International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:4, No:5, 2010

Visual Cryptography by Random Grids with Identifiable Shares

Ran-Zan Wang, Yao-Ting Lee

***Abstract*—**This paper proposes a visual cryptography by random grids scheme with identifiable shares. The method encodes an image *O* in two shares that exhibits the following features: (1) each generated share has the same scale as *O*, (2) any share singly has noise-like appearance that reveals no secret information on *O*, (3) the secrets can be revealed by superimposing the two shares, (4) folding a share up can disclose some identification patterns, and (5) both of the secret information and the designated identification patterns are recognized by naked eye without any computation. The property to show up identification patterns on folded shares establishes a simple and friendly interface for users to manage the numerous shares created by VC schemes.

***Keywords*—**Image Encryption, Image Sharing, Secret Sharing, Visual Cryptography.

I. Introduction

IN 1995, Naor and Shamir [1] proposed an image-based secret protection method, named visual cryptography (VC), to share an image among multiple participants. In the (*t*, *n*)-threshold VC scheme, an input image is encoded to *n* shares such that any subset of *t* ($2 \le t \le n$) or more shares can disclose the secret recorded on the original image, but no secret information can be revealed from any *t*−1 or fewer shares. The created shares of a VC scheme usually consist of many noisy black dots that are printed on transparent slides, and dispatched one for each to the participants. A fascinating property of the VC technique is that the decoding process is carried out by inspecting the superimposed shares using naked eye without any computer computation. Attracted by the special decoding mode, many VC schemes [2–9] followed Naor and Shamir's idea with diverse revealing effects were proposed in the past two decades.

In the literature, a similar idea for encoding pictures and shapes using two transparencies was proposed early in 1987 by Kafri and Keren [10]. The method encoded a binary image in two random grids (RGs) in such a way that the areas containing black pixels are inter-correlated, but the areas of the white pixels are uncorrected. When superimposing the two RGs, the light transmission rates vary in information areas (black pixels) from the background (white pixels) so that the content of the image is revealed and can be perceived by human eyes. Details of Kafri and Keren's encoding algorithms are described later in Section II. A nice property of their method is that each generated RG has the same scale as the input image, which is one of the glamorous characteristics purchased by many VC designers [11–13] during the past decade. Attracted with the property of maintaining invariant size of each generated RG with the original image in Kafri and Keren's method, Shyu [14,15] comprehensively explored the features of RGs, and proposed separate image encryption methods using RGs for bi-level, grey-level and color images. Chen and Tsao [16] also designed VC scheme by RGs in which the size of each generated share is the same as the input image, their method is based on the graceful designed recursively encoding procedures to generate the shares one by one. Some other VC schemes using the concept of RGs can also be found in [17].

The above VC by RGs schemes [10–17] can be applied to distribute a secret image among multiple shares with each share has same size as the input image, and the secrets on the input image can be revealed and recognized by naked eye by superimposing the shares; however, the management of the noise-look shares is a problem. For example, consider the four shares shown in Fig. 1, in which (a) and (b) are the two shares of an image, and (c) and (d) are the shares of other images. If the four shares are out of order, the user must try all possible $C_2^4 = 6$ combination ways (as shown in Fig. 2) to superimpose two of the four shares to reveal the image. It is a tedious work and the problem becomes troublesome when the number of shares gets larger.

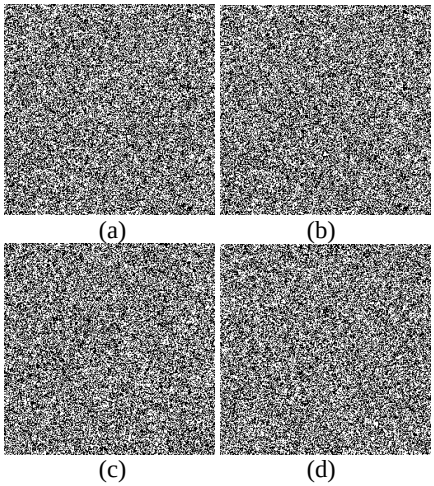


Fig. 1 Four noise-look shares created by VC scheme.

The authors are with the Department of Computer Science & Engineering, Yuan Ze University, 135 Far-East Rd., Chung-Li, Taoyuan 320, Taiwan, R.O.C. (Tel: (886)3-4638800-3003 Fax: (886)3-4638850.)

This work is supported by the National Science Council, R.O.C., under grant NSC97-2221-E-155-025-.

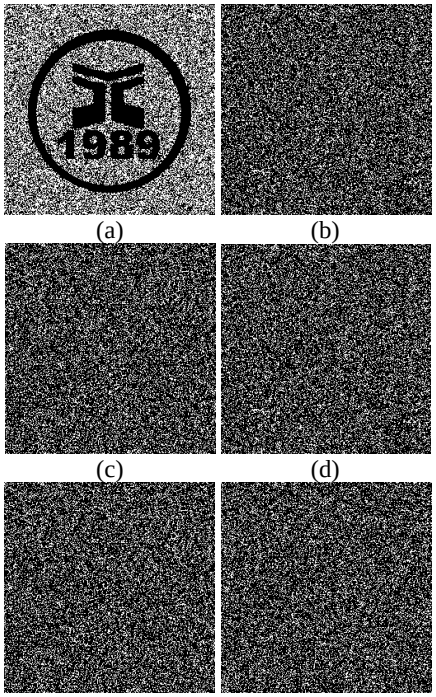


Fig. 2 The results of superimposing any two of the four shares shown in Fig. 1.

The aim of this study is to develop a VC by RGs scheme such that some designated identification patterns can be disclosed from a single share, it can provide the users with a friendly interface to manage the numerous noise-look shares created by VC schemes. The rest of the paper is organized as follows. Section II reviews the picture encryption by RGs scheme proposed by Kafri and Keren [9]. The details of the proposed VC by RGs with user-friendly shares scheme are described in Section III. The experiment results are shown in Section IV. Finally, conclusions are made in Section V.

II. Kafri and Keren's Picture Encryption by Random Grids

Kafri and Keren [9] proposed a one-step decoding method to encrypt binary pictures and shapes. They defined a random grid (RG) as a transparency comprising a two-dimensional array of fully transparent or totally opaque pixels, with the two types of pixels are equally like to occur. In their definition, the average light transmission rate (i.e. the percentage of transparency dots) of a RG is 1/2, and there is no correlation between neighboring pixels in the RG. Superimposing two RGs with the same scale results in three different light transmission rates: (1) When the two RGs are independent, the average light transmission rate is 1/4; (2) When the two RGs are identical, the average light transmission rate is 1/2; and (3) When the two RGs are complementary each other, the average light transmission rate is 0.

They suggested three methods to encrypt a binary image O in two RGs, G_1 and G_2, in such a way that each RG singly reveals no secret information about O, but superimposing G_1 and G_2 pixel by pixel can reveal the patterns on O. We summarized the steps of the three coding methods below.

Algorithm I

Step 1.Generate G_1 as a RG with same scale as O by assigning value 0 (transparent dot) or 1 (black dot) to each pixel of G_1 randomly, with the probabilities for the two alternatives are the same, i.e., $Prob(0)=prob(1)=1/2$.

Step 2. Generate G_2 as a RG with same scale as O using one of the following two substeps:

Step 2.1. If the pixel at position (i, j) of O has value 0, the pixel located on (i, j) of G_2 is copied from the pixel at position (i, j) of G_1.

Step 2.2. If the pixel at position (i, j) of O has value 1, the pixel located on (i, j) of G_2 takes the complement value of the pixel at position (i, j) of G_1.

Algorithm II

Step 1. Generate G_1 as a RG with same scale as O by assigning value 0 (transparent dot) or 1 (black dot) to each pixel of G_1 randomly, with the probabilities for the two alternatives are the same.

Step 2. Generate G_2 as a RG with same scale as O using one of the following two substeps:

Step 2.1. If the pixel at position (i, j) of O has value 0, the pixel located on (i, j) of G_2 is copied from the pixel at position (i, j) of G_1.

Step 2.2. If the pixel at position (i, j) of O has value 1, the pixel located on (i, j) of G_2 takes the value 0 or 1 randomly, with $Prob(0)=prob(1)=1/2$.

Algorithm III

Step 1. Generate G_1 as a RG with same scale as O by assigning value 0 (transparent dot) or 1 (black dot) to each pixel of G_1 randomly, with the probabilities for the two alternatives are the same.

Step 2. Generate G_2 as a RG with same scale as O using one of the following two substeps:

Step 2.1: If the pixel at position (i, j) of O has value 0, the pixel located on (i, j) of G_2 takes the value 0 or 1 randomly, with $Prob(0)=prob(1)=1/2$.

Step 2.2: If the pixel at position (i, j) of O has value 1, the pixel located on (i, j) of G_2 takes the complement value of the pixel at position (i, j) of G_1.

Figure 3 shows an encoding example of Kafri and Keren's three picture encryption algorithms. Panel 3(a) is the secret image, and the two encoded shares and their superimposing result by Kafri and Keren's algorithms I, II, and III are shown in panels (b)–(d), (e)–(g), and (h)–(j), respectively. We can see that the YZU logo appear on the superimposed images. Let the contrast be defined as the absolute difference of light transmission rates between black dot area and white dot area on the stacked RGs. It can easy to evaluate that the contrasts in the three algorithms are 1/2, 1/4, and 1/4, respectively.

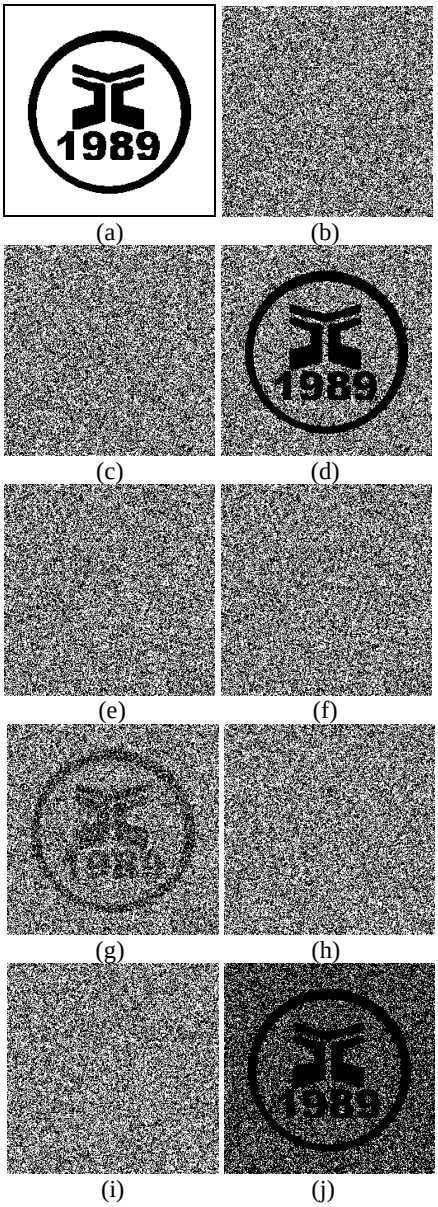


Fig. 3. Kafri and Keren's picture encryption example. The two encoded shares and their superimposing result by Kafri and Keren's algorithms I, II, and III are shown in (b)–(d), (e)–(g), and (h)–(j), respectively.

III. The Proposed Method

The goal of the proposed visual cryptographic scheme is to conceal the secret image O in two noise-like shares, in which any share singly gets no secret information on O, but superimposing the two shares can reveal the patterns on O. One new characteristic of the proposed scheme is that some identification patterns can be disclosed by folding a share up, which facilitates the user to identify and manage the noise-look shares. To meet the above requirement, a secret image O and two identification images D_1 and D_2 are manipulated in a sharing instance. The three images are encoded in two shares S_1 and S_2 which exhibits the following properties: (1) each share is a RG with the same size as O, (2) the content of O can be revealed by superimposing S_1 and S_2, (3) folding up a share will disclose some associated identification patterns. A pictorial illustration for encoding the secret image O and two identification images D_1 and D_2 in two shares S_1 and S_2 using the proposed scheme are depicted in Fig. 4. Details of the proposed method are described below.

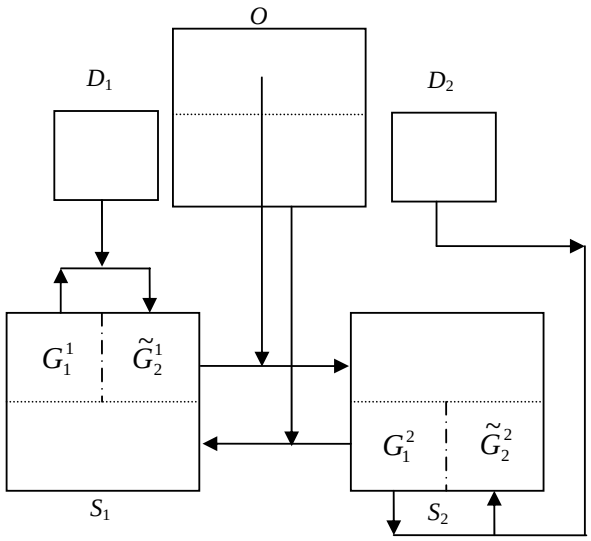


Fig. 4. A pictorial illustration for encoding a secret image O and two identification images D_1 and D_2 in two shares S_1 and S_2 using the proposed VC scheme.

Given the secret image O and two identification images D_1 and D_2, where the size of each of D_1 and D_2 is a quarter of that of O. The two identification images are first encoded using Kafri and Keren's picture encryption algorithm III [9] as shown in Section II. Without loss of generality, let D_1 be encoded in two RGs G_1^1 and G_2^1 applying Kafri and Keren's encoding Method III, and D_2 be encoded in two RGs G_1^2 and G_2^2 applying Kafri and Keren's encoding Method III. The reflections about the y-axis of the two RGs G_2^1 and G_2^2 be denoted by $\tilde{G}_2^1$ and $\tilde{G}_2^2$, respectively. The two RGs G_1^1 and $\tilde{G}_2^1$ are placed beside each other to constitute the top half part of the first share S_1. Similar, the two RGs G_1^2 and $\tilde{G}_2^2$ are placed beside each other to constitute the bottom half part of the second share S_2. The three algorithms proposed for generating the values of the pixels on the bottom half part of S_1 and the top half part of S_2 are summarized below:

Method 1

(a) If the pixel at position (i, j) on bottom half part of O has value 0, the pixel located on (i, j) of S_1 is copied from the pixel at position (i, j) of S_2; otherwise, the pixel located on (i, j) of S_1 takes the complement value of the pixel at

position (i, j) of S_2.

(b) If the pixel at position (i, j) on top half part of O has value 0, the pixel located on (i, j) of S_2 is copied from the pixel at position (i, j) of S_1; otherwise, the pixel located on (i, j) of S_2 takes the complement value of the pixel at position (i, j) of S_1.

Method 2

(a) If the pixel at position (i, j) on bottom half part of O has value 0, the pixel located on (i, j) of S_1 is copied from the pixel at position (i, j) of S_2; otherwise, the pixel located on (i, j) of S_1 takes the value 0 or 1 randomly, with $Prob(0)=prob(1)=1/2$.

(b) If the pixel at position (i, j) on top half part of O has value 0, the pixel located on (i, j) of S_2 is copied from the pixel at position (i, j) of S_1; otherwise, the pixel located on (i, j) of S_2 takes the value 0 or 1 randomly, with $Prob(0)=prob(1)=1/2$.

Method 3

(a) If the pixel at position (i, j) on bottom half part of O has value 0, the pixel located on (i, j) of S_1 takes the value 0 or 1 randomly, with $Prob(0)=prob(1)=1/2$; otherwise, the pixel located on (i, j) of S_1 takes the complement value of the pixel at position (i, j) of S_2.

(b) If the pixel at position (i, j) on top half part of O has value 0, the pixel located on (i, j) of S_2 takes the value 0 or 1 randomly, with $Prob(0)=prob(1)=1/2$; otherwise, the pixel located on (i, j) of S_2 takes the complement value of the pixel at position (i, j) of S_1.

The decoding process of the proposed scheme is conducted as simple as the traditional visual cryptographic scheme does, the secrets on O can be revealed and recognized by superimposing the two shares S_1 and S_2 without any computation. Notably, when fold up a single share S_1 (or S_2), the patterns on the associated identification image D_1 (or D_2) will appear on the folded image, which can be perceived by naked eye and provides useful information for helping users to identify and manage the noise-look shares created in VC schemes.

In the above method of VC by RG with identifiable shares, the size of each of the two identification images D_1 and D_2 is a quarter size of the secret image O, which results in the scale of each of the two generated shares (S_1 and S_2) is the same as O. The security property of a single share in this configuration is discussed below. Without loss of generality, let us examine the security property of share S_1, the security of share S_2 can be analyzed in a similar way. Consider the top half part of S_1, it is constructed by two RGs, one is the first share of D_1 and another is the reflection of the second share of D_1. It is clearly that the top half part of S_1 can reveal the patterns on D_1 by folding it up about y-axis, but it contains no information about the secret image O and the identification image D_2. However, the bottom half part of S_1 is derived from that of O and S_2, where the pixels on the bottom half part of S_2 are correlated in such a way that folding it up about y-axis can reveals the patterns on D_2. Hence, if the three pixels at the same position on the left-bottom quarter image of O, the right-bottom quarter image of O, and D_2 are all message pixels, the pixel at the corresponding position on the folded image of S_1 will also exhibits a message pixel. Figure 5 shows an encoding illustration to depict this phenomenon, where some extra regular patterns are appeared on the bottom half of the folded result of S_1 and the top half of the folded result of S_2. It not only introduces some unnecessary visual patterns on the folded share but also causes security problem to the proposed VC scheme.

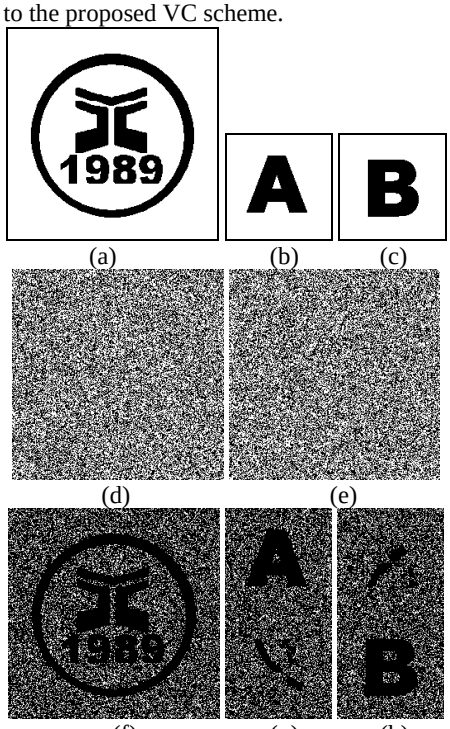
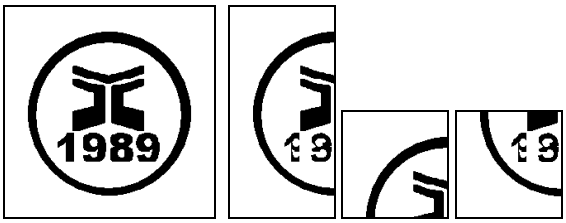


Fig. 5 An illustration of the noise regular patterns occurs on the folded shares. (a) The secret image. (b)(c) Two identification images. (d)(e) Two encoded shares. (f) The superimposing result of the two shares. (g)(h) The folded results of the two shares.

The above mentioned problem can be avoided by applying the following rules to create the patterns on the identification images. For a pixel at position (i, j) on identification image D_1, if the two pixels on the same location (i, j) on the top-left quarter and top-right quarter of O are all message pixels, the position of the pixel is defined as an unsafe position; otherwise, the position is a safe position. The patterns of identification image D_1 are limited to be designed on the areas of safe positions; Similar, for a pixel at position (i, j) on identification image D_2, if the two pixels on the same location (i, j) on the bottom-left quarter and bottom-right quarter of O are all message pixels, the position of the pixel is defined as a unsafe position; otherwise, the position is a safe position. The patterns of identification image D_2 are also limited to be recorded on the areas of safe positions. The above rules enable us to generate two identification images for our VC scheme in such a way that the folding of each generated share reveals only its associated identification patterns, and no secret information about the secret image O can be obtained in a single share. Figure 6

illustrates an example to evaluate the safe areas of the identification images, where the identification patterns can be written in such a way that no extra regular patterns will appear in the folded images in the proposed VC scheme.

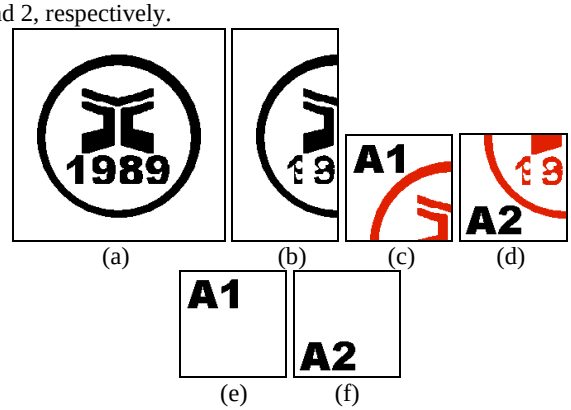


(a) (b) (c) (d)

Fig. 6 An example to evaluate the safe areas for the identification images. (a) The secret image. (b) Result of folding the secret image about the y-axis. (c) The safe areas (depicted in white color) of identification image 1. (d) The safe areas of identification image 2.

IV. Experimental Results

Two simulation results for the proposed VC by RGs scheme with identifiable shares are illustrated in this section to demonstrate the feasibility of the proposed schemes. In the first test, the secret image to be encoded is the YZU logo shown in Fig. 7(a). The folded result of the secret image is shown in Fig. 7(b), and the safe areas for placing the two identification patterns are designed and depicted in Fig. 7(c) and (d), respectively. The images shown in Fig. 7(e) to (f) are the designed identification patterns contain texts "A1" and "A2", they are designed as the identification images for the shares 1 and 2, respectively.

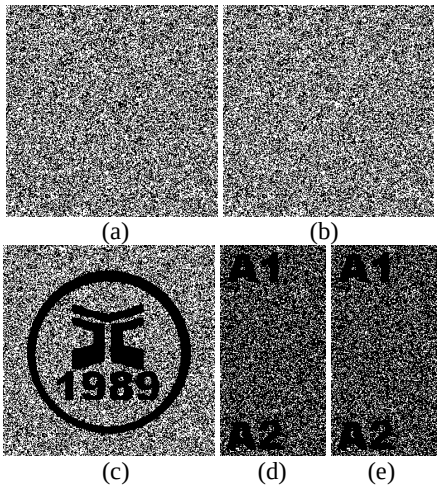


(a) (b) (c) (d)

(e) (f)

Fig. 7 The secret image and two identification images derived from it. (a) Secret image. (b) The folded result of (a). (c)(d) The safe areas of the two identification images. (e)(f) The two designed identification images.

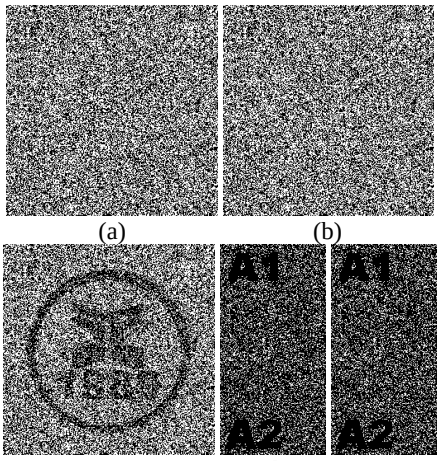
Figures 8 to 10 demonstrate the simulation results using the proposed encoding method I, II, and III, respectively, to encode the secret image and the two identification images shown in Fig. 7 in two shares. In these illustrations, panels (a) and (b) are the two generated shares. The size of each share is the same as that of the secret image, and they all have noisy appearance, the user cannot perceive any meaningful patterns on a single share. Panel (c) is the superimposing result of the two shares, where the YZU logo appears and can be seen by naked eyes. Panels (d) and (e) are the results of folding up the shares shown in Panels (a) and (b), respectively. In the proposed algorithms I and II, we can see the pattern "A1" on identification image 1 and pattern "A2"on identification image 2 all appear on the folded images. In the proposed algorithm III, the pattern "A1" is revealed by folding up share 1, while pattern "A2" is revealed by folding up share 2.



(a) (b)

(c) (d) (e)

Fig. 8 The simulation result of the proposed encoding method I in Experiment 1. (a)(b) Two generated shares. (c) Superimposing result of (a) and (b). (d) The folded result of (a). (e) The folded result of (b).



(a) (b)

(c) (d) (e)

Fig. 9 The simulation result of the proposed encoding method II in Experiment 1. (a)(b) Two generated shares. (c) Superimposing result of (a) and (b). (d) The folded result of (a). (e) The folded result of (b).

Figure 11 is another example of our VC scheme using the proposed encoding method III. In this illustration, panel (a) is the secret image contains text "ICCVIP 2010", panels (b) and (c) are the two identification images contain texts "B1" and "B2", respectively. The two generated shares are shown in panels (d) and (e), and the superimposition result of the two shares is shown in panel (f), where the secrets "ICCVIP 2010" on the original image is revealed and can be recognized by naked eyes. Panels (d) and (e) are the results of folding up the shares shown in panels (a) and (b), respectively. We can see

text “B1” appear on the folded image of share 1, and text “B2” appear on the folded image of shares.

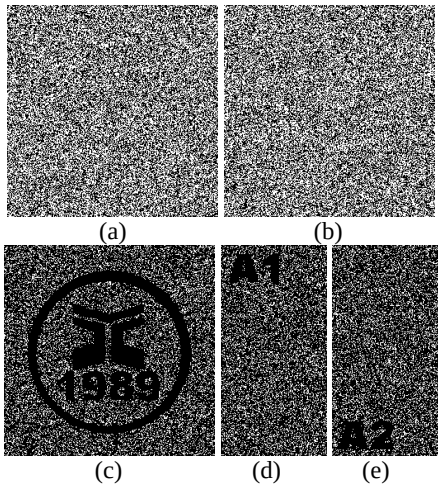


Fig. 10 The simulation result of the proposed encoding method III in Experiment 1. (a)(b) Two generated shares. (c) Superimposing result of (a) and (b). (d) The folded result of (a). (e) The folded result of (b).

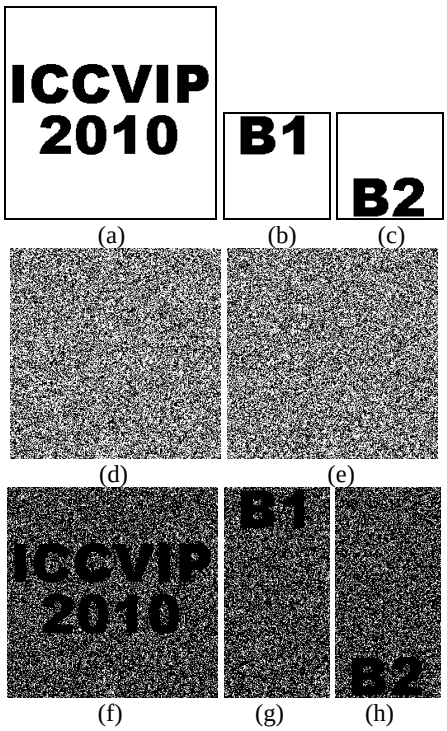


Fig. 11 Another encoding example of the proposed method. (a) the secret image, (b) (c) two identification images, (d) (e) two created shares, (f) the superimposed result of the two shares.

V. Conclusions

A VC by RGs with identifiable shares scheme is proposed in this paper. The proposed scheme owns the same properties as RG-based VC schemes reported in the literature that (1) each generated share is a noise-like RG with the same scale as the original image; (2) a RG singly reveals no secret information while superimposing two RGs reveals the secret patterns on the original image; and (c) the secrets are recognized using naked eye without any computation. Notably, a new characteristic of the proposed scheme is that some designated identification patterns can be revealed by folding a share up and recognized by naked eye easily. The identification patterns can be serve as helpful information for user to identify certain share among many noise-look ones quickly. It provides an easy-to-manage environment for the VC applications where many shares with the same material and scale are created and exhibited.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” *Advances in Cryptography: Eurocrypt’94*, pp. 1–12, 1995.
[2] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, “Visual cryptography for general access structures,” *Information and Computation*, Vol. 129, No. 2, pp. 86–106, 1996.
[3] C. Blundo and A. De Santis and D.R. Stinson, “On the contrast in visual cryptography schemes,” *Journal of Cryptology*, Vol. 12, No. 4, pp. 261–289, 1999.
[4] Y.C. Hou, “Visual cryptography for color images,” *Pattern Recognition*, Vol. 36, No. 7, pp. 1619–1629, 2003.
[5] C.C. Lin and W.H. Tsai, “Visual cryptography for gray-level images by dithering techniques,” *Pattern Recognition Letters*, Vol. 24, pp. 349–358, 2003.
[6] Z. Zhou, G.R. Arce, and G.D. Crescenzo, “Halftone visual cryptography,” *IEEE Transactions on Image Processing*, Vol. 15, No. 8, pp. 2441–2453, 2006.
[7] W.P. Fang and J.C. Lin, “Visual cryptography with extra ability of hiding confidential data,” *Journal of Electronic Imaging*, Vol. 15, No. 2, 0230201–0230207, 2006.
[8] R.Z. Wang, Region Incrementing Visual Cryptography, *IEEE Signal Processing Letters*, Vol. 16, No. 8, pp. 659–662, 2009.
[9] M. Gnanaguruparan and S. Kak, “Recursive hiding of secrets in visual cryptography,” *Cryptologia*, Vol. 26, pp. 68**–**76, 2002.
[10] O. Kafri and E. Keren, “Encryption of pictures and shapes by random grids,” *Optics Letters*, Vol. 12, no. 6, pp. 377–379, 1987.
[11] R. Ito, H. Kuwakado, and H. Tanaka, “Image Size Invariant Visual Cryptography,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, E82, No. 10, pp. 2172–2177, 1999.
[12] C.N. Yang and T.S. Chen, “Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion,” *Pattern Recognition Letters*, Vol. 26, No. 2, pp. 193–206, 2005.
[13] C. Blundo, S. Cimato and A.D. Santis,” Visual cryptography schemes with optimal pixel expansion,” *Theoretical Computer Science*, Vol. 369, pp. 169–182, 2006.
[14] S.J. Shyu, “Image encryption by random grids,” *Pattern Recognition*, Vol. 40, No. 3, pp. 1014–1031, 2007.
[15] S.J. Shyu, “Image encryption by multiple random grids,” *Pattern Recognition*, Vol. 42, No. 7, pp. 1582–1596, 2009.
[16] T.H. Chen, and K.H. Tsao, “Visual cryptography by random grids revisited,” *Pattern Recognition*, vol. 42, pp. 2203–2217, 2009.
[17] T.H. Chen, K.H. Tsao and K.C. Wei, “Multiple-Image Encryption by Rotating Random Grids,” *Proceedings of the 9th Inter. Conf. on Intel. Systems Design and Applications*, pp. 252–256, 2009.