Expert Systems with Applications 37 (2010) 7858–7869

Contents lists available at ScienceDirect

Expert Systems with Applications

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

A novel visual secret sharing scheme for multiple secrets without pixel expansion ☆

Tsung-Lieh Lin [a], Shi-Jinn Horng [a,b,c,g,*], Kai-Hui Lee [d], Pei-Ling Chiu [e], Tzong-Wann Kao [f], Yuan-Hsin Chen [c], Ray-Shine Run [c], Jui-Lin Lai [c], Rong-Jian Chen [c]

[a] Department of Electrical Engineering, National Taiwan University of Science and Technology, 106 Taipei, Taiwan
[b] Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, 106 Taipei, Taiwan
[c] Department of Electronic Engineering, National United University, 36003 Miao-Li, Taiwan
[d] Department of Computer Science and Information Engineering, Ming Chuan University, 250 Zhong Shan N. Rd., Sec. 5, 111 Taipei, Taiwan
[e] Department of Risk Management and Insurance, Ming Chuan University, 250 Zhong Shan N. Rd., Sec. 5, 111 Taipei, Taiwan
[f] Department of Electronic Engineering, Technology and Science Institute of Northern Taiwan, Taipei, Taiwan
[g] Department of Computer Science, Georgia State University, Atlanta, GA 30302-4110, USA

ARTICLE INFO

Keywords:
Visual secret sharing scheme
Contrast
Pixel expansion
Camouflage

ABSTRACT

The main concept of the original visual secret sharing (VSS) scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information of the shared secret by any combination of the n share images except for all of images. The shared secret image can be revealed by printing the share images on transparencies and stacking the transparencies directly, so that the human visual system can recognize the shared secret image without using any devices. The visual secrets sharing scheme for multiple secrets (called VSSM scheme) is intended to encrypt more than one secret image into the same quantity of share images to increase the encryption capacity compared with the original VSS scheme. However, all presented VSSM schemes utilize a pre-defined pattern book with pixel expansion to encrypt secret images into share images. In general, it leads to at least $2\times$ times pixel expansion on the share images by any one of the VSSM schemes. Thus, the pixel expansion problem becomes more serious for sharing multiple secrets. This is neither a practical nor the best solution for increasing the number of secret sharing images. In this paper, we propose a novel VSSM scheme that can share two binary secret images on two rectangular share images with no pixel expansion. The experimental results show that the proposed approach not only has no pixel expansion, but also has an excellent recovery quality for the secret images. As our best knowledge, this is the first approach that can share multiple visual secret images without pixel expansion.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

The secret sharing scheme was proposed by Blakely (1979) and Shamir (1979). The ordinary secret sharing scheme separates secret information into a set of portions for participants and achieves the objective of protecting secret information. In general, the secret sharing scheme is a (k, n)-threshold scheme, that is, the secret is separated into n different share messages. The secret can be recovered by combining at least k $(2 \leqslant k \leqslant n)$ share messages, and the secret cannot be recovered by using less than k share messages. In a traditional (k, n)-threshold scheme based on cryptography theory, the operation of separating to n share messages is called encryption, and the operation of recovery by combining k share messages is called decryption. The decryption process requires the aid of additional devices such as computers and high mathematical computation ability. Under this ordinary secret sharing scheme, it is impossible to recover the secret information without computational devices.

Another visual secret sharing scheme (VSS scheme) was introduced by Naor and Shamir (1995). In the encrypting process, devices were needed to encrypt the secret image into n $(n \geqslant 2)$ shared images for participants. But in the decrypting process, the secret image could be revealed by directly stacking share images and the recovered secret image could be recognized by the human visual system without any additional computational devices. This VSS scheme was very convenient for revealing the secret image, particularly as it could be done without any computational devices. Like the traditional (k, n)-threshold scheme, the (k, n)-VSS scheme

☆ This work was supported in part by the National Science Council under contract number NSC 96-2918-I-011-002, 97-2221-E-239-022, 95-2221-E-011-032-MY3.

* Corresponding author at: Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology, 106 Taipei, Taiwan. Tel.: +886 2 27376700; fax: +886 2 27301081.

E-mail addresses: jabezlin@yahoo.com.tw (T.-L. Lin), horngsj@yahoo.com.tw (S.-J. Horng), khlee@mcu.edu.tw (K.-H. Lee), plchiu@mcu.edu.tw (P.-L. Chiu), tkao@ms6.hinet.net (T.-W. Kao), yschen@nuu.edu.tw (Y.-H. Chen), run5116@ ms16.hinet.net (R.-S. Run), jllai@nuu.edu.tw (J.-L. Lai), rjchen@nuu.edu.tw (R.-J. Chen).

0957-4174/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2010.04.051

could reveal the shared secret image when at least k ($2 \leqslant k \leqslant n$) share images were stacked together. Of course, any single share image or less than k share images stacked together could not reveal the shared secret even when using computational devices.

During the past decade, VSS has attracted the attention of many researchers. Some of the literature has been related to the construction of a visual secret scheme (Ateniese, Blundo, De Santis, & Stinson, 1996; Chen, Chan, Huang, Tsai, & Chu, 2007; Verheul & van Tilborg, 1997; Yang, 2004; Wang, Zhang, Ma, & Li, 2007). Based on the concept of sharing binary secret images, researchers have extended the visual secret sharing scheme to suit the sharing of gray secret images (Iwamoto & Yamamoto, 2003; Wang et al., 2007; Yang & Chen, 2006) and color secret images (Chang, Lin, Le, & Le, 2008; Hou, 2003; Shyu, 2006; Yang & Chen, 2008). In terms of the number of share secret images, the literature has been solely concerned with sharing only one secret image. However, it would be useful to be able to share more than one secret image simultaneously. Clearly, it would be worthwhile to develop a visual secret sharing scheme for multiple secrets (is called the VSSM scheme).

Based on the traditional VSS scheme, some schemes have been proposed in order to share multiple secrets simultaneously. Wu and Chen (1998) proposed a (2,2) visual secret sharing scheme to share two secret images in two square share images, noted as S_1 and S_2. By stacking the two square share images of S_1 and S_2, the first secret image SE_1 could be revealed, and the second secret image SE_2 could be revealed by stacking shared image S_1 and the other share image S_2 with a 90° rotation angle (Wu & Chen, 1998). The rotation angle could be easily modified to be one of $q \times 90°$, $1 \leqslant q \leqslant 3$. Wu and Chang (2005) developed a multi-secrets sharing scheme which could share two secret images by embedding secret images into two circle share images. The rotation angle of the rotated share image in Wu and Chang's scheme was a factor of 360°, not being limited to 90°, 180°, and 270° as in Wu and Chen's sharing scheme (Wu & Chen, 1998) when the two circle share images were stacked together. Shyu, Huang, Lee, Wang, and Chen (2007) scheme permits share $x \geqslant 2$ secret images in two circle share images S_1, and S_2, and x secret images could be revealed one by one stacking the first circle share image S_1 and the rotated second shared image S_2 with $q \times r°$ ($0 \leqslant q \leqslant x-1$, $r = 360°/x$) different rotation angles. Feng, Wu, Tsai, Chang, and Chu (2008) proposed a (2,2)-x-VSSM scheme to share $x \geqslant 2$ secret images by using two cylinder share images so that the secret image could be revealed from the two share images by stacking with an aliquot angle.

Although the above-mentioned VSSM schemes could share at least two secret images, unfortunately, the obvious and serious problem of pixel expansion (means $m = size_{share\ image}/size_{secret\ image}$), existed in these visual multiple secrets sharing schemes (Feng et al., 2008; Shyu et al., 2007; Wu & Chen, 1998; Wu & Chang, 2005). In the scheme of Wu and Chen (1998), the size of the share image was 4 times larger than that of the secret image; that is, the pixel expansion was 4, as was the pixel expansion of Wu and Chang's proposed scheme (Wu & Chang, 2005), while in the scheme of Shyu et al. (2007) the pixel expansion was $2x$ when x secret images were shared. According to the (2,2)-x-VSSM in Feng et al. (2008), pixel expansion was $3x$, with x as the number of secret images to be shared. For the above-mentioned schemes, the problem of pixel expansion was a definite disadvantage and it became critical to develop a VSSM scheme. However, the challenge of obtaining no pixel expansion in a VSSM scheme has not yet been resolved.

In VSSM scheme, researchers have faced another challenge in that the contrast quality in the revealed secret images has been so low that it could not be effectively discerned by human visual system. The best contrast was 1/4 in the multiple secrets sharing schemes of Wu and Chen (1998) as well as Wu and Chang (2005). The contrast in Shyu et al.'s scheme (Shyu et al., 2007) was $1/(2x)$, and for Feng et al. (2008) it was $1/(3x)$ when x secret images were shared, with the greater number of sharing secrets causing the lower contrast for the schemes of Shyu et al. and Feng et al. The state-of-the-art on VSSM schemes, no existed scheme has overtaken the upper contrast (=1/4) in the revealed secret images.

In this paper, we have proposed a novel VSSM scheme for sharing two binary secret images in two share images S_1 and S_2 with no pixel expansion, and have achieved an excellent recovery quality for the revealed secret images. During the encrypting process, the proposed scheme generated share images without any pre-defined pattern books. This process was different from any existing VSS schemes. By directly stacking the two share images, S_1 and S_2, the first secret SE_1 could be revealed and be recognized by the human visual system, and the second secret SE_2 could be revealed by stacking one share image and the other with a rotation angle of 180°. Neither of the two share images leaked any information of the two secret images. Our proposed VSSM scheme has resolved the pixel expansion problem existing in VSS schemes, whether sharing one or multiple secrets, and has increased the contrast quality of the revealed secret image by adopting the appropriate encrypting process.

The remainder of this paper has been organized as follows. In Section 2.1, the original visual sharing secret scheme proposed by Naor and Shamir has been reviewed and 4 other visual multiple secrets sharing schemes have been reviewed in Sections 2.2 and 2.3. The proposed scheme for sharing two secret images in two share images with no pixel expansion and no pre-defined pattern book has been described in Sections 3.1–3.4 and 3.5. The experimental results and comparisons are presented in Section 4 with the conclusions presented in the last section.

2. Related literature review

2.1. Naor and Shamir's visual secret sharing scheme

The (n,n)-threshold visual secret sharing scheme, first proposed by Naor and Shamir (1995), is used to share one secret image on n share images (Naor & Shamir, 1995). The secret image is encrypted into n share images of which every one of the n share images is a meaningless random image and cannot reveal the secret image. By stacking n share images together, the hidden secret image is revealed and can be recognized by the human visual system without any computation. Fig. 1 shows a (2,2)-threshold VSS scheme used to share the secret image "CRYPT". As shown in Fig. 1(b) and (c), the shares images are meaningless. No one can recognize the secret image "CRYPT" by staring at the shared images. In Fig. 1(d), the secret image is revealed by stacking the share images, as shown in Fig. 1(b) and (c).

The stacking operation prints n share images on n different transparencies, T_1, T_2, ..., T_n. T_1, T_2, ..., and T_n are stacked together with a corresponding position. This process is an "OR" operation for the corresponding pixels on transparencies T_1, T_2, ..., and T_n. According to the color level of the corresponding pixels on T_1, T_2, ..., and T_n, the color level on the secret image can be revealed by this stacking operation. Eq. (1) describes the detailed operation. In Eq. (1), the digit 1 represents the black color level and digit 0 represents the white color level. The $o_k^{(i,j)}$ represents the pixel color on the (i,j) position of transparency T_k, $1 \leqslant k \leqslant n$. If all corresponding pixels are white (means $o_k^{(i,j)} = 0$), then the stacked result is white (=0). If at least one pixel color is black (=1), the stacked result pixel is black (=1). Obviously, the color level on the stacked transparencies can reveal the secret image by an subtle encrypting method.

Download English Version:

https://daneshyari.com/en/article/386191

Download Persian Version:

https://daneshyari.com/article/386191

Daneshyari.com