J. Vis. Commun. Image R. 33 (2015) 31–41

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Friendly progressive random-grid-based visual secret sharing with adaptive contrast[☆,☆☆]

Chih-Hung Lin[a], Yao-Sheng Lee[b], Tzung-Her Chen[b,*]

[a] *Graduate Institute of Mathematics and Science Education, National Chiayi University, Chiayi 621, Taiwan, ROC*
[b] *Department of Computer Science and Information Engineering, National Chiayi University, Chiayi 600, Taiwan, ROC*

ARTICLE INFO

Article history:
Received 19 August 2014
Accepted 31 August 2015
Available online 8 September 2015

Keywords:
Visual secret sharing
Random grid
Pixel expansion
Friendly
Progressive
Chaos
Adaptive contrast
Visual cryptography

ABSTRACT

Visual secret sharing (VSS) schemes providing secret communication services are classified into two categories depending on the method of encoding the secret: visual cryptography (VC)-based and random grid (RG)-based schemes. A friendly progressive version of the VC-based VSS scheme was presented in 2008; however, it is marred by pixel expansion, which is the innate deficiency of conventional VC-based VSS schemes. This paper proposes a suitable user-friendly RG-based VSS scheme with progressive secret reconstruction and without pixel expansion. The experimental results of the developed scheme validated its feasibility, and a theoretical analysis demonstrated its visual quality and security.

1. Introduction

Visual secret sharing (VSS) has attracted considerable attention in academia, and an increasing number of VSS applications, such as image encryption [1], visual authentication [2], image hiding [3], and digital watermarking [4], have been developed. Naor and Shamir [4] first proposed visual cryptography (VC) in 1994. VC can encode a secret image into numerous meaningless shared images, where each shared image alone does not reveal any information about the secret. Specifically, Naor and Shamir presented a *k-out-of-n* (k,n)-VSS concept that entails dividing a secret image into n shares, and reconstructing the original image requires stacking at least k shares. However, conventional VC-based VSSs have several drawbacks. Three of the major drawbacks are outlined as follows: (1) pixel expansion, (2) requirement of a sophisticated codebook designed for various applications, and (3) management of increasingly meaningless shares.

Managing an increasing number of meaningless shares is challenging because all shares for different secrets available are noise-like and are therefore difficult to manage or use and require careful labeling and storage. To manage a high number of meaningless shares, Ateniese et al. [6] proposed an extended VC scheme that involves encoding a secret into numerous meaningful shares. A meaningful share implies that a logo message used for identification appears on the share. Thus, managing the shares is easy. Zhou et al. [7] proposed a halftone VC to achieve meaningful shares. The sizes of the encoded shared images obtained using both extended VC [6] and halftone VC [7] were at least four times larger than those of secret images. To mitigate this problem, Tsai et al. [8] proposed a VC-based VSS scheme to generate meaningful shares; in this scheme, the pixel expansion was reduced to two, achieving higher meaningfulness and lower pixel expansion rate compared with schemes presented in previous studies [6,7].

Although the aforementioned VSS schemes can completely reveal the original secrets, they cannot achieve the goal of progressive image sharing, in which the more shared images are superimposed, the higher the quality of the recovered secret becomes. Jin et al. [9] proposed the first progressive VC scheme. However, this method requires extra computation, which violates the essential assumption of VSS. Fang and Lin [10] proposed another VC-based progressive method, which did not require extra computation; nevertheless, pixel expansion was four times higher compared with other methods. To avoid pixel expansion, Hou and Quan [18] presented a progressive VC scheme with unexpanded shares. When the goal of progressive secret reconstruction is achieved, the progressive schemes presented in previous studies [9,10,18] were not user-friendly in managing the meaningless shares.

[☆] This paper has been recommended for acceptance by M.T. Sun.
[☆☆] This work was presented in part at The 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2009), Kyoto, Japan, 2009 [20].
[*] Corresponding author.
E-mail address: thchen@mail.ncyu.edu.tw (T.-H. Chen).

http://dx.doi.org/10.1016/j.jvcir.2015.08.018
1047-3203/© 2015 Elsevier Inc. All rights reserved.

Fang [11] combined the progressive VC-based VSS [10] and friendly VC-based VSS methods to form a new scheme. However, Fang's scheme is marred by a pixel expansion of up to four times.

More recently, researchers have begun to focus on a random grid (RG)-based VSS scheme first proposed by Kafri and Keren [12] in 1987. Inspired by Kafri and Keren's scheme, Shyu [13] proposed two RG-based VSS schemes for managing both gray-level and color images. To remove the limitation of (2,2) RG-based VSS [12,13], Shyu [15] and Chen and Tsao proposed their own $(2,n)$ and (n,n) [14] and (k,n) schemes [17]. The friendly RG-based VSS scheme [19] lacks the design of a progressive secret construction. To meet this requirement, in 2009, Chen and Lee [20] and Chen [21] have presented friendly progressive RG-based VSS schemes. Previous studies have failed to theoretically demonstrate the security and accuracy of VSS schemes in terms of friendliness and progression. Recent studies have not addressed the trade-off in visual quality, called contrast-flexibility trade-off, between reconstructed secrets and logo images obtained through generated RGs.

This paper proposes a friendly and progressive VSS (FPVSS) scheme involving RGs. In this scheme, a contrast-flexibility trade-off between reconstructed secrets and logo images was obtained through generated RGs. Moreover, the FPVSS scheme is superior to existing VSS schemes in terms of user-friendliness and progressive secret reconstruction. The proposed scheme exhibits the following advantages: (1) eliminating pixel expansion, (2) eliminating the necessity of designing a sophisticated codebook, (3) managing shares in an easy and friendly manner, (4) progressively reconstructing the secret, and (5) providing adaptive contrast. Its accuracy was validated through a theoretical analysis, and several experiments were conducted to demonstrate its feasibility.

The remainder of this paper is organized as follows. Section 2 describes the proposed scheme. Sections 3 and 4 demonstrate the performance and experimental results, respectively. Sections 5 and 6 present further discussions and conclusions.

2. Proposed method

In the proposed scheme, a secret image S is encoded into n meaningful RGs G_k with distinct logo images L_k. A secret image $S = \{S[i,j]|S[i,j] = 0 \text{ or } 1, 0 \leqslant i \leqslant (w-1), 0 \leqslant j \leqslant (h-1)\}$, and n logo images $L_k = \{L_k[i,j]|L_k[i,j] = 0 \text{ or } 1, 0 \leqslant i \leqslant (w-1), 0 \leqslant j \leqslant (h-1)\}$ $(k = 1, 2, \ldots, n)$, serving as references for the generated shared images, are used as inputs. The value 0 or 1 is adopted to represent a transparent or an opaque pixel. The proposed scheme outputs n meaningful RGs $G_k = \{G_k[i,j]|G_k[i,j] = 0 \text{ or } 1, 0 \leqslant i \leqslant (w-1), 0 \leqslant j \leqslant (h-1)\}$ $(k = 1, 2, \ldots, n)$ of the same size.

In the decoding phase, the staking of any two of the RGs reveals the secret, and the two logo images disappear by becoming noise-like. In addition, the higher the number of stacked RGs is, the higher the quality of the secret becomes.

2.1. Design guideline

In the proposed scheme, to meet the contrast-flexibility requirement, the parameter t $(1 \leqslant t \leqslant w \times h)$ is designed to control the quality of the logo images and reconstructed secret image. The higher the value of t is, the higher the quality of the reconstructed image becomes. By contrast, the lower the value of t is, the higher the quality of the logo images becomes.

The design concept involves encoding a secret or logo pixel (Fig. 1). To demonstrate this, we must determine the current encoding process used to manage the secret or logo images with the probability determined using the parameter t. If a secret pixel $S[i,j]$ is selected, all n RG pixels $G_k[i,j]$ are generated using the $(2,n)$-based RGVSS [14]. Otherwise, the value of $G_k[i,j]$ equals that of the logo pixel $L_k[i,j]$, and the color of the other $n-1$ grid-pixel values $G_r[i,j]$ $(r = 1, 2, \ldots, n$ but $r \neq k)$ is black.

2.2. Encoding

Before describing the details of the encoding process, we define the required functions as follows.

Definition 1 (*Random pixel value generation function*). ***Chaos*(.):** $r \leftarrow Chaos(n)$, r is the output of function $Chaos(.)$ with input n, where $Chaos(.)$ is the function used to generate a random value r by using a logistic map [16]. The logistic map is defined as follows: $x_{k+1} = 4x_k(1-x_k)$ $x_k \in (0,1)$. In this case, an initial value x_0 is selected as an input, where each value of the random number sequence r is obtained using the equation $r = x_k \times 10^{13} \bmod n$, where $r \in \{0, 1, \ldots, n-1\}$. □

The encoding processes comprise the following steps.

Step 1: Quality: Determine the quality parameter t that makes the grid pixels generated by the secret pixel $S[i,j]$ with probability $\frac{t}{n+t}$ and one of the n logo pixels $L_k[i,j]$ with probability

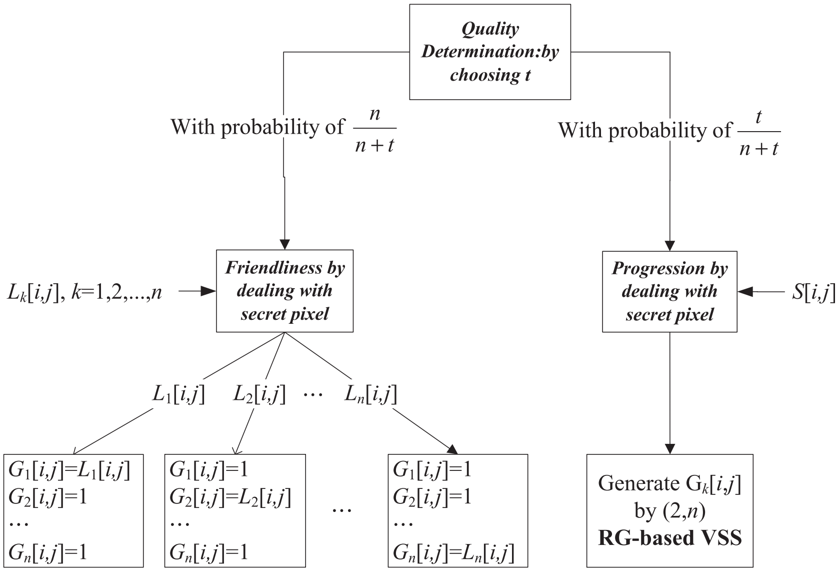
Quality Determination:by choosing t
With probability of $\frac{n}{n+t}$
With probability of $\frac{t}{n+t}$
$L_k[i,j]$, k=1,2,...,n
Friendliness by dealing with secret pixel
Progression by dealing with secret pixel
$S[i,j]$
$L_1[i,j]$ $L_2[i,j]$ ⋯ $L_n[i,j]$
$G_1[i,j]=L_1[i,j]$ $G_2[i,j]=1$ ⋯ $G_n[i,j]=1$
$G_1[i,j]=1$ $G_2[i,j]=L_2[i,j]$ ⋯ $G_n[i,j]=1$
$G_1[i,j]=1$ $G_2[i,j]=1$ ⋯ $G_n[i,j]=L_n[i,j]$
Generate $G_k[i,j]$ by $(2,n)$ RG-based VSS

Fig. 1. The main concept of the proposed scheme for encoding a secret or logo pixel.