Digital Signal Processing ••• (••••) •••–•••

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Random-grid based progressive visual secret sharing scheme with adaptive priority

Her-Chang Chao [a], Tzuo-Yau Fan [b,*]

[a] Department of Computer Science and Information Engineering, Ming Chuan University, Taoyuan, Taiwan
[b] Department of Electronic Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Visual secret sharing
Visual cryptography
Progressive
Priority
Random grid

ABSTRACT

This paper describes a random-grid-based progressive visual secret sharing scheme, wherein the priority weighting of each share can be adjusted. In this scheme, shares are recovered progressively to obtain a secret image. Therefore, with increasing number of shares that are collected, more information of the secret image is recovered, and vice versa. In addition, each user participating in the secret sharing can adjust the priority weighting of a share based on their determined level of secrecy; thus, each share generated by the proposed scheme has a different priority weighting value. During decryption, depending on the priority weightings of the stacked shares, the secret image can be recovered to different extents. Further, the priority level of these shares cannot be distinguished based on the average light transmission of the reconstructed image, thereby guaranteeing high security.

1. Introduction

In 1995, Naor and Shamir proposed a visual secret sharing (VSS) scheme for encoding secret images [1]. This scheme encodes a secret image into n noise-like images (also called shares), and the shares do not reveal any information regarding the secret image. During the recovery of the secret image, when $k(\leq n)$ shares are stacked, the secret image can be recognized by visually inspecting the difference in the brightness of the black and white pixels in the stacked image. Therefore, this scheme does not require complex computations. This is known as the (k, n)-threshold VSS scheme.

A VSS scheme typically has the following characteristics [1–3]: (a) it requires encoding matrices (or codebooks) to construct the pixels of the shares. (b) It involves pixel expansion, and different encoding matrices result in different levels of pixel expansion in the shares. (c) The shares are noise-like images; a single share cannot reveal any information about the secret image, and thus the secret messages cannot be recognized visually. On the basis of the aforementioned characteristics, researchers have extended the VSS scheme technology by using different approaches, such as increasing the number of the secret images being shared [4,5], sharing secret messages through various media [6], and enhancing the quality of the recovered secret images [7]. In addition, the safety and simplicity of the VSS scheme led to its application to different areas of study, such as digital watermarking [8,9] and visual authentication [10].

Progressive visual secret sharing (PVSS) scheme is a different concept of secret sharing [11–18]. In a PVSS scheme, the secret image is encoded into many shares. The number of shares that are stacked determines the number of secret messages recovered during decryption. Therefore, with increasing number of shares that are stacked, the clarity of the recovered secret image improves. Conversely, when fewer shares are stacked, the recovered image is less clear. Thus, a secret image is recovered progressively through the PVSS scheme. Fang and Lin proposed a PVSS scheme that requires pixel expansion [11]. In this scheme, a secret image is first converted into a halftone image. If the pixel of the converted secret image is black, it is then expanded into a fully black 2×2 block. If the pixel is white, it is expanded into a 2×2 block with two black dots and two white dots. After all the pixels are expanded, the halftone image is transformed into a basis image. Subsequently, in this basis image, each pixel value is arbitrarily assigned to a corresponding area on the shares. Although this scheme fulfills the goal of progressively recovering the secret image, the recovery requires pixel expansion, and the messages in the secret image are not easily recovered. Wang proposed another type of PVSS scheme called region incrementing visual secret sharing (RIVSS) [12]. Wang's scheme splits the content of a secret image into multiple regions and assigns a level of secrecy to

* Corresponding author.
E-mail addresses: herchang@mail.mcu.edu.tw (H.-C. Chao), yaufan0625@gmail.com (T.-Y. Fan).

http://dx.doi.org/10.1016/j.dsp.2017.05.009
1051-2004/

each region. When more shares are stacked, the number of the secret regions recovered corresponds to the secrecy levels assigned. However, in Wang's scheme, the extent of the secret regions being revealed affects the extent of pixel expansion.

To avoid the problems associated with pixel expansion, Hou and Quan proposed a PVSS scheme that does not involve pixel expansion [13]. Before generating shares, this scheme creates two $n \times n$ encoding matrices, $\mathbf{C}_0$ and $\mathbf{C}_1$, as shown in (1). In (1), n denotes the number of shares; $\mathbf{C}_0$ is a matrix where the elements in the first row are all equal to 1, whereas the other elements are equal to 0; and $\mathbf{C}_1$ is a matrix where the elements in the main diagonal are all equal to 1, whereas the other elements are equal to 0. In these two matrices, 1 denotes a black pixel and 0 denotes a white pixel.

$$\mathbf{C}_0 = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}_{n\times n} ; \quad \mathbf{C}_1 = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}_{n\times n} \tag{1}$$

By using the pixel values of a secret image, this PVSS scheme randomly assigns a row of elements in $\mathbf{C}_0$ or $\mathbf{C}_1$ to the corresponding pixel values of the shares. In this secret image, the white pixels are encoded by $\mathbf{C}_0$ and the black pixels are encoded by $\mathbf{C}_1$. Although this scheme does not require pixel expansion, it has to create and store the encoding matrices that are generated. In the Wang's scheme [12], this method could achieve a RIVSS scheme, their adoption of expanding pixels meant that more storage space is needed. Shyu and Jiang [14] addressed this problem by proposing a RIVSS scheme where the encoding matrices require smaller pixel expansion. Their scheme minimizes the pixel expansion of the shares and thus reduces the burden of storing the encoding matrices. Hou and Quan proposed a PVSS scheme that divides a secret image into several blocks for decryption [15]. However, this scheme requires several encoding matrices to generate the shares and assigns a different matrix to each block in the secret image. Thus, when more shares are stacked, the messages of secret image in different blocks are recovered progressively.

Hou et al. [16] successfully implemented a PVSS scheme where no pixel expansion was required, wherein each share was assigned different priorities. This scheme assigns different levels of secrecy to the shares; therefore, each share has a different level of priority, which determines the number of messages in the secret image that can be revealed. Shares with a higher priority can be used to recover more messages in the secret image, and vice versa. In the PVSS scheme proposed by Hou et al. [16], the average light transmission of each share is not identical; thus, the priority level of the share can be obtained through its average light transmission. The priority level determines the number of messages in the secret image that can be recovered. Yang et al. [18] proposed a modified version of Hou et al.'s PVSS mechanism [16], wherein the average light transmission of each generated share remains identical, thereby preventing the visual recognition of the priority weighting of each share. However, a codebook is required when generating shares by using this mechanism.

In this paper, we describe a novel random grid-based progressive visual secret sharing scheme (RGPVSS) where the level of priority can be adjusted. In the proposed scheme, the pixel values of the shares are classified into different location sets. Each location set is assigned a different pixel value, and the number of pixel values is determined by the priority weighting of each share. On the basis of the random grid-based visual secret sharing (RGVSS) scheme proposed by Kafri and Keren [19], the proposed scheme generates shares with different priority weightings by encoding the assigned pixel values to different location sets in the secret image. The proposed scheme has the following features: (a) each generated share does not result from pixel expansion, and has the same size as the original secret image. (b) The generated shares are assigned with different priority weightings, which can be adjusted by the users participating in the secret sharing process. (c) The average light transmission of each generated share is 1/2, thereby preventing the revelation of the priority weighting from any of these shares. (4) This scheme does not require an encoding matrix to generate shares.

The remainder of this paper is organized as follows. In the next section, we introduce related work. In Section 3, the random-grid based progressive visual secret sharing scheme with adaptive priority is described. The experimental results are described in Section 4. In Section 5, we provide our concluding remarks.

2. Related work

In this section, we introduce Kafri's RGVSS scheme [19] in Section 2.1 and Hou's PVSS scheme [16] in Section 2.2.

2.1. Kafri's RGVSS scheme

In 1987, Kafri and Keren proposed RGVSS [19], in which three simple algorithms were designed to encrypt a binary secret image S using two random grids R_1 and R_2.R_1 and R_2 look like noise images; R_1 and R_2 do not reveal any information related to S, yet S can be recovered by collecting and superimposing R_1 and R_2. The steps of the three algorithms are as follows:

Input: Binary secret image S of size $h \times w$.
Output: Two binary random grids R_1 and R_2, both of size $h \times w$.

RGVSS Algorithm 1.

Step 1: Generate the pixels of R_1 using *random_pixel*().
// *random_pixel*() can return a pixel value of 0 or 1 with equal probability.
Step 2: For each pixel $s(i, j)$ of S and $r_1(i, j)$ of R_1, determine the pixel $r_2(i, j)$ using the following rule:

$$r_2(i,j) = \begin{cases} r_1(i,j), & \text{if } s(i,j) = 0 \text{ (white pixel)} \\ \overline{r_1(i,j)}, & \text{otherwise} \end{cases}$$

Step 3: Output R_1 and R_2.

Where — denotes the Boolean NOT operation.

RGVSS Algorithm 2.

Step 1: Generate the pixels of R_1 using *random_pixel*().
Step 2: For each pixel $s(i, j)$ of S and $r_1(i, j)$ of R_1, determine the pixel $r_2(i, j)$ using the following rule:

$$r_2(i,j) = \begin{cases} r_1(i,j), & \text{if} s(i,j) = 0 \\ \textit{random\_pixel}(), & \text{otherwise} \end{cases}$$

Step 3: Output R_1 and R_2.

RGVSS Algorithm 3.

Step 1: Generate the pixels of R_1 using *random_pixel*().
Step 2: For each pixel $s(i, j)$ of S and $r_1(i, j)$ of R_1, determine the pixel $r_2(i, j)$ using the following rule:

$$r_2(i,j) = \begin{cases} \textit{random\_pixel}(), & \text{if } s(i,j) = 0 \\ \overline{r_1(i,j)}, & \text{otherwise} \end{cases}$$

Please cite this article in press as: H.-C. Chao, T.-Y. Fan, Random-grid based progressive visual secret sharing scheme with adaptive priority, Digit. Signal Process. (2017), http://dx.doi.org/10.1016/j.dsp.2017.05.009