J. Vis. Commun. Image R. 25 (2014) 1543–1557

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Multi-factor cheating prevention in visual secret sharing by hybrid codebooks

Chih-Hung Lin [a], Tzung-Her Chen [b,*], Yan-Ting Wu [b], Kai-Hsiang Tsao [b], Kai-Siang Lin [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 25 July 2013
Accepted 18 June 2014
Available online 27 June 2014

Keywords:
Visual secret sharing
Cheating attack
Cheating prevention
Hybrid codebook
Multi-factor
Visual cryptography
Share image
(k,n) Codebook

ABSTRACT

Visual secret sharing, or the so-called visual cryptography, is a well-known scheme that encrypts a secret image into several meaningless share images, usually printed on transparencies, and decrypts as stacking some or all share images by the human visual system. More and more researches about visual secret sharing and its applications have been recently proposed. Unfortunately, the cheating attack in which malicious participants cheat the honest one(s) by forging a fake share image has existed. Since 2006, some cheating prevention schemes have been proposed but suffered from one or more disadvantages as follows: (1) maintaining extra share images used to verify the integrity of a share image prior to stacking, (2) introducing extra pixel expansion, (3) raising heavy computation cost, and (4) giving ambiguous cheating detection. In this paper, a multi-factor cheating–preventing scheme, aiming at exploiting the hybrid codebook to hide the additional verification images into the share images, has been proposed without suffering the above-mentioned deficiencies. Two-factor cheating–detection exploits the design of verification to both share images and stacked results to deter attackers' cheating. The experimental results demonstrate the proposed scheme is feasible.

1. Introduction

With the progress of computer technology and the development of networks, the transmission of digital images becomes a daily operation. For the security of secret images transmitting over public networks, modern cryptosystems such as DES, and AES [1] have been proposed to guarantee confidentiality. But these cryptosystems are expensive in both encryption and decryption. Therefore, multimedia security, such as digital watermarking [2], and image authentication [3], becomes imperative in both academia and industry.

Visual secret sharing (VSS), first proposed by Naor and Shamir in 1995 [4], encodes a secret image to create several meaningless shares subsequently distributing to participants. Participants decode the secret by stacking the collected shares and using human visual system without any computation involved to reconstruct the secret image. No additional or complicated computation is required. A k-out-of-n visual secret sharing scheme, also called (k,n) VSS, means a secret image is encoded into n shares, and stacking any k or more shares ($k \leqslant n$) can reconstruct the secret image.

In (2,2) VSS scheme, a secret image is encoded into two share images S^A and S^B by a codebook (see Table 1). With the color of a pixel of secret image, S^A and S^B are assigned an adaptive sub-block for secret information. The size of sub-blocks is 2×2 such that the size of the share images and reconstructed image is expanded.

In the VSS environment, cheating occurs when some malicious participants, called cheaters, intend to fool or cheat honest participants. In 2006, Horng et al. [5] claimed the (k,n) VSS exists the cheating problem if $k < n$. Table 2 shows a codebook of (2,3) VSS scheme and Table 3 shows an example in such a way that a cheating attack is easy to demonstrate. Participants A and B may cheat the honest participant C by means of giving a fake share image. Assume that Participants A and B obtain sub-pixel □□■ and □□■, respectively. The participants A and B can infer the sub-pixel of participant C is □□■ according to the (2,3) codebook. Taking the above-mentioned actions, participants A and B can do nothing if they hope the stacked result with participant C is white, or modify their sub-pixel as ■□□ or □■□ if they hope the stacked result with participant C is black. As the same process, if the participants A and B obtain sub-pixel ■□□ and □■□, respectively. The participants A and B can infer the sub-pixel of participant C is □□■ according to the (2,3) codebook. Then, participants A and B can do nothing if they hope the stacked result with participant C is black, or modify their sub-pixel as □□■ if they hope the stacked result with

* Corresponding author.
E-mail address: thchen@mail.ncyu.edu.tw (T.-H. Chen).

http://dx.doi.org/10.1016/j.jvcir.2014.06.011
1047-3203/

Table 1
The codebook of (2,2) VSS scheme.

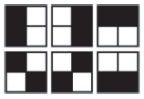
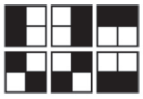
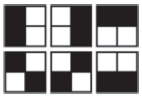
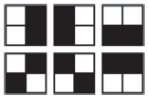
Secret pixel	S^A	S^B	Stacked results
□			
■			

Table 2
The codebook of (2,3) VSS scheme.

Secret pixel	S^A	S^B	S^C	$S^A \oplus S^B$	$S^B \oplus S^C$	$S^A \oplus S^C$	$S^A \oplus S^B \oplus S^C$
□							
■							

Table 3
Example of (2,3) VSS cheating case.

Secret pixel	S^A	S^B	S^C	Reconstructed cheating pixel	$S^{A'}$	$S^{B'}$	$S^{A'} \oplus S^C$	$S^{B'} \oplus S^C$
□				□				
				■				
■				□				
				■				

participant C is white. Therefore, the cheating problem does exist in (k,n) VSS if $k < n$.

Several papers [5–9,11] have proposed to solve the cheating problem. Yang and Laih [6] proposed two approaches to detect the fake shares. The first approach needs the help of a trusted authority (TA). TA holds a check share. If stacking the check share with the share of a participant, the verification image can be reconstructed to distinguish the participant. The second approach is a kind of (k,n) VSS scheme. Any two of them can reveal the verification image used to verify the validity of a share image, while at least k shares can reconstruct the secret image. This approach can work without any help of the TA.

In 2006, while Prisco and Santis provided a formal definition of cheating [11], Horng et al. [5] proposed two schemes to prevent