J. Vis. Commun. Image R. 33 (2015) 358–367

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

A privilege-based visual secret sharing model ☆

Young-Chang Hou [a],*, Zen-Yu Quan [b], Chih-Fong Tsai [b]

[a] *Department of Information Management, Tamkang University, Taiwan, ROC*
[b] *Department of Information Management, National Central University, Taiwan, ROC*

ARTICLE INFO

Article history:
Received 3 May 2015
Accepted 3 October 2015
Available online 22 October 2015

Keywords:
Visual secret sharing
Visual cryptography
Privileged share
Progressive reconstruction
Image sharing
Image encryption
Unexpanded share
Information hiding

ABSTRACT

In traditional visual secret sharing (VSS) schemes, every transparency has the same capability for recovery of the secret image. This means that managers are unable to assign an appropriate privilege to participants according to their importance. One way to solve this problem would be to assign each share a suitable recovery capability. In this study, we propose a novel secret sharing method, the privilege-based visual secret sharing model (PVSSM), which allows participants with different privileges. It is assumed that participants having a higher privilege will have a higher ability to recover the secret image. The proposed PVSSM has the following advantages: (1) Each share has an appropriate capability to reveal the secret information corresponding to the privilege of the share holder. (2) The restored image has a better contrast than the traditional VSS method can achieve. (3) The share has the same size as the secret image.

1. Introduction

The development of information technologies and computer peripherals has led to an inevitable trend to publish, transmit and share the digitized data over the network systems. Although great progress has been made in information technologies, it remains a very critical issue to protect the important data transmitted over the Internet from attack. The most popular solution for data protection is based on cryptography, where confidential data is transformed into meaningless messages by encryption. The hidden information is revealed by the corresponding decryption process utilizing the proper key. With restricted time and computing facilities, it is hard for attackers to decrypt the confidential data by means of exhaustive or statistical attack. The goal of computational security is thus achieved.

A (k, n) secret image sharing (SIS) scheme encrypts a secret image into n shadow images (or shares) such that k is a threshold value for the number of shadow images required to reveal the secret. That is, one can reconstruct a secret image by k or more shares, but cannot derive any information from $(k-1)$ or fewer shares [1]. In general, there are two common approaches to deal with the (k, n)-SIS scheme. One popular approach is to embed the secret pixels as the coefficients in a $(k-1)$-degree polynomial. Then the polynomial is used to generate the noise-like shares for a group of participants [2–8]. Shamir [2] first proposed a (k, n)-threshold secret sharing scheme by hiding the secret pixel into the constant coefficient of a random $(k-1)$-degree polynomial. Based on Shamir's scheme, Thien and Lin [3] used all coefficients of the polynomial for embedding secret pixels, and reduced the share size to $1/k$ times the size of the secret image. The secret image can be perfectly reconstructed using Lagrange's interpolation. Although this approach can provide distortion-free visual quality in the reconstructed secret image, it needs a computing device to solve the polynomials.

The other commonly-used approach is visual cryptography (VC) which was first proposed by Naor and Shamir [9] in EuroCrypt'94. With this method, a secret image is decomposed into n meaningless shares which are then distributed to n participants. Decryption is possible by overlapping an adequate number (say, k) of shares. The hidden message will be naturally revealed and can be decoded by the human visual system (HVS) without the necessity of any complicated computation or replacement algorithms. Moreover, no knowledge of sophisticated cryptographic techniques is needed for the encryption and decryption processes. However, the secret image will be invisible if the number of stacked shares is less than k. This is called the (k, n)-threshold mechanism. Despite no actual encryption/decryption in VC, hereinafter the process of image decomposition would still be called encryption and the process of image stacking be called decryption. VC can be applied not only in information hiding but also in access control, watermarking, authentication and identification, key exchange, etc. [10].

Previous SIS schemes have the threshold property that recovers either the entire image or nothing. However, in the real world, not

☆ This paper has been recommended for acceptance by Zicheng Liu.
* Corresponding author. Fax: +886 2 26209737.
E-mail address: ychou@mail.im.tku.edu.tw (Y.-C. Hou).

http://dx.doi.org/10.1016/j.jvcir.2015.10.005
1047-3203/© 2015 Elsevier Inc. All rights reserved.

everything is top secret. There are some images which are important and sensitive enough but still need to be processed daily. Using traditional SIS sometimes causes certain inconveniences for daily processing that needs easier management of shares, especially for large k and n. Hence, a new progressive VC (PVC) scheme with the scalable decryption capability was introduced recently to overcome this problem [10–16]. The scalability is that the information amount of the reconstructed image is proportional to the number of shares engaged in decryption and the quality of a reconstructed image depends on the number of available shares.

Most of the existing SIS schemes consider that each participant plays the same role in the revealing process [2–7,9–15]. In other words, every share has the same capability to restore the hidden information. An important individual couldn't be awarded a greater privilege to reveal the secret image more than others. However, there are many examples where some participants may have special privileges due to their status or importance, e.g., heads of a government, managers of a company, etc. So, we have to give special treatments to some persons for some reasons. Most existing SIS strategies cannot provide an appropriate level of privilege to corresponding participants to satisfy a diversity of needs.

In order to remove the above restrictions, we propose a novel sharing model, namely the privilege-based visual secret sharing model (PVSSM). In the PVSSM, a secret image is shared by n participants with different privileges. Each participant is assigned a privilege level (PL) PL_i ($1 \leqslant i \leqslant n$), and shares are then created and dispatched to participants depending on their importance. The recovery rate and the quality of the stacked image are dependent on the participant's significance. Thus, a share with a higher privilege contributes more information to restore the hidden data. In contrast, a lower privileged share has less recovery capability.

The remainder of this paper is organized as follows. In the next section, we offer a concise introduction of related works. In Section 3, the proposed PVSSM design is presented. The experimental results are discussed in Section 4. Finally, conclusions are given in Section 5.

2. Review of the related works

2.1. Polynomial-based secret image sharing

Based on the concept of Thien and Lin's scheme [3], Chen and Lin [4] proposed a multi-resolution approach by setting h thresholds r_i ($1 \leqslant i \leqslant h$). Their method first simultaneously took r ($r = r_1 + r_2 + \cdots + r_h$) pixels from the secret image. The gray values of the pixels are rearranged according to the order of the bit-planes, from the most significant bit to the least significant bit. Finally, r new values are reproduced. In the encoding phase, the new values will fill in the coefficients of h polynomial equations, each with ($r_i - 1$)-degree, to produce shares. When fewer shares are gathered, the recovered image is coarse, because only the pixels' most significant bits can be revealed. As the number of shares increases, the recovered image becomes clearer and clearer. Consequently, a lossless image can be revealed by gathering a number of shares equal to or more than r_h. Wang and Shyu [5] also took advantage of the different importance on different bit-planes, and decomposed the gray values of an image into j bit-plane groups to perform progressive secret sharing. Yang and Huang [6] and Yang and Chu [7] proposed a scheme that provided the threshold property and the scalability to construct a (k, n)-scheme, respectively. The information amount of a reconstructed secret will be proportional to the number of shadows used in decryption. Li et al. [8] considered that some shadows might be more important than others. In their scheme, all n shadows are classified into s essential shadows and (n–s) non-essential shadows. When reconstructing the secret image, the scheme needs k shadows, which should include at least t essential shadows. However, all the shares in the above works [4–8] are constructed by solving polynomials using Lagrange interpolation. Therefore, it is not possible for those schemes to implement the direct decryption of the secret image simply by stacking shares. Computers are needed to restore the secret information. Therefore, these practices could not be applied in VC.

2.2. Visual-based secret image sharing

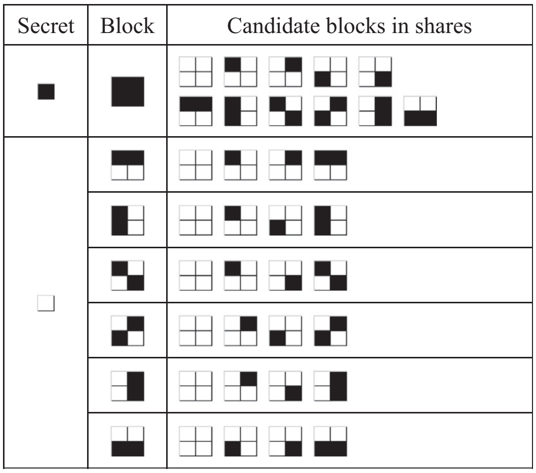
Fang and Lin [11] first proposed a progressive sharing method for VC. Their method magnified each pixel in a secret image to a 2 × 2 block. This block is fully black if the secret pixel is black. The block is comprised of randomly decided two-black-and-two-white spots if the secret pixel is white. Each corresponding block on the shares will be assigned 0–2 black spots as shown in Table 1.

Since Fang and Lin's method is based on pixel expansion, the shares are 4 times larger than the original image, which requires more storage space and processing time. As the way of selecting image blocks is based on random sampling, when the shares are superimposed, it cannot guarantee that black pixels will be restored as fully black blocks, and white pixels will be reconstructed as half-white-and-half-black blocks. Moreover, on the share, the probability of black in the secret black regions is greater than that in the secret white regions. This makes it easy to see the secret outline on the shares which leads to security leakage as a consequence. To solve the above problems, Hou and Quan [12] came up with a sharing method which combined the progressive sharing method without pixel expansion.

Chang et al. [13] proposed a friendly progressive visual secret sharing scheme without expanding the share size. It applied a 2 × 2-sized block-wise operation to generate the reconstructed secret image block by block. However, they also have the same drawbacks in security, contrast, and total reconstruction as Fang and Lin faced.

Chen and Tsao [14] utilized the random grid-based VC to encode the secret pixel so that b_1 and b'_2 are obtained. b'_2 is encoded in the same way to generate b_2 and b'_3. The operation is repeated until $b_1; b_2; \ldots; b_k$ ($= b'_k$) are obtained. The remaining $b_{k+1}; \ldots; b_n$ are assigned a value of 0 or 1 randomly. Then $b_1; \ldots; b_n$ are distributed to shares 1 to n randomly. Yan et al. [10] adopted Chen and Tsao's [14] approach and proposed a VC scheme with the

Table 1
Fang and Lin's [11] sharing model.



Secret	Block	Candidate blocks in shares