Digital Signal Processing 71 (2017) 36–45

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Contrast-improved visual secret sharing based on random grid for general access structure

Xuehu Yan *, Yuliang Lu

Hefei Electronic Engineering Institute, Hefei 230037, China

ARTICLE INFO

Article history:
Available online 6 September 2017

Keywords:
Visual cryptography
Progressive visual secret sharing
Random grid
General access structure
Improved visual quality

ABSTRACT

Random grid (RG)-based visual secret sharing (VSS) owns the advantages of no pixel expansion and codebook design. VSS for general access structure (GAS) possesses wider applications than VSS for (k, n) threshold. Previous RG-based VSS studies for GAS had the drawbacks of "all-or-nothing" or low visual quality. In this paper, we will develop a progressive VSS (PVSS) algorithm for GAS with improved visual quality based on RG. We employ different regions of the secret image and their generated corresponding random bits to improve the visual quality of the revealed secret image as well as to gain GAS with progressive feature, where the random bits are divided into three parts. In addition, our scheme has neither pixel expansion nor codebook design due to RG. We show the effectiveness of our proposed scheme in terms of experiments and analyses.

1. Introduction

Visual secret sharing (VSS) (namely visual cryptography scheme (VCS)) [1,2] encrypts the secret image into different shadow images (also called shares) and then distributes them among the participants. The decryption method of VSS is only based on stacking without any computational device or cryptographic knowledge. VSS may be useful in many scenarios, such as, access control, transmitting passwords, key management, information hiding [3], authentication, watermarking, distributed storage and computing in cloud computing, etc. [4,5].

Naor and Shamir [1] first introduced VSS for (k, n) threshold [6–9]. They share a secret binary image into n noise-like shadow images. We can stack any k or more shadow images based on human visual system (HVS) to recover the original secret image. While less than k shares cannot reveal any information about the secret by inspecting the shares. The main advantage of VSS is simple recovery method, i.e., the decryption of the secret is only by stacking or HVS without any computation. However, the original method has the weaknesses of codebook (basic matrices) design, pixel expansion and no general access structure (GAS) [2].

Some VSS schemes with no pixel expansion were designed to decrease the pixel expansion. Ito et al. [10] realized the probabilistic VSS through equally picking up a column from the basic matrix. Yang [11] gave probabilistic VSS with different thresholds. Cimato et al. [12] realized generalization probabilistic VSS.

Many other researchers pay attention to random grid (RG)-based VSS (RGVSS) [13,14] since RGVSS has neither pixel expansion problem nor codebook design. Kafri and Keren [15] first exploited RG-based encryption for secret binary image, which is encrypted into two random RGs (i.e., shadow images) with the same size as the original secret image. The decryption method is superimposing as well. Following Kafri and Keren's study, some relative schemes were extended to threshold [16] or improve the visual quality [17–19]. Unfortunately, in previous RG-based studies, only case (k, n) is achieved instead of GAS as well as the background may be darker when we superimpose more shares.

In VSS for GAS, the user can appoint the qualified participants combinations that can recover the secret, i.e., a specification of all qualified subsets of participants can be allocated by the user. VSS for GAS [20] possesses wider applications than VSS for (k, n) threshold. Therefore, some RGVSS schemes for GAS were researched. By utilizing (k, n) threshold, Wu and Sun [21], and Kumar and Sharma [22] achieved VSS for GAS, respectively. Through employing the collection of maximal forbidden sets and the basis set, Shyu [23] presented two RGVSS construction methods for GAS. Unfortunately, the above RGVSS schemes for GAS owe the shortcomings of low visual quality, "all-or-nothing" or darker background when more shares are collected.

The contribution of this paper is that, we propose RG-based progressive VSS (PVSS) for GAS with improved visual quality. In contrast to "all-or-nothing", PVSS has the merit that, higher visual quality of the recovered secret image will be gained when more

* Corresponding author.
E-mail address: publictiger@126.com (X. Yan).

http://dx.doi.org/10.1016/j.dsp.2017.08.006
1051-2004/

Table 1
Notations used in this paper.

Notations	Descriptions
0 (resp. 1)	A white (resp. black) pixel
S	The secret binary image
$S(0)$ (resp. $S(1)$)	The area of all the white (resp. black) pixels in S
$\otimes$	Stacking (OR) operation
$\oplus$	Boolean XOR operation
$SC_1, SC_2, \ldots, SC_n$	Shares generated by VSS schemes
t	Number of collecting shares in the recovery phase
$SC_{\{i_1,i_2,\ldots,i_t\}}$	Stacked result by shares $SC_{i_1}, SC_{i_2}, \ldots, SC_{i_t}$
$\alpha_{\{i_1,i_2,\ldots,i_t\}}$	Contrast of the revealed secret image from shares $SC_{i_1}, SC_{i_2}, \ldots, SC_{i_t}$ by stacking recovery
$SC[S(0)]$ (resp. $SC[S(1)]$)	The corresponding area of all the white (resp. black) pixels in image SC
$A \cap B (A \cup B, A \backslash B)$	The Intersection (Union, difference) set of sets A and B
$\|A\|$	The element number of a set A
$\exists$ (!) $c_1 \in C : f(c_1)$	There exists (only) c_1 in C satisfying $f(c_1)$
$Prob(x)$	the probability when any event x occurs

shares with the same minimum set are stacked. At location (i, j), for the n bits corresponding to the n shares, we first randomly pick up one minimum qualified subset for each secret pixel. Then different (k_0, k_0) thresholds are applied to obtain progressive property and GAS, where every (k_0, k_0) threshold is performed in parallel. More importantly, five categories are designed and checked for the last $n - k_0$ bits to improve the visual quality of the recovered secret image, where we assume here x bits are modified. Finally, we directly let the last $n - k_0 - x$ bits be white (0) so that to decrease the background darkness. Our designed five categories and white bits are the key differences between our method and related RGVSS schemes for GAS. As a result, we will reveal the secret with improved contrast and progressive property by superimposing for the qualified sets with the same minimum set. Moreover, our scheme has no pixel expansion or codebook design on account of RG. We show the effectiveness of our proposed scheme in terms of experiments and analyses.

We organize the rest of our paper as follows. Section 2 introduces some basic requirements for the proposed scheme. In Section 3, the proposed scheme is illustrated in detail. Section 4 gives the performance analyses of the proposed scheme. Section 5 is dedicated to experimental results. Finally, Section 6 concludes this paper.

2. Preliminaries

Prior to presenting the proposed scheme, we give some VSS and RG-related definitions. Furthermore, Table 1 illustrates notations applied in this paper.

$\{\Gamma_{Qual}, \Gamma_{Forb}\}$ is known as a GAS. [24] gave a general VSS, i.e., the $\{\Gamma_{Qual}, \Gamma_{Forb}\}$-VSS for GAS, which is a specification of all qualified and forbidden subsets (Γ_{Qual} and Γ_{Forb}) of participants. Here Γ_{Qual} and Γ_{Forb} exhibit non-empty subsets of a set $P = \{1, 2, \ldots, n\}$, where $i \in [1, n]$ means a participant with the order number of "i", $\Gamma_{Qual} \subseteq 2^P$, $\Gamma_{Forb} \subseteq 2^P$ and $\Gamma_{Qual} \cap \Gamma_{Forb} = \phi$. Any set $X = \{i_1, i_2, \ldots, i_r\} \in \Gamma_{Qual}$, where participants $i_1, i_2, \ldots, i_r \in P$, can reveal the secret image while any set $X \in \Gamma_{Forb}$ reveals nothing of the secret, which illustrates the security of VSS for GAS.

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

$$\Gamma_0 = \left\{ Q \in \Gamma_{Qual} \middle| Q' \notin \Gamma_{Qual}, \forall Q' \subset Q \right\} \tag{1}$$

where each element of Γ_0 is one minimum qualified set, i.e., there is not any qualified set less than the element of Γ_0.

Participant $p \in P$ is called an essential participant if $\{A | A \cup \{p\} \in \Gamma_{Qual}, A \notin \Gamma_{Qual}\} \neq \phi$, where A indicates any subset of P. $p \in P$ is an essential participant tells that at least one subset of P needs to contain p to be a qualified set. We say a GAS is strong and Γ_0 is a basis if Γ_{Qual} is monotone increasing and Γ_{Frob} is monotone decreasing. In the following of this paper, we assume that all the participants are essential and the GAS is strong. Progressive feature for a strong GAS indicates that, for the qualified subsets with the same minimum set, when more shares are stacked, higher visual quality of the reconstructed secret image will be obtained.

In addition, for generating a secret bit, when a certain minimum set is applied and if two participants can switch their order in an access structure, we say they are equivalent. Here, we introduce the definition that any two participants are equivalent as follows.

Definition 1 *(Equivalent participants).* When $A \in \Gamma_0$ is selected as the current selected minimum qualified set, we say participant c_i is equivalent to participant a_i in A about Γ_0 if $c_i \cup \{A \backslash a_i\} \in \Gamma_{Qual}$, denoted as $c_i \sim a_i|_A$, where $a_i \in A$ and $c_i \notin A$.

In the proposed scheme, some random pixels are employed to generate the shares, therefore, some definitions for RGVSS are given as follows.

Definition 2 *(Average light transmission, denoted as T).* For a certain pixel s in a binary image S with size of $M \times N$, the light transmission of a transparent (resp. opaque) pixel is given as $T(s) = 1$ (resp. $T(s) = 0$). In addition, the average light transmission of S is as follows

$$T(S) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} T(S(i, j))}{M \times N} \tag{2}$$

The average light transmission of S indicates the white (transparent) pixels probability in S.

Definition 3 *(Contrast, denoted as α).* The visual quality of the revealed secret image S' corresponding to the secret image S is evaluated by contrast, which is defined as follows.

$$\alpha = \frac{T\left(S'[S(0)]\right) - T\left(S'[S(1)]\right)}{1 + T(S'[S(1)])} \tag{3}$$

Contrast can decide how well human eyes will recognize the revealed secret, so that it is expected to be as high as possible to gain better visual quality. About how the contrast values map to reconstruction quality, please refer to [25]. Herein, to give readers some intuitions about the expected performance, we give some example images with their corresponding contrast values in Fig. 1. According to Fig. 1 and [25], from practical respects we know that.

1. When $\alpha \in [0, 0.03]$, we cannot recognize the secret image.
2. When $\alpha \in (0.03, 0.14]$, we can see a little information of the secret image.
3. When $\alpha \in (0.14, 0.21]$, the secret image will be recognized with acceptable visual quality.
4. When $\alpha \in (0.21, 1]$, the secret image will be fast recognized with good visual quality.

Definition 4 *(Visually recognizable).* The recovered secret image S' could be revealed as the corresponding original secret image S in theory if $\alpha > 0$ when S' is recovered from an element of Γ_{Qual} [1].

Definition 5 *(Security).* The scheme is secure if $\alpha = 0$ when S' is recovered from an element of Γ_{Forb}, which implies no information of S could be revealed through S' [1] in theory.