Signal Processing 93 (2013) 977–995

Contents lists available at SciVerse ScienceDirect

Signal Processing

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

Improving the visual quality of random grid-based visual secret sharing

Xiaotian Wu [a], Wei Sun [b,*]

[a] School of Information Science and Technology, Sun Yat-sen University, Guangzhou 510006, China
[b] School of Software, Sun Yat-sen University, Guangzhou 510006, China

ARTICLE INFO

Article history:
Received 11 March 2012
Received in revised form
12 November 2012
Accepted 14 November 2012
Available online 23 November 2012

Keywords:
Visual secret sharing
Visual quality
Random grid
Contrast
Void-and-cluster

ABSTRACT

Pixel expansion and visual quality of the revealed secret image are two major concerns in visual secret sharing (VSS). Random grid (RG) is an alternative approach to solve the pixel expansion problem by making the share as big as the original secret image, at the expense of sacrificing the visual quality of the reconstructed secret image. In this paper, two algorithms, including a contrast-enhanced RG-based VSS and a void-and-cluster-based (VAC-based) post-processing, are introduced to improve the reconstructed image quality. Experimental results and theoretical analysis are provided, illustrating that competitive visual quality is obtained by combined use of the two proposed methods.

1. Introduction

With the rapid development of multimedia technology, digital images are easily obtained and manipulated. The security of digital image becomes a concerned problem to be solved. To protect the images, techniques such as image encryption [1–3], data hiding [4–6] and watermarking [7,8] are proposed.

Secret image sharing is another technique to solve the security problem for digital images. VSS, which is also called visual cryptography (VC), is a significant branch of secret image sharing. It is such an approach to protect a secret image among a group of participants via splitting the secret image into random-looking images (called shares or shadows) and recovering the secret by superimposing sufficient shares.

The basic concept of VSS was proposed by Naor and Shamir in 1995 [9]. Generally speaking, in a (k,n)-threshold VSS, a binary secret image is encrypted into n meaningless shares, which are distributed to n associated participants. When any k or more participants print their shares on transparencies and stack them together, the secret image is visually revealed. However, any $k-1$ or less participants cannot guess any information about the secret by inspecting their shares. Advanced merit of VSS is that the decryption of secret image is completely based on human visual system without the aid of any computational devices.

Based on the pioneer work by Naor and Shamir [9], many investigations on VSS have been conducted. To provide flexible sharing strategies, general access structure (GAS) for conventional VSS was proposed [10,11]. For the aim of generating meaningful shares, extended VSS [12,13] and halftone VSS [14,15] were introduced. For sharing different types of images, constructions for graylevel/color images were presented [16–19]. Misalignment problem of VSS was discussed in [20]. However, most of the above-mentioned conventional VSS schemes still suffer from the following drawbacks:

- Pixel expansion. The output shares are $m \geq 2$ times as big as the original secret image, where m is referred to the pixel expansion.

[*] Corresponding author.
E-mail address: sunwei@mail.sysu.edu.cn (W. Sun).

0165-1684/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2012.11.014

- Code book needed. A code book is required in the encryption phase of VSS. Sometimes, designing a code book for a specific sharing strategy is not trivial.

To construct size invariant shares, probabilistic methods were proposed. Ito et al. [21] introduced a size invariant probabilistic VSS, where each secret pixel is encoded by a column matrix selected from the corresponding basis matrix. Yang [22] proposed a non-expansible probabilistic VSS that adopts column matrices to encrypt the secret pixel. Cimato et al. [23] further extended the model proposed by Yang to form a generalized probabilistic VSS. For $m=1$, their method reduces to the one of Yang's methods [22]. For big enough values of m, for which a deterministic scheme exists, their method reduces to the classical deterministic model.

RG serves as an alternative approach to implement the size invariant VSS. In 1987, three distinct algorithms that employ RG to encrypt a binary image into two shares were proposed by Kafri and Kerenv [24]. Shyu [25] extended the pioneer work by Kafri and Keren to encode a grayscale/color image into two RGs. Later, the same author proposed a RG-based VSS for the (n,n) case [26]. In the same year, RG-based VSS schemes for the $(2,n)$ and (n,n) cases were presented by Chen and Tsao [27]. Recently, Chen and Tsao introduced a more generalized RG-based VSS model for the (k,n) threshold [28]. Other research topics on RG-based VSS such as collusive cheating activities [29] and multi-secret sharing [30] were also proposed. Note that, significant different between probabilistic VSS and RG-based VSS is that code book is not required in RG-based VSS. In addition, designing such a tailor-made code book for specific case is complicated.

Probabilistic VSS and RG-based VSS generate size invariant shares at the expense of sacrificing the visual quality of the reconstructed secret image. In this paper, we (1) extend Chen and Tsao's method [28] to develop a contrast-enhanced RG-based VSS, and (2) propose a VAC-based post-processing to improve the evenness of the reconstructed secret image. Competitive visual quality of the revealed secret image is obtained by combined use of the two proposed methods.

The remaining part of this paper is organized as follows. Section 2 formulates the (k,n) RG-based VSS proposed by Chen and Tsao [28], as well as some definitions on RG. The contrast-enhanced RG-based VSS and VAC-based post-processing are described in Section 3. Experimental results and discussions are illustrated in Section 4. Section 5 concludes our work.

2. RG-based threshold VSS

A RG is defined as a transparency consisting of a two-dimensional array of pixels [24]. Each pixel can be fully transparent (white) or totally opaque (black), and the choice between the alternatives is made by a coin-flip procedure. There is no correlation between the values of different pixels in the array.

In a RG-based (k,n)-threshold VSS, a secret image S is encrypted into n RGs $R_1, \ldots, R_n$. To reveal the secret image, any k or more RGs $R_{i_1}, \ldots, R_{i_k}$ are stacked together directly. Let $\otimes$ denote the Boolean OR operation, the stacked result of $R_{i_1}, \ldots, R_{i_k}$ can be represented by $R_{i_1} \otimes \cdots \otimes R_{i_k}$. Prior to describing the RG-based threshold VSS, some definitions on RG are given as follows, which are borrowed from [25,28]. In addition, digit 0 denotes a white pixel and digit 1 denotes a black pixel in this paper.

Definition 1 (*Average light transmission, Shyu [25]*). For a certain pixel p in a binary image R whose size is $M \times N$, the light transmission of a white pixel is defined as $T(p)=1$. Whereas, $T(p)=0$ for p is a black pixel. Totally, the average light transmission of R is defined as

$$T(R) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} T(R(i,j))}{M \times N}.$$

Definition 2 (*Area representation, Shyu [25]*). Let $S(0)$ (resp. $S(1)$) be the area of all the white (resp. black) pixels in secret image S where $S = S(0) \cup S(1)$ and $S(0) \cap S(1) = \emptyset$. Therefore, $R[S(0)]$ (resp. $R[S(1)]$) is the corresponding area of all the white (resp. black) pixels in the RG R.

Definition 3 (*Contrast, Shyu [25], Chen and Tsao [28]*). The contrast of the reconstructed secret image $S_{i_1 \otimes \cdots \otimes i_k} = R_{i_1} \otimes \cdots \otimes R_{i_k}$ with respect to the original secret image S is

$$\alpha = \frac{T(S_{i_1 \otimes \cdots \otimes i_k}[S(0)]) - T(S_{i_1 \otimes \cdots \otimes i_k}[S(1)])}{1 + T(S_{i_1 \otimes \cdots \otimes i_k}[S(1)])}.$$

Contrast determines how well human eyes can recognize the reconstructed secret image. It is considered to be as large as possible.

Definition 4 (*Visual recognition, Chen and Tsao [28]*). The revealed secret image $S_{i_1 \otimes \cdots \otimes i_k} = R_{i_1} \otimes \cdots \otimes R_{i_k}$ is visual recognizable as the original secret image S by contrast $\alpha > 0$. Precisely, it is $T(S_{i_1 \otimes \cdots \otimes i_k}[S(0)]) > T(S_{i_1 \otimes \cdots \otimes i_k}[S(1)])$. Whereas, it gives no clue about the secret image when $\alpha = 0$.

The RG-based (k,n)-threshold VSS proposed by Chen and Tsao [28] is formulated as follows.

```
**RG-based VSS for $(k,n)$ threshold.** [28]
**Input:** $AM \times N$ binary secret image $S$.
**Output:** $n$ RGs $R_1, \ldots, R_n$.
**Step 1:** For each position $(i,j) \in \{(i,j) | 1 \le i \le M, 1 \le j \le N\}$, repeat Steps 2–5.
**Step 2:** Generate $k-1$ bits $b_u$ $(1 \le u \le k-1)$ by randomly assigning value 0 or 1 to $b_u$.
**Step 3:** Compute the $k$-th bit $b_k$ by

    $b_k = S(i,j) \oplus b_1 \oplus \cdots \oplus b_{k-1}$

where $\oplus$ denotes the Boolean XOR operation.
**Step 4:** Generate $n-k$ bits $b_v$ $(k+1 \le v \le n)$ by randomly assigning value 0 or 1 to $b_v$.
**Step 5:** Randomly rearrange the order the $n$ bits $b_1, \ldots, b_n$, and assign the rearranged $n$ bits to $n$ RGs $R_1(i,j), \ldots, R_n(i,j)$.
**Step 6:** Output the $n$ RGs $R_1, \ldots, R_n$.
```

3. The proposed algorithms

In this section, a contrast-enhanced (k,n) RG-based VSS is introduced, as well as the theoretical analysis on the