Displays 32 (2011) 118–134

Contents lists available at ScienceDirect

Displays

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

A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares

Der-Chyuan Lou [a], Hong-Hao Chen [b], Hsien-Chu Wu [c], Chwei-Shyong Tsai [d,*]

[a] Department of Computer Science and Information Engineering, Chang Gung University Kweishan, Taoyuan 33302, Taiwan
[b] Department of Computer Science and Information Engineering, Nation Taiwan University 1, Section 4, Roosevelt Road, Taipei City, Taiwan, ROC
[c] Department of Computer Science and Engineering, National Taichung Institute of Technology 129, Section 3, San Min Road, Taichung City, Taiwan, ROC
[d] Department of Management Information Systems, National Chung Hsing University 250, Kuo Kuang Road, Taichung City, Taiwan, ROC

ARTICLE INFO

Article history:
Received 23 January 2010
Received in revised form 20 October 2010
Accepted 1 February 2011
Available online 16 February 2011

Keywords:
Visual cryptography
Authenticatable color visual secret sharing
Non-expansion meaningful shares

ABSTRACT

In this paper, a novel visual secret sharing scheme is presented to hide a secret image into two meaningful cover images which are called share images with no pixel expansion. Simultaneously, the proposed scheme embeds an extra confidential image in these two share images. People who gather the two share images can obtain the secret image by stacking them without any complex computation. After one of the share images is shifted for certain unit, people can get the extra confidential image by their visual system to check the validity of the revealed secret image. Except for sharing binary secret image, the proposed scheme can also be applied to color visual secret sharing scheme to hide color secret image into two meaningful color halftone images without any pixel expansion, and people can derive the extra confidential image for authentication by shifting one of the share images.

1. Introduction

In recent years, along with the fast development of network technologies, most people share their secret information via the public Internet. In order to insure the security of sharing secret information, people usually conceal the secret data with symmetric or asymmetric cryptographic algorithms, such as DES [6], AES [25], RSA [7], and ECC [1]. Nevertheless, these cryptographic methods should need high computation cost in encryption and decryption processes. Therefore, many visual secret sharing schemes were proposed.

In 1995, Naor and Shamir proposed 2 out of 2 threshold visual secret sharing ((2, 2)-VSS) scheme [16], which separates a secret image into two share images, and anyone gets only one of the two share images cannot obtain the secret image. On the contrary, the participants/owners can recover the secret image by merely stacking the two share images without any computation. The primary feature of visual secret sharing schemes is that it does not require any computation when decryption process. For example, the typical application is the launch of cannon. When cannon shooting, captain and vice captain have to be approved simultaneously. Otherwise, if the captain was bribed, the results will be unimaginable. Therefore, the secret message is divided into two parts, and distributed to captain and vice captain. Each part of secret message cannot get any information about secret message, only when they combine their parts, then recover the original secret message. There are many applications of secret sharing, especially when we have no computing devices or have only low-power devices, the visual secret sharing will play an important role owing to its efficient decryption.

Afterwards, in order to enhance the quality of share image and the amount of embedded secret, more and more visual secret sharing schemes were proposed. For sharing multiple visual secret, Chen and Wu [3] proposed a (2, 2)-VSS for two secret images. It hides two secret images into two share images with particular angles such as 90°, 180°, or 270°. In order to overcome the limit of Chen and Wus' scheme, Hsu et al. [13] embeds two secret images with arbitrary rotating angles as a higher application scheme. Afterwards, Feng et al. [9] proposed a visual secret sharing scheme for multiple secrets. It embeds arbitrary number of secret images, and these secret images can be reconstructed at aliquot stacking angles.

However, the above-mentioned (2, 2)-VSS schemes share secret image has pixel expansion and meaningless share images so that it will attract attackers. Chang et al. [2] proposed another type hiding scheme, which embeds the secret image in two meaningful cover images, such as scenic images or portrait photographs. Therefore, the output share images have no pixel expansion. People who want to obtain the secret image just need to stack the two meaningful share images together, and then the secret image will be revealed. Although Chang et al.s' data hiding scheme makes the share images meaningful and no pixel expansion, it is still insecure. If a hacker

* Corresponding author. Fax: +886 4 22857173.
E-mail address: tsaics@nchu.edu.tw (C.-S. Tsai).

0141-9382/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.displa.2011.02.001

holds one of the two share images, he/she can exploit the share image and a counterfeit secret image to create a fake share image, and then dispatches it to the receiver. The receiver will be fooled, since he/she cannot verify the reconstructed secret image.

Fang and Lins' [8] visual cryptography scheme not only shares the secret image, but also provides extra ability of hiding confidential data. This scheme separates a secret image into two share images, and embeds the extra confidential data for authentication. Participants can get the secret image by stacking the two share images. Furthermore, participants fix one of the two share images, and move the other share image for certain unit. The extra confidential image is revealed by human visual system. If the share images are fakes created by hackers, the participants will not reveal the extra confidential data. Therefore, the participants will not be fooled. Despite that, this scheme still has some weaknesses, such as the pixel expansion, meaningless share images, and the less quantity of hiding extra confidential data.

For color secret image sharing, Hou [11] proposed a color visual cryptographic scheme which transforms a color secret image to three cyan (C), magenta (M), and yellow (Y) halftone images, and generates the share images by processing these C, M, Y images. Nevertheless, the meaningless share images and pixel expansion are weaknesses to arouse the hacker's attention and increase the delivery cost. Afterwards, in 2008, Wu et al. [24] proposed a color visual cryptography scheme by using meaningful share images. This scheme extracts some pixels from the input color halftone images as important information called extracted image, and generates two share images by CCT (cover coding table) and SCT (secret coding table). However, pixel expansion still exists.

In order to reduce the expanding ratio of share images, Shyu [19] proposed a c-colored (k, n)-VSS scheme to improve Yang and Laihs' scheme [27]. It focuses on reducing the size of pixel expansion. The pixel expansion of this scheme is $\lceil \log_2 \rceil c \times m$, where c denotes the number of colors in the secret image, and m denotes the pixel expansion size of each color. Unfortunately, the share images of this scheme are meaningless.

In order to overcome the above-mentioned defects, meaningless shares, pixel expansion, and cheating by fake shares, in this paper, we present a visual secret sharing scheme which achieves meaningful shares, non-expansion, and the proposed scheme not only shares secret image but also embeds an extra confidential data for authentication. In existing literature, there are few existing VSS schemes which are non-expansion and meaningful shares. The two most common methods are pixel swapping [2] and random grids [5]. Their generated share image and recovered secret are displayed in Section 4 (Fig. 19). Owning to the share image quality of pixel swapping method is superior to random grids method's, the proposed method is performed based on pixel swapping technique. The object is to achieve the similar recovered image of the original pixel swapping method, but provide authentication ability. Although the proposed scheme is based on pixel swapping, the kernel is different from the original scheme [2] which only modifies one of the cover images. In the original scheme [2], if the secret image is more complex, the modified cover image will be distorted seriously, so that the attackers may be attracted. In contrast, the proposed scheme can determine which blocks within the two cover images will be chosen to be modified. Thus, the quality of share images will be enhanced. In addition, our scheme can be applied to color visual secret sharing.

The share images generated by [4,11,12,14,15,17,18,21–24,26] are either pixel expansion or meaningless share images. [19,27] improve the weakness of pixel expansion, but still suffer from meaningless share images. Briefly, the proposed scheme simultaneously achieves the specialties of (1) meaningful share images, (2) no pixel expansion, (3) the more quantity of hiding extra confidential image than [8] under the same transmission cost, (4) applying to share color secret image, and (5) providing authentication ability.

The rest of this paper is organized as follows. Section 2 reviews the related works of error diffusion halftone techniques, visual cryptography with extra ability of hiding confidential data [8], and new data hiding scheme using pixel swapping [2]. Section 3 describes the proposed visual secret sharing for modifying diffusion, secret sharing based on pixel swapping to provide authentication, the process to enhance the quality of share image by modifying diffusion, and the proposed color visual secret sharing. Section 4 presents the experimental results. Section 5 shows the performance analysis. Finally, Section 6 is devoted to the conclusions.

2. Related works

2.1. Error diffusion halftone technique

Digital halftoning represents the variety of grayscale with the density of black pixels. The denser of black pixels in a region represents lower degree of grayscale. On the contrary, the sparser of black pixels in a region represents higher degree of grayscale. In digital halftoning, error-diffusion techniques distribute the quantization residual to neighboring pixels which have not been processed yet. The error diffusion of Floyd–Steinberg matrix [10] is shown in Fig. 1, and the flow chart of Floyd–Steinberg dithering process is shown in Fig. 2.

The Floyd–Steinberg dithering process can be described by the following equations:

$$u_{i,j} = x_{i,j} + \sum (h_{k,l} \times e_{i-k,j-l})$$

$$Q(u_{i,j}) = \begin{cases} 255 \text{ (white-pixel-color)}, & u_{i,j} \geqslant 128 \\ 0 \text{ (black-pixel-color)}, & u_{i,j} < 128 \end{cases}$$

$$e_{i,j} = \begin{cases} u_{i,j} - 255, & u_{i,j} \geqslant 128 \\ u_{i,j}, & u_{i,j} < 128 \end{cases}$$

where $e_{i,j}$ is the quantified error at location (i, j), $Q(u_{i,j})$ is used to determine a pixel value to be 0 or 255, $u_{i,j}$ is a state variable, and h is the error diffusion kernel.

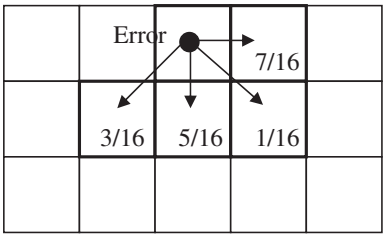

Fig. 1. Floyd–Steinberg diffusion matrix of distributing the error fractions to four neighboring pixels.

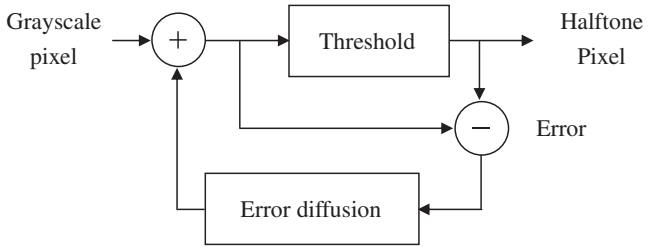

Fig. 2. Flow chart of the Floyd–Steinberg dithering process.