J. Vis. Commun. Image R. 23 (2012) 441–453

Contents lists available at SciVerse ScienceDirect

J. Vis. Commun. Image R.

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

Improvements of a two-in-one image secret sharing scheme based on gray mixing model

Peng Li [a,*], Pei-Jun Ma [a], Xiao-Hong Su [a], Ching-Nung Yang [b]

[a] Department of Computer Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China
[b] Department of Computer Science and Information Engineering, National Dong Hwa University, #1, Sec. 2, Da Hsueh Rd., Hualien, Taiwan

ARTICLE INFO

Article history:
Received 7 July 2011
Accepted 5 January 2012
Available online 13 January 2012

Keywords:
Image secret sharing
Visual cryptography
Polynomial-based secret sharing
Gray mixing model
Information hiding
Lagrange interpolation
(*k*,*n*)-threshold scheme
Image processing

ABSTRACT

Yang and Ciou recently proposed a two-in-one image secret sharing scheme (TiOISSS), which can easily preview a vague image by human eyes, but also provide a perfect reconstruction of the original image by computation. However, their scheme cannot recover the lossless image by computation as they claimed. In this paper, we resolve the problem of lossless reconstruction. In addition, we improve the visual quality of the previewed image. Also, we introduce a new definition of contrast to evaluate the visual quality of the previewed image. Compared with Yang and Ciou's TiOISSS, our scheme can gain the lossless secret image and meantime enhance the contrast of previewed image.

1. Introduction

Secure digital imaging is an important and active research area combining methods and techniques coming from cryptography and image processing. The image secret sharing scheme (ISSS) encrypts a secret image into shadow images (referred to be shadows). If shadows are not combined in a prescribed way, the secret information cannot be revealed. ISSS is usually referred to be a (k,n)-threshold ISSS, where $k \leq n$, that a secret image is divided into n shadows distributed to n participants, in which the secret image can only be reconstructed by k or more shadows; but for any $k-1$ or less shadows cannot get any information about the secret image.

An important category of (k,n)-ISSS is visual cryptography scheme (VCS) proposed by Noar and Shamir [1]. In VCS, any k participants may photocopy their shadows on transparencies and stack them on an overhead projector to visually decode the secret through human visual system without any hardware or computation. However, any $k-1$ or fewer shadows cannot retrieve any secret information. The merit of VCS is the stacking-to-see property, while the disadvantages are the large pixel expansion and the low visual quality of the reconstructed image. Many researchers are dedicated on reducing the pixel expansion [2–5] and improving the visual quality of the reconstructed image [6,7]. There were also some VCSs proposed for sharing gray and chromatic secret images by using halftone and color decomposing techniques [8–12]. Since the shadows are noise-like, a malicious intruder may be attracted to such meaningless shadows, and thus the extended VCSs with meaningful shadows were proposed in [13–15]. In addition, there were also some VCSs with specific properties, such as for sharing multiple secret images [16,17], cheating prevention [18–20], XOR-based VCS [21–23]. Up to date there are vast research papers in the literature, and recently a book covering an extensive range of topics related to VCS is published [24].

Another category of ISSS is the polynomial-based image secret sharing scheme (PISSS). Shadows are generated by hiding the secret pixel in the constant term of a $(k-1)$-degree polynomial using Shamir's secret sharing [25]. The secret image can be perfectly reconstructed by Lagrange's interpolation. Thien and Lin [26] embedded the secret pixels in all coefficients in a $(k-1)$-degree polynomial and reduced the shadow size to $1/k$ of the secret image. The less shadow size is more convenient for transmission and storage. Recently, some PISSSs with steganography were proposed to further authenticate the integrity of shadows [27–30]. Compared with VCS, the PISSS can reconstruct the original grayscale image but it needs complex computation.

To achieve the perfect reconstruction of secret image and meantime quickly preview the secret image, the authors in [31,32] designed two-in-one ISSSs (TiOISSS) with two decoding options. The first option is stacking shadows to see a vague reconstructed image like VCS, and the second option is to perfectly reconstruct the original grayscale secret image by Lagrange's interpolation like PISSS.

* Corresponding author. Address: School of Computer Science and Technology, Harbin Institute of Technology, Harbin, Heilongjiang 150001, China. Fax: +86 0451 86413309.
E-mail address: lphit@163.com (P. Li).

1047-3203/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.jvcir.2012.01.003

However, these two TiOISSSs have the large expansion of shadow size, which is not convenient for the storage and transmission. Recently, Yang and Ciou [33] designed a new TiOISSS using the concept of gray mixing model. The shadow size is reduced significantly. It shares a grayscale secret image into n shadows by PISSS, and then embeds the grayscale pixels into the shadows of VCS to get n grayscale shadows. In the first phase of the reconstruction process, one can reconstruct a vague secret image by stacking k grayscale shadows. In the second phase, one can extract k shadows of PISSS from k grayscale shadows in VCS, and then reconstruct the original secret image by Lagrange's interpolation. However, their scheme is not lossless as they claimed that. The shadows of PISSS may be extracted incorrectly in the second phase of the decoding process, and results in a speckled reconstructed image. In addition, there is another weakness of their scheme. The visual quality of the decoded image by stacking shadows is very poor, and one can hardly perceive the information about the secret image.

In this paper, we solve the problem of lossless reconstruction for Yang and Ciou's TiOISSS. Meantime, we also improve the visual quality of the reconstructed image by stacking shadows. A new definition of the contrast is also introduced to evaluate the visual quality. The rest of this paper is organized as follows: Section 2 reviews some related works, including VCS, PISSS and Yang and Ciou's TiOISSS [33]. Weaknesses in Yang and Ciou's TiOISSS are presented in Section 3. In Section 4, we propose the lossless TiOISSS. An enhanced TiOISSS with the high-contrast of the previewed image is presented in Section 5. Experimental results follow in Section 6. Conclusions are drawn in Section 7.

2. Related works

2.1. VCS

The first concept of (k,n)-VCS was introduced by Noar and Shamir [1]. Generally, a VCS is consisted of a pair of collections of $n \times m$ Boolean matrices (C_0, C_1) with entries '1' and '0' denoting black and white sub-pixel, respectively. The matrices in the collections (C_0, C_1) are called share matrices. If the secret pixel is white (resp. black), randomly choose a share matrix in C_0 (resp. C_1) and distribute each row of the share matrix to corresponding shadows as a block of sub-pixels. Let $OR(D|r)$ denotes the 'OR'-ed vector of any r rows of D, and $H(v)$ be the Hamming weight of vector v. For a (k,n)-VCS, the collections of share matrices C_0 and C_1 should satisfy the following conditions:

(a) (*Contrast condition*) For any $D \in C_0$, $H(OR(D|k)) \leqslant l$, whereas for any $D \in C_1$, $H(OR(D|k)) \geqslant h$, where $0 \leqslant l < h \leqslant m$.

(b) (*Security condition*) For any $i_1 < i_2 < \cdots < i_t$ in $\{1,2,\ldots,n\}$ with $t < k$, the two collections of $t \times m$ matrices E_j, $j = 0, 1$, obtained by restricting each $n \times m$ matrix in C_j, $j = 0, 1$, to rows $i_1, i_2, \ldots, i_t$, are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first condition is related to the contrast of the reconstructed image. It implies that stacking any k out of n shadows can recover the secret image (i.e., the gray level of a reconstructed black pixel is higher than the gray level of a reconstructed white pixel). The second condition is called the security condition, which ensures that the (k,n)-VCS provides the perfect security.

Usually, the collection of share matrices C_0 (resp. C_1) can be constructed from a basis matrix B_0 (resp. B_1) by permuting the columns of B_0 (resp. B_1), where B_0 and B_1 are $n \times m$ Boolean matrices.

Example 1. We construct a (2,2)-VCS with $m = 2$, $l = 1$ and $h = 2$, using basis matrices $B_0 = \begin{bmatrix} 10 \\ 10 \end{bmatrix}$ and $B_1 = \begin{bmatrix} 10 \\ 01 \end{bmatrix}$.

It is observed that $H(\mathrm{OR}(D|2)) = 2$ for $D \in C_1$, and $H(\mathrm{OR}(D|2)) = 1$ for $D \in C_0$, and $H(\mathrm{OR}(D|1)) = 1$ for $D \in C_1$, and $H(\mathrm{OR}(D|1)) = 1$ for $D \in C_0$, satisfy contrast and security conditions. For simplicity, we use xByW to represent $(\overbrace{1\cdots1}^{x}, \overbrace{0\cdots0}^{y})$ and its permutations. In a reconstructed image, a black color is 2B0 W and a white color is 1B1 W. Thus, we can visually decode the secret image. Because every 2-subpixel block in shadows is 1B1 W, shadows are noise-like. We take a printed-text image 'Harbin Institute of Technology' (HIT) as the secret image (see Fig. 1(a)). Two shadows are shown in Fig. 1(b) and (c), and the reconstructed image by stacking two shadows is given in Fig. 1(d). The text 'HIT' can be visually recognized by human eyes.

2.2. PISSS

Shamir [25] introduced the (k,n)-threshold secret sharing scheme to share a secret numerical value to n shadows by a $(k-1)$-degree polynomial:

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}) \bmod p \tag{1}$$

in which p is a prime number, a_0 is replaced by the secret value and all other coefficients are random numbers. The n shadows are generated by $(i, f(i))$, $i = 1,2,\ldots,n$. Later, through any k out of n shadows, one can recover the polynomial $f(x)$ by Lagrange's interpolation $f(x) = \sum_{j=1}^{k} f(j) \prod_{i=1, i\neq j}^{k} \frac{(x-i)}{(j-i)} \bmod p$. The secret is obtained as $f(0)$. However, any $k-1$ or fewer shadows cannot get any information about the secret value.

In order to share secret image with small size of shadows, Thien and Lin [26] adopted all coefficients of $f(x)$ to embed the secret pixels. For each time, it can share k secret pixels, and each shadow receives one shadow pixel. Therefore, the shadow size is reduced to $1/k$ of that of the secret image. The prime number p is chosen as 251, which is the largest prime number smaller than 255. Most PISSSs adopt $GF(251)$, an ordinary arithmetic (mod 251), for simple calculation. However, the gray-scale values (>250) should be modified to 250 and results in distortion. In this work, we use Galois field $GF(2^8)$ to embed 256 grayscales in an image to avoid distortion. As we know, using the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$, we may construct $GF(2^8)$. Using 255 = (11111111) and 251 = (11111011) as an example, consider the calculation of 255×251 in $GF(2^8)$. Since $255 = \alpha^{175}$ and $251 = \alpha^{90}$ (i.e., a power of a primitive element α), we have $255 \times 251 = \alpha^{175} \times \alpha^{90} = \alpha^{265} = \alpha^{10}$ (Note: $\alpha^{255} = 1$). In $GF(2^8)$, $\alpha^{10} = \alpha^2 \times \alpha^8 = \alpha^2 \times (\alpha^4 + \alpha^3 + \alpha^2 + 1) = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 = (01110100) = 116$. Thus, we have $255 \times 251 = 116$. On the other hand, the addition in $GF(2^8)$ is same to the addition modular 2, and thus we have $255 + 251 = (11111111) \oplus (11111011) = (00000100) = 4$. In this paper, we construct the polynomial in $GF(2^8)$ to derive a lossless secret image:

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}) \text{ in } GF(2^8). \tag{2}$$

In this way, it can achieve lossless PISSS by directly processing 8-bit pixel values, and the size of each shadow is exactly $1/k$ of the grayscale secret image.

2.3. Yang and Ciou's TiOISSS

Recently, Yang and Ciou [33] designed a new TiOISSS by using color mixing model. Their TiOISSS is a hybrid: half is VCS and half is PISSS. The advantages of both schemes, the easy decoding of VCS and the perfect reconstruction of PISSS, are simultaneously achieved. In the first decoding phase, we can preview a vague image by stacking shadows. On the other hand, we can obtain a finer gray-level secret image by computation in the second decoding phase.