Digital Signal Processing 23 (2013) 1496–1504

Contents lists available at SciVerse ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Visual secret sharing with cheating prevention revisited

Yu-Chi Chen [a,*], Du-Shiau Tsai [b], Gwoboa Horng [a]

[a] Department of Computer Science and Engineering, National Chung Hsing University, Taiwan
[b] Department of Information Networking Technology, Hsiuping University of Science and Technology, Taiwan

ARTICLE INFO

Article history:
Available online 31 May 2013

Keywords:
Visual secret sharing
Secret sharing
Cheating
Cheating prevention
Security

ABSTRACT

Visual secret sharing (VSS) is a variant form of secret sharing, and is efficient since secret decoding only depends on the human vision system. However, cheating in VSS, first showed by Horng et al., is a significant issue like a limelight. Since then, plenty of studies for cheating activities and cheating prevention visual secret sharing (CPVSS) schemes have been introduced. In this paper, we revisit some well-known cheating activities and CPVSS schemes, and then categorize cheating activities into meaningful cheating, non-meaningful cheating, and meaningful deterministic cheating. Moreover, we analyze the research challenges in CPVSS, and propose a new cheating prevention scheme which is better than the previous schemes in the aspects of some security requirements.

1. Introduction

Visual secret sharing (VSS) is inspired from secret sharing [1]. A secret is converted to a secret image (SI), and then SI will be encoded into many shares. Shares, given to participants by the dealer (a trusted party, $\mathcal{D}$), are formed into transparencies in VSS. $\mathcal{X}$ is an authorized subset, and the participants in $\mathcal{X}$ can visually reconstruct the secret image by stacking their transparencies together without performing any complicated cryptographic computation. In the k-out-of-n visual secret sharing (for short, (k,n)-VSS), there are n participants, while any k participants in $\mathcal{X}$ are able to reconstruct the secret by stacking their transparencies. Overall, a VSS scheme usually consists of three phases: (1) encoding, (2) distributing, (3) decoding. Encoding is performed by the dealer to generate all transparencies, then $\mathcal{D}$ distributes those transparencies to participants. Finally, the participants in $\mathcal{X}$ can decode the secret image by stacking their transparencies.

In particular, a special and important property to differ VSS from secret sharing [2] is that the security of VSS is achieved by loosing the contrast and the resolution of the SI. Indeed, the quality of the reconstructed secret image is inferior to the original secret image, but the secret is still seen by human's vision. With the development of VSS, many applications and related techniques have been proposed, such as visual authentication, visual identification, and image encryption. In addition, many kinds of VSS schemes were proposed to be used in different scenarios or to achieve different requirements [3–10].

1.1. Related work

In 2006, as well as the cheaters in secret sharing [11,12], Horng et al. showed that cheating is possible in (k,n)-VSS, where $k < n$ [13]. The dishonest participants (referred to as cheaters) collude and want to fool victims, which is called "cheating activity" (CA). CA can cause unpredictable damage to the victims; therefore, the victims accept a fake secret image (as known as a cheating image) different from the actual secret image as authentic. They presented two kinds of cheating prevention methods, share authentication and blind authentication:

- *Share authentication* (SA): Using the verifiable messages, decided by the participant or the dealer, authenticates a share transparency from another participant. A fake transparency, generated by the cheaters, must pass the authentication. However, if the fake transparency can pass the authentication, the victim will accept the stacking result.
- *Blind authentication* (BA): Without relying on any verifiable message, the cheaters predict the structure of the transparencies of the other participants is hard, such that the cheaters are difficult to generate a fake transparency.

They also attached two cheating prevention schemes, authentication based cheating prevention scheme and $(k,n+l)$-CPVSS scheme. In addition, Hu and Tzeng presented three kinds of cheating activities: CA-1, CA-2, and CA-3. They also gave a generic transformation that can make all VSS schemes to achieve cheating prevention. HTCP scheme denotes Hu and Tzeng's transformation scheme, which is share authentication. In 2010, De Prisco and De Santis also discuss the problem of cheating in VSS [14]. They proved that cheating actually exists in $(2,n)$-VSS and (n,n)-VSS,

[*] Corresponding author.
E-mail addresses: wycchen@ieee.org (Y.-C. Chen), dstsai@hust.edu.tw (D.-S. Tsai), gbhorng@cs.nchu.edu.tw (G. Horng).

1051-2004/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.dsp.2013.05.014

and gave the definition for deterministic cheating. They showed two kinds of cheating activities for $(2,n)$-VSS and (n,n)-VSS, respectively. The cheating activities in $(2,n)$-VSS is almost the same as Horng et al.'s. The other in (n,n)-VSS is denoted by DD-CA. Moreover, they proposed two CPVSS schemes, one is the simple (k,n)-VSS scheme where k is 2 or n, and the other is the better $(2,n)$-VSS scheme. These two schemes are blind authentication. To the best of our knowledge, the papers that deeply discuss cheating in visual secret sharing are the papers by Horng et al. [13] and De Prisco and De Santis [14] in theory. Recently, Chen et al. and Liu et al. also proposed cheating prevention schemes [15,16].[1]

1.2. Contribution and organization

We analyze cheating activities and propose a novel cheating prevention visual secret sharing scheme and attach the security analysis. This scheme is provably secure against the meaningful deterministic cheating, and it is better than the previous schemes in the expansion of a pixel. It is also a share authentication cheating prevention scheme without added transparencies.

The rest of the paper is organized as follows. Section 2 provides preliminaries: the model of VSS and the definition of cheating. Section 3 briefly analyzes some cheating activities and cheating prevention schemes. Section 4 shows a novel cheating prevention visual secret sharing scheme. Finally, Section 5 concludes this paper.

2. Visual secret sharing (VSS)

2.1. The model

A VSS scheme is a special variant of a k-out-of-n secret sharing scheme, where the shares given to participants are xeroxed onto transparencies. Taking the secret image, SI, as input, and generating the transparencies, each black and white pixel of SI is handled separately. It appears as a collection of m black and white subpixels in each of the n transparencies. The m subpixels are denoted by a *block*. One pixel of the secret image corresponds to nm subpixels, and then the nm subpixels are denoted by an $n \times m$ boolean matrix, called a *base matrix*. $S = [S_{ij}]$ expresses the base matrix, such that $S_{ij} = 1$ if and only if the jth subpixel of the ith share is black and $S_{ij} = 0$ if and only if the jth subpixel of the ith share is white. The grey level of the stack of k shared blocks is determined by the Hamming weight $H(V)$ of the "or"ed m-vector V of the corresponding k rows in S. This grey level is interpreted by the visual system of the users as black if $H(V) \geqslant d$ and as while if $H(V) \leqslant d - \alpha * m$ for some fixed threshold d and relative difference α. We would hope m to be as small as possible and α to be as large as possible, while at present, the lower bound of α for human's vision is uncertain. Formally, a solution to the (k,n)-VSS consists of two collections C^0 and C^1 of $n \times m$ base matrices. To share a white pixel, the dealer randomly chooses one of the matrices from C^0, and to share a black pixel, the dealer randomly chooses one of the matrices from C^1. The chosen matrix determines the m subpixels in each one of the n transparencies. The following definition is given by Naor and Shamir [1].

Definition 1. A solution to the (k,n)-VSS is composed of two collections C^0 and C^1 of $n \times m$ base matrices. The solution is considered valid if the following conditions are hold:

Contrast conditions:

1. For any matrix S^0 in C^0, the "or" V of any k of the n rows satisfies $H(V) \leqslant d - \alpha * m$.
2. For any matrix S^1 in C^1, the "or" V of any k of the n rows satisfies $H(V) \geqslant d$.

Security condition:

3. For any subset $\{i_1, i_2, \ldots, i_q\}$ of $\{1, 2, \ldots, n\}$ with $q < k$, the two collections D^0, D^1 of $q \times m$ matrices obtained by restricting each $n \times m$ matrix in C^0, C^1 to rows $i_1, i_2, \ldots, i_q$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

For convenience, let W_V be an integer which satisfies $W_V \leqslant d - \alpha * m$ and B_V be an integer which satisfies $B_V \geqslant d$. We can use W_V and B_V to judge a stacking block is black or white in a VSS scheme.

Now we show the base matrices of Naor and Shamir's $(2,3)$-VSS scheme and $(3,3)$-VSS scheme [1]. In $(2,3)$-VSS, C^0 is all the matrices obtained by permuting the columns of $\begin{bmatrix} 1&0&0 \\ 1&0&0 \\ 1&0&0 \end{bmatrix}$, and C^1 is all the matrices obtained by permuting the columns of $\begin{bmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{bmatrix}$; conveniently, in this paper, we will express

$$C^0 = \begin{bmatrix} 1&0&0 \\ 1&0&0 \\ 1&0&0 \end{bmatrix}, \qquad C^1 = \begin{bmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{bmatrix}.$$

In $(3,3)$-VSS, the base matrices are showed as follows:

$$C^0 = \begin{bmatrix} 0&0&1&1 \\ 0&1&0&1 \\ 0&1&1&0 \end{bmatrix}, \qquad C^1 = \begin{bmatrix} 0&0&1&1 \\ 0&1&0&1 \\ 1&0&0&1 \end{bmatrix}.$$

Hereafter, Naor–Shamir's (k,n)-VSS is denoted by (k,n)-VSS for short in this paper.

2.2. Cheating in VSS

Before to introduce the well-known cheating activities, we show the following definitions of cheating in VSS from the paper of De Prisco and De Santis [14].

Definition 2. For any pixel, if the probability of that the cheaters can successfully modify a black/white pixel into a white/black pixel in the stacking result is equal to 1, the cheating is the deterministic cheating. $\Pr[\mathit{Black} \longleftrightarrow \mathit{White}] = 1$ expresses that a cheating prevention scheme is insecure against the deterministic cheating, where the cheaters can modify a black/white pixel into a white/black pixel.

This definition makes researchers more easily to analyze the security for CPVSS. Taking the most real attack power into consideration, we must assume $n-1$ collusive cheaters (dishonest participants) and one victim in a (k,n)-VSS scheme.

2.2.1. Horng et al.'s cheating activity

Horng et al. proposed that cheating is possible in (k,n)-VSS where $k < n$ [13]. The cheating activity of Horng et al. is that the $n-1$ cheaters collusively use their transparencies to know the secret and infer the victim's transparencies T_v, thus they can generate a fake transparencies *FTs* to make the victim to accept the cheating image by stacking $\mathit{FTs} + T_v$.

We take a $(2,3)$-VSS scheme as an example. A secret image is encoded into three distinct transparencies, denoted T_1, T_2 and T_3. Then, the three transparencies are respectively delivered to Alice,

[1] The scheme of Liu et al. [16] is insecure because base matrices of some pixels are revealed.