IJDCST @Dec-2015, Issue- V-3, I-8, SW-05
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

An Optimization model for Sharing Visual Secrets in Single Image

Saikumar Yerramsetti [1], S.V.C. Gupta [2]

[1] M.Tech (CSE), Sri Vasavi Institute of Engineering and Technology, A.P., India.

[2] Head of the Department, Dept. of Computer Science & Engineering, Sri Vasavi Institute of Engineering and Technology, A.P., India.

Abstract — The technique we use to share and protect secret images is Visual cryptography schemes (VCSs), which generate random and meaningless shares. Conventional VCSs suffer from a transmission risk problem because the noise-like shares will raise the suspicion of attackers and the attackers might intercept the transmission. Previous research has involved in hiding shared content in halftone shares to reduce these risks, but this method exacerbates the pixel expansion problem and visual quality degradation problem for recovered images. In this paper, a binocular VCS (BVCS), called the (2, n)-BVCS, and an encryption algorithm are proposed to hide the shared pixels in the single image random dot stereograms (SIRDSs). Because the SIRDSs have the same 2D appearance as the conventional shares of a VCS, this paper tries to use SIRDSs as cover images of the shares of VCSs to reduce the transmission risk of the shares. The encryption algorithm alters the random dots in the SIRDSs according to the construction rule of the (2, n)-BVCS to produce nonpixel expansion shares of the BVCS. Altering the dots in a SIRDS will degrade the visual quality of the reconstructed 3D objects. Hence, we propose an optimization model that is based on the visual quality requirement of SIRDSs to develop construction rules for a (2, n)-BVCS that maximize the contrast of the recovered image in the BVCS.

Keywords — Visual cryptography, single image random dot Stereograms, transmission risk, pixel expansion.

I. INTRODUCTION

Encrypting a secret image into n shares, with each participant holding one share, can be done by using Visual cryptography (VC); for any participant with less than k, $2 \leq k \leq n$, shares cannot reveal any information about the secret image. Stacking the k shares reveals the secret image, which can be recognized directly by the human visual system [1].

Conventional shares [1]–[4], which consist of many random and meaningless pixels satisfy the security requirement for protecting secret contents, but they have a drawback—there is a high transmission risk because noise-like shares raise the suspicion of attackers, who may intercept the shares. Thus the risk both to the participants and to the shares increases in turn increasing the probability of transmission failure.

Previous research into the Extended Visual Cryptography Scheme (EVCS) provided a meaningful appearance for shares to make the noise-like shares manageable for participants [5]–[9]. However, the meaningful shares still present a risk of detection. In EVCSs, the shares that are printed on transparencies still contain many noise-like pixels and/or display low-quality images. Such shares are easily detected by the naked eye and participants who transmit the shares can easily raise the suspicion of potential attackers.

Other research involves sharing secret images via high quality shares [10]–[12]. Zhou et al. proposed a *(*2, 2*)*-VCS using the half toning technique to construct meaningful binary images as shares carrying significant visual information [10]. The visual quality of the halftone is significantly better than that attained by extended VC. The shares obtained using Zhou et al.'s approach can reduce the transmission risk of the shares, but that approach exacerbates the pixel expansion problem and the visual quality degradation problem for the recovered images. Other studies [11], [12] suffer from the same drawbacks as Zhou et al.'s method. Given these drawbacks, the extension ability of these approaches could be limited. Therefore, further research is needed on the current VCSs to find an alternative way to reduce the transmission risk problem for participants and shares.

In 1838, Wheatstone discovered stereoscopic vision and published an explanation of stereopsis (binocular depth perception) arising from differences in the horizontal positions of images in the two eyes. When we look at two flat, dissimilar, 2D pictures, our mind perceives an illusion of 3D depth. In 1960, Julesz developed the random-dot format of the stereogram, in which the 3D form bypasses the monocular processes and is visible only when stereoscopic fusion is obtained. A random-dot stereogram (RDS) is a stereo pair of images of random dots, which when viewed with the aid of a stereoscope or with the eyes focused on a point in front of or behind the images, produces a sensation of depth, with objects appearing to be in front of or behind the display level. Tyler and Clarke proposed a stereoscopic technique that allows the stereoscopic presentation of 3D form from a single printed image by a random dot pattern. These are known as Single Image Random Dot Stereograms (SIRDS), or Random Dot Autostereograms [13].

The appearance of a SIRDS consists of many random dots that have a similar appearance with shares in a VCS. The only difference is that people can reconstruct the original 3D object via binocular disparity from a SIRDS. Hence, hiding a share of a VCS in a SIRDS can reduce suspicion of hidden secrets. This property indicates that the SIRDS is a natural, and the best, candidate to serve as a cover image for a share of a conventional VCS. We are interested in developing a novel technique for sharing visual secrets using SIRDSs.

In this study, a 2-out-of-*n* binocular VCS, called the *(*2, *n)*-BVCS, is proposed to provide non-expanded and high quality cover images for shares of the VCS to reduce the risk of interception during the transmission phase. The proposed *(*2, *n)*-BVCS shares a binary secret image with *n* participants *(n* ≥ 2*)*; when any two participants stack their transparences, the encrypted secret is revealed. The shares of the *(*2, *n)*-BVCS are hidden in *n* SIRDSs to reduce susceptibility to attackers during the transmission phase. The proposed encryption procedure consists of two phases. In the first phase, the procedure generates *n* SIRDSs by using existing autostereogram generation programs. In the second phase, the procedure alters the random dots in the SIRDSs according to a construction rule of the *(*2, *n)*-BVCS for hiding the binary secret image. The construction rule is a guideline for hiding the secret image in the SIRDSs securely. However, altering the dots in a SIRDS will interfere with the human brain's ability to perceive the original 3D objects in the SIRDSs and degrade the visual quality of the reconstructed 3D objects. Hence, we adopt an optimization approach to find construction rules for the *(*2, *n)*-BVCS such that the encryption process yields a secure BVCS and the contrast of the recovered secret image can be maximized, subject to the visual quality of the SIRDSs.

II. PROBLEM STATEMENT

Although both SIRDSs and shares of VCSs have the same noise-like appearance, the pixel distributions for a set of SIRDSs and for shares of a specific VCS are quite different. The pixel distribution among shared pixels must obey the construction rules or codebooks of the VCS. Shared pixels mean that a set of pixels shares the same secret pixel in a VCS. In Example 1, the codebook (i.e., C0 and C1*)* and the chosen-probability sets (i.e., F0 = {0.5, 0, 0, 0.5} and F1 = {0, 0, 1, 0}*)* are used to construct *(*2, 3*)*-ProbVCS, Hence, the pixel distribution patterns in the resultant shares comply with C0 and C1. If the encryption process selects column vector [1 0 1]T from C1 for sharing a black secret pixel, shares 1 and 3 will get a black pixel and share 2 will get a white pixel, and the pixel distribution pattern for the shares will be 2B1W. The pixel distribution pattern, *i*B*(n* − *i)*W, indicates there are *i* black pixels and *n* − *i* white pixels distributed among *n* shared pixels. The probability of each pixel distribution pattern for the *(*2, 3*)*-ProbVCS is listed in Table I. Notation *d*, is called the pixel density of a share (or a SIRDS), denotes the frequency of appearance of black pixels in a share (or in a SIRDS). In this example, pixel density *d* of each share is 2_3.

On the other hand, in a SIRDS, the image contains many random-dot patterns that periodically repeat in the horizontal direction; the stereopsis of the objects arises from differences in the horizontal positions of the image. The pixel distribution in *n* SIRDSs that were generated independently is totally independent. Suppose each SIRDS has the same pixel density *d*, the probability of pixel distribution pattern *i*B*(n*−*i)*W can be calculated as following:

$$\mathrm{P}_{i,n}^{d} = \binom{n}{i} \times d^{i} \times (1-d)^{n-i}.$$

The pixel distribution among three SIRDSs is listed in Table I. In general, while all SIRDSs are stacked, each pixel distribution pattern will uniformly appear in the stacked image. Hence, it is almost impossible to reveal any meaningful information by stacking two shares together. In this study, we try to alter pixels in SIRDSs such that the altered SIRDSs can share secret images the same way as VCSs. In the following, we will investigate whether the altered-pixels in a SIRDS will interfere with the visual effect of stereopsis in the SIRDS.

Fig. 1 illustrates an example for altering pixels in a SIRDS. The depth map, as shown in Fig. 2(a), is used to create the SIRDS in Fig. 2(b). In this paper, all autostereograms can be viewed in the wall-eyed viewing. The terms "wall-eyed" is a condition where eyes do not point in the same direction when looking at an object. Wall-eyed viewing requires the two eyes to adopt a relatively parallel angle. Hence, it is informally known as parallel-viewing. Fig. 2(c) shows the verification image of a stereopsis in the SIRDS. The verification image, which is a computer-generated 2D image, can disclose the stereopsis in a SIRDS in 2D format. The verification image for a SIRDS can be generated as follows

Definition 8 (Verification Image Generation Rule): Assume *px,y* denotes pixel *(x, y)*, in a SIRDS, and each pixel (*pvx,y)* in the verification image can be produced by operation
$pvx,y = px,y \oplus px{-}\varepsilon,y$, where $px{-}\varepsilon,y = 0$ if $x < \varepsilon$. Parameter ε is the separation parameter of the SIRDS and logical operator $\oplus$ represents the XOR operation.

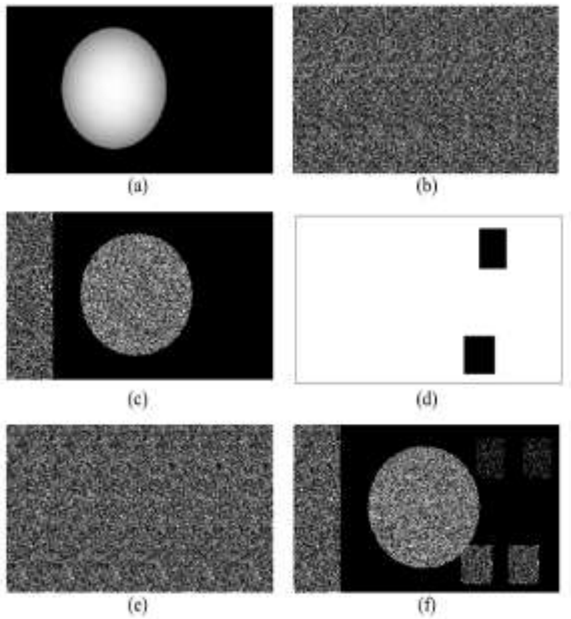

Fig 1 An example of hiding a secret image in a SIRDS

Suppose the color of the original pixels in the SIRDS, as shown in Fig. 1(b), will be altered, black boxes in a location map, as shown in Fig. 1(d), indicates that the pixels in which regions of the SIRDS could be altered. The color of the original pixels within two black boxes is randomly altered in various probabilities (20% and 50% for the top and bottom boxes, respectively). Fig. 1(e) demonstrates the SIRDS after altering the original pixels. By viewing Fig. 1(e) binocularly, we perceive that additional stereopsis appear in Fig.1(e). The stereopsis (i.e., two boxes) in the bottom of Fig. 1(e) is clearer than the stereopsis in the top of Fig. 1(e). In Fig. 1(f), the verification image of Fig. 1(e) shows the same result.

III. RELATED WORK

From the perspective of research methodology, research into the VCSs with meaningful shares can be classified into two approaches: cryptography approaches and embedded approaches.

The cryptographic approach uses a set of basis matrices [5], [6] or an algorithm [7], [9] to simultaneously encrypt a VCS and provide a meaningful appearance for the shares of the VCS. The former method requires designing a set of basis matrices for a specific VCS, and suffers from the pixel expansion problem. The random-grid-based (RG-based) approach (an algorithmic method) involves constructing VCSs and EVCSs [7], [9]. The main idea behind the RG-based EVCS algorithm approach is that it encrypts a secret image to the shares according to a given probability *p* and stamps cover images on the shares with *(*1 − *p)* probability. The encryption of the secret image can use any existing RG-based VCS. By adjusting probability *p*, the algorithm can tune the visual qualities between the recovered image and the shares of an EVCS. Chen et al. and Guo et al. proposed RG-based *(*2, 2*)*- and *(k, k)*-EVCSs, respectively. Chen et al.'s approach must use a pair of complementary images as cover images.

Guo et al.'s approach does not need to adopt complementary images as cover images, but the visual quality of the shares is reduced when probability *p* is too small or too large.

The embedded approach tries to stamp covering images in the shares of a VCS [8] or to hide shares behind covering images [10]–[12]. Zhou et al. proposed a halftone VCS that can construct *(*2, 2*)*-EVCSs via complementary covering shares [10]. First, they prepared a pair of complementary halftone images, I and I, as covers of noisy shares. Halftone image I is obtained by applying any halftoning method on a gray-level image. Halftone image I is obtained by reversing all black/white pixels of image I to white/black pixels. Second, a secret pixel is encoded as *m* sub-pixels (called secret information pixels) for each share; the sub-pixels are randomly selected from two basis matrices (i.e., C0 and C1*)* of the conventional *(*2, 2*)*-VCS. These sub-pixels are used to modify the Q1×Q2 halftone cell in both shares, I and I. Zhou developed a void and cluster algorithm to select *m* positions in the halftone cells to embed the *m* secret information pixels. Hence, the secret image is revealed by the secret information pixels when the shares are stacked together. In Fig. 1, a secret pixel is shared to two 4 × 4 halftone cells in shares I and I. If the secret pixel is black, two sub-pixels for each share, [0 1] and [1 0], are randomly selected from C1. The positions for embedding the secret information pixels are marked A and B. In this way, the stacked halftone cell will reveal a black secret pixel. Another example for sharing a white pixel is shown in Fig. 1(b). Applying Zhou's approach, the size of a halftone cell must be greater than or equal to the pixel expansion factor. The visual quality of the halftone shares improves as the size of a halftone cell increases; however, there is a tradeoff between the visual quality of the meaningful shares and the visual quality of the recovered images. Zhou's approach can be extended to an arbitrary access structure, but it may require distributing several images to participants.

IV. CONCLUSION

This study proposed a *(*2, *n)*-BVCS and developed a new method for hiding a size-invariant *(*2, *n)*-VCS in *n* SIRDSs. This work explored the possibility of hiding a share of a VCS in SIRDSs that are printed on transparencies. We developed a mathematical model that defines a set of construction rules so that the recovered images of *(*2, *n)*-BVCSs have the highest contrast under the constraint of the interference introduced into the SIRDSs. Using this mathematical model, a desired visual quality for shares and recovered images can be found by adjusting parameters P*a,max* and *d*. The best contrast for the recovered images in *(*2, *n)*-BVCSs, $2 \leq n \leq 10$, ranges between 0.5 and 0.2, and can produce clear recovered images for a *(*2, *n)*-BVCS. The experimental results prove the effectiveness and the flexibility of the proposed *(*2, *n)*-BVCSs. In the near future, we plan to extend this study to explore new methods for hiding a *(k*, *n)*-VCS in *n* SIRDSs.

REFERENCES

[1] M. Naor and A. Shamir, “Visual cryptography,” Advances in ryptology—EUROCRYPT (Lecture Notes in Computer Science). New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[2] R. Ito, H. Kuwakado, and H. Tanaka, “Image size invariant visual cryptography,” IEICE Trans. Fundam. Electron., Commun., Comput. Sci., vol. E82-A, no. 10, pp. 481–494, 1999.

[3] C. N. Yang, “New visual secret sharing schemes using probabilistic method,” Pattern Recognit. Lett., vol. 25, no. 4, pp. 481–494, Mar. 2004.

[4] P. L. Chiu and K. H. Lee, “A simulated annealing algorithm for general threshold visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011.

[5] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” Theoretical Comput. Sci., vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[6] D. Wang, F. Yi, and X. Li, “On general construction for extended visual cryptography schemes,” Pattern Recognit., vol. 42, no. 11, pp. 3071–3082, Nov. 2009.

[7] T.-H. Chen and K.-H. Tsao, “User-friendly random-grid-based visual secret sharing,” IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693–1703, Nov. 2011.

[8] K.-H. Lee and P.-L. Chiu, “An extended visual cryptography algorithm for general access structures,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

[9] T. Guo, F. Liu, and C. Wu, “k out of k extended visual cryptography scheme by random grids,” Signal Process., vol. 94, pp. 90–101, Jan. 2014.

[10] Z. Zhou, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography,” IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[11] Z. Wang, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[12] F. Liu and C. Wu, “Embedded extended visual cryptography schemes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun. 2011.