2012 Sixth International Conference on Genetic and Evolutionary Computing

Verifiable Visual Cryptography

Shuo-Fang Hsu[1], Yu-Jie Chang[2], Ran-Zan Wang[3,*], Yeuan-kuen Lee[4], Shih-Yu Huang[4]
[1]Dept. of Comput. Sci., National Chiao Tung Univ., HsinChu, Taiwan
[2]Dept. of Comput. & Comm. Eng., National Kaohsiung First Univ. of Science & Technology, Kaohsiung, Taiwan
[3,*]Dept. of Comput. Sci. & Eng., Yuan Ze Univ., Taoyuan, Taiwan. Corresponding author, email: rzwang@saturn.yzu.edu.tw
[4]Dept. of Comput. Sci. & Info. Eng., Ming Chuan Univ., Taoyuan, Taiwan

***Abstract*—The paper presents a verifiable visual cryptography (VC) scheme for checking the validness to the shares engaged in a VC decoding instance. The idea is to stamp a continuous pattern on the shares belonging to the same secret image, and a part of the pattern can be revealed through aligning and stacking half of two shares together. The visual coherent among the revealed patterns of all pair of shares provides evidence to the genuine of the shares engaged in the decoding process. Compare to the reported cheating prevention VC schemes, the proposed scheme maintains the original pixel expansion in VC scheme without cheating prevention ability, and the share verification process is done without resorting to any additional verification image. Besides, the proposed verification mechanism can easily be attached to any VC schemes in the literature to endow legitimate user with the ability to prevent cheating from malicious participants.**

Keywords- Visual Cryptography; Secret Sharing, Image Sharing, Cheating Prevention

I. INTRODUCTION

Visual Cryptography (VC) is a secret sharing scheme for protecting image-based secret. It was introduced by Noar and Shamir [1] in 1995, thereafter attracted many researchers' attention and many schemes were proposed to improve the efficiency and exhibit different revealing effects to the secret image. In a typical (t, n)-threshold VC scheme, the input image is encoded to n transparent shares in such a way that any subset of t ($2 \leq t \leq n$) or more shares can decrypt the secret, but no secret information can be revealed from any t–1 or fewer shares. The decryption process of VC is carried out by carefully aligning and stacking the gathered shares, where the patterns about the secret will occur on the stacked shares and can be inspected and recognized using naked eye without any computation. The nice property of decoding the secret without any computation makes the technique possible and welcome for sharing secrets in the environment without sufficient computing power. In general, pixel expansion and luminance difference are two most important properties used to measure the efficiency to a VC scheme, the pixel expansion refer to the number of pixels in a share used to encode a pixel of the secret image, and the contrast is the luminance difference between the area of black pixels and the area of white pixels in the stacked image. Smaller pixel expansion and higher contrast are considered good properties for a VC scheme, and are the mainly research topics in VC schemes [2–7] investigated in the past two decades. There are many other VC schemes developed to explore the capability and diverse revealing effects to the secret. Halftone VC schemes [8–9] encode the secret image in natural-look shares to decrease the suspicious of the track about the secret. Multi-secret VC schemes [10–11] encode more than one secret among the shadow images to increase the payload in a sharing instance. Progressive VC scheme [12] displays the secret image gradually in quality while incrementing VC scheme [13] discloses more number of secrets when more shares are superimposed.

In 1999 Yang and Laih [14] presented two cheating prevention VC schemes to break the misleading secrets forged by dishonest participants. The first method generates an additional verification share to check the validness to each share, where the verification share should be hold by the trusted authority (TA) to verify the validness to each share. The second method transforms a conventional VC scheme to another cheating-prevention VC scheme with greater pixel expansion in each generated shares. The stacking of any two shares reveals the verification image, which can be inspected by user to check the validness to the shares. In 2006 Horng et. al. [15] demonstrated a process of collusive cheating by n+1 participants to the other user in (2, n) VC schemes, and presented two simple possible solutions to address the problem. The first method generates a dedicated verification share to each participant, which can be applied to investigate the genuine of the shares gathered form other participants. The second one uses a (2, n+l), $l \geq 1$, VC scheme instead of (2, n) scheme in a 2-out-of-n coding instance, that frustrates the malicious user in predicting the structure the transparencies possessed by other participants. Later, Hu and Tzeng [16] presented three robust methods to improve the weaknesses of previously cheating prevention VC schemes [14, 15], two for conventional VC and another for extended VC. However, like the previous cheating prevention VC schemes in [14, 15], additional verification share or greater pixel expansion is required to endow the ability about resisting cheating against malicious participants.

In this paper, a novel verification mechanism for checking the validness to the revealed secret in VC schemes is proposed. The idea is by stamping a continuous pattern on the shares belonging to the same secret image to serve as evidence for later checking the genuine to these shares. The user can visually inspect the coherence among the revealed patterns to assure the genuine to the shares participated in the

978-0-7695-4763-3/12 $26.00 © 2012 IEEE
DOI 10.1109/ICGEC.2012.150

IEEE computer society

decoding instance, and assures the correctness to the revealed secrets. The remainder of this paper is organized as follows: Section 2 presents the proposed scheme. Experiment and simulation results are shown in Section 3, and a brief conclusion is made finally in Section 4.

II. The Proposed Scheme

Given a set of n binary shares $\{S_1, S_2, \ldots, S_n\}$ of an image O generated in a VC coding instance, with each share has scale $h \times w$. A binary verification image V with scale $h \times w \times n/2$ is created and a verification pattern Q is designed and drawn on V to provide evidence for later checking the validness to the shares engaged in a decoding instance. Let $V_1, V_2, \ldots, V_n$ denote n disjoint partitions of V such that

$$\begin{cases} \bigcup_j V_j = V \quad \text{for} \quad 1 \le j \le n, \\ P_i \cap P_j = \varnothing \quad \text{for} \quad 1 \le i \ne j \le n, \\ \text{Size}(V_i) = \frac{1}{n}\text{Size}(V) \quad \text{for} \quad 1 \le i \le n. \end{cases} \tag{1}$$

In this study, an authentication pattern Q is said to be effective if it satisfies the following two requirements: (1) all of the n partitions V_j, $j = 1, 2, \ldots, n$ are partially occupied by Q , and (2) the pattern of Q should visually smooth across every two adjacent partitions V_j and $V_{(j+1)\%n}$. Figure 1 shows some examples of authentication pattern in an authentication image with three partitions separated by red lines. The pattern shown in panel (a) satisfies all of the above two requirements and is considered effective. The pattern in panel (b) is ineffective because no authentication pattern is drawn on partition 1, which violates the requirement (1) mentioned above. The pattern drawn in panel (c) is also not an effective pattern due to the inconsistency in the boundary of the left partition and the middle partition, which violates the second requirement of an effective authentication pattern.

Let $\Psi(S_i, S_j)$ denote the operation of superimposing two shares S_i and S_j partially in such a way half of the two images are overlapped (for example, the right-half of S_i is overlapped with left-half of S_j), the proposed scheme stamps V on the n shares that exhibit the following properties:

$$\begin{cases} \Psi(S_j, S_{(j+1)\%n}) = V_j \quad \text{for } 1 \le \ j \le n, \\ \bigcup_i V_i = V, \ \text{for} \quad 1 \le i \le n, \end{cases} \tag{2}$$

That is, 1) each two consecutive shares can reveal a partition of V by superimposing them in half-size, 2) the whole V can be revealed by arranging all of the n shares sequentially in a cylinder, with each adjacent two shares are half overlapped.

The stamping of V on the n shares is done by stamping each of the n partitions V_j, j=1, 2, …, n in two consecutive shares S_j and $S_{(j+1)\%n}$. Without loss of generality, the process of stamping V_1 on shares S_1 and S_2 is introduced, and the processes of stamping the V_j, j=2, …, n can be done using similar process.

The probabilities of white pixel and black pixel are assumed the same in all of the shares generated in a coding instance, which is the usual case in most of the VC schemes. Let P_0 and P_1 be the probabilities of white pixel and black pixel in a share. Note that the size of V_1 is equal to a half of that of a share, hence the three images include V_1, left-half of S_1, and right-half S_2 are with the same dimension. In this study the pixels located on the same positions in the three images are defined as the corresponding pixels.

The following steps are conducted to stamp V_1 on shares S_1 and S_2 :

1) Fetch a pixel p from V_1 sequentially in scan order, (i.e. from left to right and from top to bottom), and then examine the colors of the two corresponding pixels, q_1 in S_1 and q_2 in S_2. Encode p using one of the following two encoding rules:

2a) If the color of p is black, the colors of q_1 and q_2 are both white, one of q_1 and q_2 is selected with equal probabilities, and the color of the selected pixel is set to black.

2b) If the color of p is white, the color of the q_1 is white and the color of q_2 is black, set the color of q_1 to black in a probability $P_0/2$.

2c) If the color of p is white, the color of q_1 is black and the color q_2 is white, set the color of q_2 to black in a probability $P_0/2$.

2d) If the color of p is white, the color of q_1 and q_2 are both white, set the color of q_1 to black in a probability $P_0/2$, and q_2 to black in a probability $P_0/2$.

3) Repeat Steps 1 and 2 until all of the pixels in V_1 are processed. The verification image partition V_1 is stamped in shares S_1 and S_2.

The above process is applied to stamp all of the partitions of the authentication pattern in shares $\{S_1, S_2, \ldots, S_n\}$ to get n verifiable shares $\{\hat{S}_1, \hat{S}_2, \ldots, \hat{S}_n\}$. Note that each cheating prevention share $\hat{S}_j, j = 1,2,..,n$ contains authentication patterns in the two authentication partitions V_j and $V_{(j+1)\%n}$. In the decoding phase, when a user receives share(s) from other user, he can stack the share with his own share (which is assumed definitely genuine) such that half of the two shares are overlapped to reveal the authentication patterns. The gathered shares are considered genuine only if these revealed patterns are continuous in the boundary, and are claimed as fake shares otherwise. If the above authentication process shows that all of the shares gathered are valid. The secret decoding process is done by stacking and aligning a set of qualified shares together done as the VC scheme which encodes the shares without stamping the authentication pattern does. The secrets in the secret image will be revealed on the stacked image.

III. Similation Results

Two experiments are conducted to demonstrate the effectiveness of the proposed scheme. In the first experiment, the conventional matrix-based VC scheme proposed by Noar and Shamir [1] are selected to test the verification capability of the proposed scheme. Figure 2 is a computer simulation result of the (2, 2) verifiable VC scheme in this experiment, where Fig. 2(a) is the 256×256 secret image containing secret text "ICGEC 2012", 2(b) is the authentication image on which two solid ellipses are drawn. The two generated shares using Noar and Shamir's scheme are shown in Figs. 1(c) and (d), the probability of a pixel to be black on all pixels of the two shares are all 1/2, which makes the shares noisy and with no secret being obvious. The superimposing result of the two shares is shown in Fig. 1(e), on which the secret text "ICGEC 2012" appears and can easily be recognized by naked eye. Figures 1(f) and (g) are the two shares with verification pattern stamped inside, that are obtained using the proposed scheme. It can be seen that the appearances of the two shares are also uniform and noisy. The superimposing result of left-half of 1(f) and right-half of 1(g) is shown in Fig. 1(h), we can see a half of the authentication pattern appear on the stacked image. The superimposing result of right-half of 1(f) and left-half of 1(g) is shown in Fig. 1(i), where the other half of the authentication is revealed on the stacked share. If we overlap the two shares in 1(f) and 1(g) half-by-half and arrange the result in a cylinder, we can see all of the authentication patterns revealed on the stacked share. The superimposing result of 1(f) and 1(g) entirely is shown in Fig. 1(k), where the secret text "ICGEC 2012" is revealed and can easily be recognized by naked eye.

The second experiment applied the probabilistic-VC to generate the shares for stamping the authentication patterns. Figures 3 is the computer simulation results of (2, 2) verifiable VC sharing instance in this experiment. In this experiment the size of each share is the same as that of the secret image, and the size of the authentication image is also same with that of the secret image. Again we can see that the appearances the generated shares are noisy and with no secret being obvious, and the authentication pattern is revealed by superimposing the two shares half-by half, which serves as the evidence for verifying the validness to the shares engaged in the decoding process.

IV. Conclusion

This paper presents a novel method to prevent legitimate user from cheating by misleading secrets provided by malicious users in VC schemes. Given a set of shares belonging to a secret image that can be generated using any reported VC scheme, a verification pattern stamping process is designed to stamp an authentication pattern on these shares to support evidence to the genuine of these shares. Like the decoding process of a typical VC schemes does, the secrets in the secret image can be revealed by fully stacking and aligning any subset of qualified shares. Furthermore, aligning and stacking half of two consecutive shares will display a part of the verify pattern, and the coherent among the revealed patterns supports evidence about the genuine to the shares engaged in the decoding process. The proposed share verification mechanism is simple but efficient, it can easily be added to any VC schemes to endow the legitimate participant with the ability of preventing cheating against dishonest participants.

References

[1] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptography: Eurocrypt'94*, pp. 1–12, 1995.

[2] C. Blundo, 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.

[3] S. Cimato, A. De Santis, A.L. Ferrara and B. Masucci, "Ideal contrast visual cryptography schemes with reversing**,"** *Information Processing Letters*, Vol. 93, No. 4, 28, pp. 199–206, 2005.

[4] 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.

[5] C. Blundo, S. Cimato and A.D. Santis, "Visual cryptography schemes with optimal pixel expansion," *Theoretical Computer Science*, Vol. 369, No. 1-3, pp. 169–182, 2006.

[6] T.L. Lin, S.J. Horng, K.H. Lee, and P.L. Chiu "A novel visual secret sharing scheme for multiple secrets without pixel expansion," *Expert Systems with Applications*, Vol. 37, No. 12, pp. 7858–7869, 2010.

[7] S.J. Shyu and M.C. Chen,"Optimum pixel expansions for threshold visual secret sharing schemes," *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 3, pp. 960–969, 2011.

[8] 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.

[9] Z. Wang, G.R. Arce and G.D. Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Transactions on Image Processing*, Vol. 4, No. 3, pp. 383–396, 2009.

[10] S.J. Shyu, S.Y. Huang, Y.K. Lee, R.Z. Wang and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognition*, Vol. 40, No. 12, pp. 3633–3651, 2007.

[11] T.L. Lin, S.J. Horng, K.H. Lee, and P.L. Chiu, "A novel visual secret sharing scheme for multiple secrets without pixel expansion," *Expert Systems with Applications*, Vol. 37, No. 12, pp. 7858–7869, 2010.

[12] D. Jin, W.Q. Yan, and M.S. Kankanhalli, "Progressive color visual cryptography," *Journal of Electronic Imaging*, Vol. 15, No. 3, pp. 033019: 1–13, 2005.

[13] R.Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Processing Letters.* Vol. 16, No. 8, pp. 659–662, 2009.

[14] C.N. Yang and C.S. Laih, "Some new types of visual secret sharing schemes," *in Proc. Nat. Computer Symp.*, Vol. 3, pp. 260–268, 1999.

[15] G.B. Horng, T.H. Chen, and D.S. Tsai, "Cheating in Visual Cryptography," *Designs, Codes and Cryptography*, Vol. 38, pp. 219–236, 2006.

[16] C.M. Hu and W. G. Tseng, "Cheating prevention in visual cryptography," *IEEE Transactions on Image Processing*, Vol. 16, No. 1, pp. 36–45, 2007.

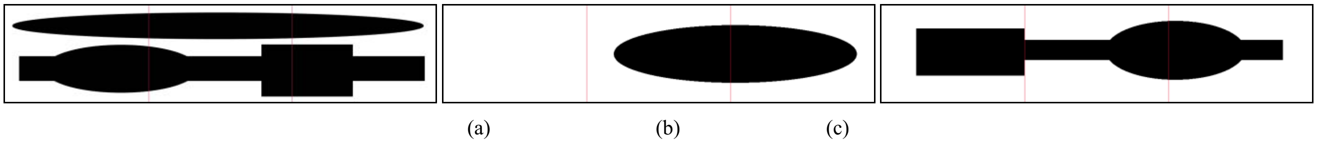

Fig. 1 Examples of effective and ineffective patterns for an authentication image with three equal-partitions.

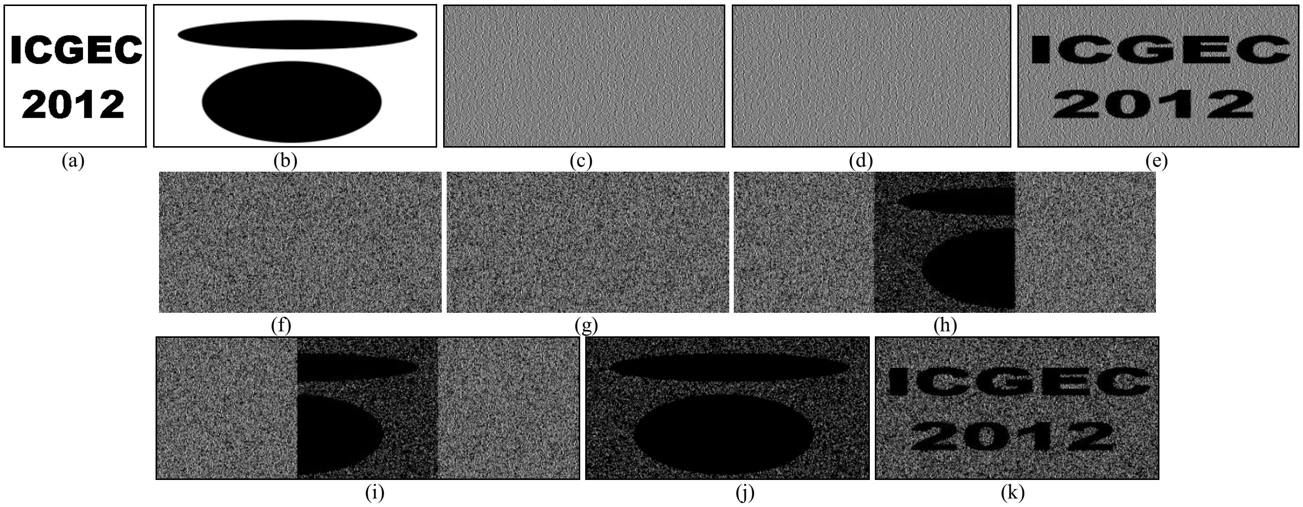

Fig. 2 Simulation results of experiment I. (a) Secret image, (b) Verification image, (c)(d) Two generated shares, (e) Superimposing result of (c) and (d), (f)(g) the two shares obtained in the proposed scheme, (h) Superimposing result of left-half of (f) and right-half of (g), (i) Superimposing result of right-half of (f) and left-half of (g), (j) The reveal pattern by cylinder, (h) and (i) in a circle, (k) Superimposing result of (f) and (g).

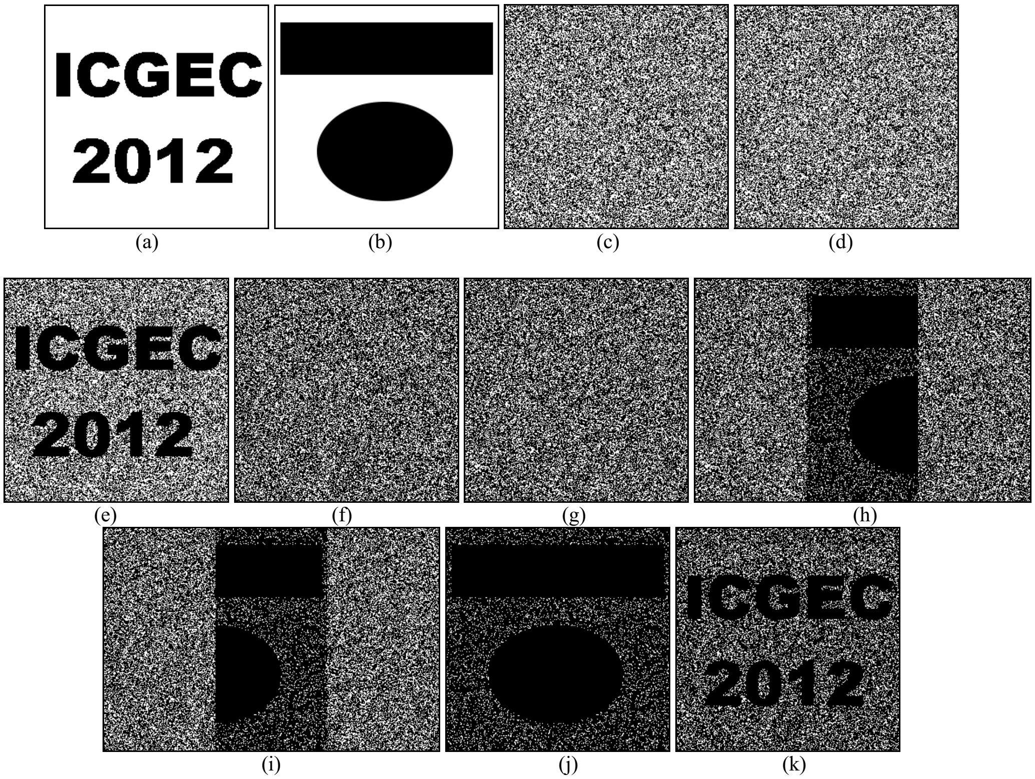

Fig. 3 Simulation results of experiment II. (a) Secret image, (b) Verification image, (c)(d) Two generated shares, (e) Superimposing result of (c) and (d), (f)(g) the two shares obtained in the proposed scheme, (h) Superimposing result of left-half of (f) and right-half of (g), (i) Superimposing result of right-half of (f) and left-half of (g), (j) The reveal pattern by cylinder, (h) and (i) in a circle, (k) Superimposing result of (f) and (g).