi University, Chiayi 621, Taiwan, ROC

ARTICLE INFO

Article history:
Received 4 September 2014
Received in revised form 12 August 2015
Accepted 2 September 2015
Available online 8 September 2015

Keywords:
Random grids
Visual secret sharing
Visual cryptography
General access structures

ABSTRACT

For visual secret sharing (VSS), general access structure (GAS), which can freely define the qualified set and the forbidden set, provides dealers the ability to share secret information with the qualified set but not the forbidden set. In previous studies, the proposed GAS schemes have focused on strong GAS, but it has retained restrictions and inconvenience in some secret-sharing scenarios. Recently, the random-grid-based VSS (RG-based VSS) technique has aimed to overcome the problem of pixel expansion from which the visual-cryptography-based VSS (VC-based VSS) techniques usually suffer. This paper presents a flexible GAS VSS scheme by RG that is appropriate for wide use and that serves special cases like $(2, n)$, (n, n), and (k, n). The paper also outlines how the scheme can be extended for multiple secrets. The performance and the security of the scheme are theoretically analyzed.

1. Introduction

1.1. Background

1.1.1. Threshold VC-based VSS

In 1979, Shamir [16] and Blakley [3] proposed the k-out-of-n secret-sharing scheme, which is used to share secret information by dividing it into n shares and to recover the original secret information later by collecting any of at least k shares. This scheme opened a new era of information security. In 1995, Naor and Shamir [15] proposed a visual secret-sharing scheme based on visual cryptography (VC-based VSS) in which, according to a predefined codebook, a binary secret image can be encoded into n share images. In the decoding phase, by directly stacking at least k shares carefully, the secret information can be reconstructed by human eyes without any extra computational cost required.

1.1.2. Strong GAS VSS

Even though the (k, n)-VC-based VSS technique provides a way to share secrets, it cannot deal with arbitrary access structures. To compensate for this drawback, Ateniese et al. [1] extended (k, n)-VC-based VSS to general access structures (GAS) in 1996, in which an access structure is defined by the form $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$, where Γ_{Qual} denotes a set of qualified sets and Γ_{Forb} a set of forbidden sets.

Thus, a VSS scheme that realizes such an access structure is denoted as a $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$-VC-based VSS. A $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$-VC-based VSS can split a binary image into n shares, such that any qualified set $Q \in \Gamma_{\mathrm{Qual}}$ of participants/shares can recover the secret image, whereas no forbidden set $F \in \Gamma_{\mathrm{Forb}}$ of participants/shares can extract any secret information.

Let $\mathsf{N} = \{1, 2, \ldots, n\}$ be a set of n shares, and let $\mathsf{P}(\mathsf{N})$ denote the set of all subsets of N, i.e., the power set of N. Let $\Gamma_{\mathrm{Qual}} \subseteq \mathsf{P}(\mathsf{N})$ and $\Gamma_{\mathrm{Forb}} \subseteq \mathsf{P}(\mathsf{N})$, where $\Gamma_{\mathrm{Qual}} \cap \Gamma_{\mathrm{Forb}} = \varnothing$. We call members of Γ_{Qual} *qualified* sets, and call members of Γ_{Forb} *forbidden* sets. Any qualified set $Q \in \Gamma_{\mathrm{Qual}}$ of shares can be used to recover the secret image, whereas no forbidden set $F \in \Gamma_{\mathrm{Forb}}$ of shares can be used to recover any secret information. The pair $(\Gamma_{\mathrm{Qual}}, \Gamma_{\mathrm{Forb}})$ is called the access structure on N. For $A \subseteq \mathsf{P}(\mathsf{N})$, we say that A is monotone increasing if, for any $B \in A$ and any $C \subseteq \mathsf{N}, B \cap C = \varnothing$, we have $B \cup C \in A$. That is, any superset of a set belonging to A is also in A. We say that A is monotone decreasing if, for any $B \in A$ and any $C \subseteq B, B \setminus C \in A$. That is, any subset of a set belonging to A is also in A. To highlight the robustness of GAS, the following definition describes strong GAS VSS.

Definition 1 (*Strong GAS*). We say that the GAS is *strong* given a GAS that satisfies the following conditions:

(a) Γ_{Qual} is monotone increasing,
(b) Γ_{Forb} is monotone decreasing, and
(c) $\Gamma_{\mathrm{Qual}} \cup \Gamma_{\mathrm{Forb}} = \mathsf{P}(\mathsf{N})$. □

[*] Corresponding author.
E-mail address: thchen@mail.ncyu.edu.tw (T.-H. Chen).

http://dx.doi.org/10.1016/j.displa.2015.09.001
0141-9382/© 2015 Elsevier B.V. All rights reserved.

Example 1 (*Strong GAS*). Let $\mathsf{N} = \{1, 2, 3\}$ be the set of shares. Suppose that the sets {1, 2}, {1, 3} and {1, 2, 3} can be used to decode the secret image. However, the set {2, 3} and any one share must not leak out any information about the secret image. This access structure can be represented as $\Gamma_{\text{Qual}} = \{\{1,2\},\{1,3\},\{1,2,3\}\}$ and $\Gamma_{\text{Forb}} = \{\{1\},\{2\},\{3\},\{2,3\}\}$. In this way, Γ_{Qual} is monotone increasing—that is, it satisfies that we have the subsets {1, 2} and {1, 3} such that Γ_{Qual} must include {1, 2, 3}—and Γ_{Forb} is monotone decreasing—that is, it satisfies that we have {2, 3} such that Γ_{Forb} must include {2} and {3}. Since $\Gamma_{\text{Qual}} \cup \Gamma_{\text{Forb}} = \mathsf{P}(\mathsf{N})$, this GAS is *strong*. □

1.2. Motivation

1.2.1. Flexible GAS VSS

Unfortunately, the "strong" properties of monotone increasing in Γ_{Qual} and monotone decreasing in Γ_{Forb} (see Definitions 1(a) and (b), respectively) are too tight to reflect some practical applications in which such properties are unnecessary. In Example 1, the qualified subset {1, 2, 3} is necessarily defined for strong GAS if {1, 2} and {1, 3} $\in \Gamma_{\text{Qual}}$. For some applications, this may be an inconvenient restriction.

Hence, the authors re-define a flexible GAS to relax the restriction of strong GAS, as shown in Definition 2. The flexible GAS is more flexible and practical in VSS applications than the strong GAS.

Definition 2 (*Flexible GAS VSS*). Given a GAS that satisfies $\Gamma_{\text{Qual}} \cup \Gamma_{\text{Forb}} = \mathsf{P}(\mathsf{N})$, we say the access structure is *flexible*. □

Example 2 (*Flexible GAS*). Let $\mathsf{N} = \{1, 2, 3, 4\}$ be the set of shares $\Gamma_{\text{Qual}} = \{\{1,2\},\{1,3\},\{1,4\},\{2,4\},\{1,2,3\},\{1,2,4\}\}$ and $\Gamma_{\text{Forb}} = \{\{1\},\{2\},\{3\},\{4\},\{2,3\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\}$. In this case, Definitions 1(a) and (b) are removed because they are not necessary in our flexible scenario. □

This design lights on the possibility of scenario that three close friends, say Participants 1, 2 and 4, don't want to share the secret, sharing among them, to Participant 3.

Compared with (k, n)-VC-based VSS, $(\Gamma_{\text{Qual}}, \Gamma_{\text{Forb}})$-VC-based VSS, which can be regarded as a generalization of the threshold scheme, provides more flexibility in sharing secrets. Recently, many researchers have focused on the visual secret-sharing schemes for general access structures [2,9–12,23].

1.2.2. RG-based VSS

VC-based VSS may have two main drawbacks: (1) the sophisticated codebook needed to be predefined and (2) the pixel expansion problem. Thanks to another VSS scheme proposed by Kafri and Keren [13] in 1987, the random-grid-based VSS (RG-based VSS) is used to encode a secret image into two noisy random grids and decode the secret by directly stacking two random grids. Today, RG-based VSS has been conferred again and further extended to the threshold VSS, such as (2, n), (n, n) [4,6] and (k, n) [7] VSS, without the two drawbacks mentioned above.

1.3. Contribution

With RG-based VSS still in its infancy, the authors propose a flexible general access structure visual secret-sharing scheme by random grids, in which the (2, n), (n, n), and (k, n) schemes are covered as special cases. The proposed scheme is more flexible and practical for VSS applications than those in previous work. The experimental results demonstrate that the proposed scheme is feasible, and the theoretical analysis in terms of performance and security is demonstrated.

As many studies have been focused on multiple secrets, whether VC-based VSS [5,8,10,11,14,18,20–22] or RG-based VSS [5], this paper also outlines how the proposed scheme can be extended for multiple secret sharing to benefit from saving the data transmission bandwidth and decreasing the storage requirement.

The rest of the paper is organized as follows. The traditional random-grid VSS scheme is briefly described in the next section. Section 3 describes the details of the proposed flexible GAS RG-based VSS scheme. Sections 4 and 5 show the formal analysis and the experimental results. The extended method for multiple-secret RG-based VSS is demonstrated in Section 6. Conclusions are provided in the final section.

2. Review of RG-based VSS

This section describes the traditional random grids algorithms proposed by Kafri and Keren [13] in 1987. The binary secret image S with the size of $h \times w$ is encoded into two random grids R_1 and R_2 with the same size as that of S.

First, we randomly generate the value 0 and 1 to indicate the color white or black and assign them to each pixel of the first random grid R_1. Next, the other random grid R_2 is created by referring both the corresponding pixels of secret image S and those of R_1 to one of Kafri and Keren's three algorithms. The function $f_{ran}(0, 1)$ is the coin-flip function that generates randomly the value 0 or 1, $f_{equ}(x)$ and $f_{com}(x)$, output as the same value of x and the inverse of x, respectively. Kafri and Keren's three algorithms are given in Algorithms 2.1, 2.2 and 2.3. The reader may refer to Ref. [13] for details.

```
Input: A binary secret image $S = \{S[i,j] | S[i,j] \in 0 \text{ or } 1, 1 \leqslant i \leqslant h,$
    $1 \leqslant j \leqslant w\}$
Output: Two random grids $R_1 = \{R_1[i,j] | R_1[i,j] \in 0 \text{ or } 1,$
    $1 \leqslant i \leqslant h, 1 \leqslant j \leqslant w\}$ and $R_2 = \{R_2[i,j] | R_2[i,j] \in 0 \text{ or } 1,$
    $1 \leqslant i \leqslant h, 1 \leqslant j \leqslant w\}$

Algorithm 2.1
//Step 2.1-1 Generating the first random grid $R_1$
For $i$ = 1 to $h, j = 1$ to $w$
    $R_1[i,j] = f_{ran}(0,1)$
//Step 2.1-2 Generating the second random grid $R_2$
For $i$ = 1 to $h, j = 1$ to $w$
//Step 2.1-2.1 Generating the corresponding area in $R_2$ with
    respect to white area in $S$
      If $S[i,j]$ = 0        $R_2[i,j] = f_{equ}(R_1[i,j])$
//Step 2.1-2.2 Generating the corresponding area in $R_2$ with
    respect to black area in $S$
      Else                   $R_2[i,j] = f_{com}(R_1[i,j])$

Algorithm 2.2
//Step 2.2-1 Generating the first random grid $R_1$
For $i$ = 1 to $h, j = 1$ to $w$
    $R_1[i,j] = f_{ran}(0,1)$
//Step 2.2-2 Generating the second random grid $R_2$
For $i$ = 1 to $h, j = 1$ to $w$
//Step 2.2-2.1 Generating the corresponding area in $R_2$ with
    respect to white area in $S$
      If $S[i,j] = 0$        $R_2[i,j] = f_{equ}(R_1[i,j])$
//Step 2.2-2.2 Generating the corresponding area in $R_2$ with
    respect to black area in $S$
      Else                   $R_2[i,j] = f_{ran}(0,1)$

Algorithm 2.3
//Step 2.3-1 Generating the first random grid $R_1$
```

(continued on next page)