

A Novel Weighted Visual Cryptography Scheme with High Visual Quality

I-Chun Weng, Tzung-Her Chen
(Corresponding author: Tzung-Her Chen)

Department of Computer Science and Information Engineering, National Chiayi University
Chiayi 600, Taiwan, R.O.C.

(Email: thchen@mail.ncyu.edu.tw)

(Received Sept. 6, 2016; revised and accepted Jan. 15, 2017)

Abstract

Visual Cryptography (VC) has been developed to encode a secret image into n shares for n participants in the past decades, in which each share is treated with the same priority. However, the privilege for participants in a group is not always the same. In this paper, a weighted visual cryptography scheme is proposed such that each participant obtains her/his share with different weight according to the different group of predefined privilege. The secret can be disclosed only if stacking predefined k or more shares in which containing predefined some specific shares from the specific groups. Otherwise, no information about the secret can be revealed. It is worthwhile to note that the higher value of total weight of stacking shares; the more information about the secret revealed from the stacked result. The experimental results demonstrate that the proposed scheme does work.

Keywords: Random Grid; Visual Secret Sharing; Weighted Visual Cryptography

1 Introduction

With the technology continually upgrading and improving, people communicate each other on the Internet conveniently. However, the security for the transmission of information through the public channel will be taken into consideration seriously. To this end, traditional cryptography, including DES, AES and RSA [12, 16], has been well-defined to guarantee confidentiality, authentication, integrity, etc. Security of these computational cryptographic tools is determined by the strength of encryption/decryption key's length. This draws the security to be relative but not absolute.

Visual Secret Sharing (VSS) has drawn much attention in academia, in which the concept of k -out-of- n threshold is presented to encode a secret into n share images by a codebook and, then, recover the secret by recognizing the stacked result of at least k share images ($2 \leq k \leq n$).

Compared with traditional encryption, VSS offers unbreakable encryption if less than k meaningless share images are collected. Furthermore, VSS provides the decryption operations without the needs of cryptographic knowledge and computational devices. It is worthwhile to note that VSS is suitable for the applications of high-security needed and without computational devices given.

Within VSS there are three categories: (1) Visual Cryptography (VC) [11]; (2) Probabilistic VC (PVC) [19]; and (3) Random Grid-based (RG) [3, 8]. It is a trade-off between adopting VC or PVC/RG techniques. It is well-known that VC has two main disadvantages: codebook design and pixel expansion [3] while size-invariant PVC/RG has one main concern compared with VC, i.e., lower visual quality of reconstructed secret image. However, the size of pixel expansion seems not always a problem nowadays since of the rapid development of Internet bandwidth and display resolution including HDTV, smart phone, digital camera/recorder, etc. At this stage, VC does not have its own grievances in terms of pixel expansion.

VSS is further extended in various application, such as Progressive VSS [5], General Access Structure (GAS) [1], (k, n)-threshold based VSS [13], Meaningful VSS [4], Multi-secret VSS [6], etc. By the way, Secret Image Sharing (SIS) [15] performs secret sharing like VSS, but computational devices are needed to encode and decode.

A traditional VSS mechanism assumes that each share is treated as the same priority. However, the privilege for participants is not always the same. Hence, the assumption does not reflect the actual situation in real life because everyone stays in different level of job with different duty. For example, the company is composed of the different level of employees. Simultaneously, these employees can be further subdivided into the general manager, the manager and the staff. It is reasonable that a staff of k or more has the same privilege as the manager's. Likewise, only k or more managers have the same privilege as the general manager's.

In the literature, there are several VSS or SIS schemes

taking privilege into account. Chen et al. [2] proposed a weighted SIS method, in which the encoding process is divided into two phases. Firstly, sharing shares generated by a (k, n) threshold SIS scheme obtain the same weight. Secondly, these shares are further divided into some groups. The final shares of each group with different privilege are generated respectively. Inspired by the previous SIS method, Lin et al. [10] and Shyu et al. [14] presented their weighted SIS schemes.

Li et al. [9] proposed the (t, s, k, n) -Essential secret image sharing (ESIS) scheme, in which the traditional threshold property is combined with the essential property in the decoding process. ESIS generates n shares containing s essential shares and $(n - s)$ non-essential shares. Within k or more shares including t or more essential shares, the hidden secret can be disclosed computationally; otherwise, no secret is revealed.

Yan et al. [18] further extend Li et al.'s SIS scheme to form (k_0, n_0, k, n) -Essential RG-based scheme. In Yan et al.'s scheme, participants are divided into two group: *essential* and *non-essential*. In the decoding process, the essential share is essential to disclose the secret; otherwise, no secret is revealed without any *essential* share. There are n shares which contain n_0 essential shares and $n - n_0$ non-essential shares. Only k or more shares within containing at least k_0 essential shares can be used to recover the secret. Since Yan et al. adopt a size-invariant VSS scheme, for instance, Wu and Sun's RG-based VSS scheme [17], the visual quality of disclosed secret is potentially concerned.

In 2015, the concept of privilege is introduced into VC by Hou et al. [7] to benefit from the following advantages: (1) each share with an predefined capability to disclose the secret according to the participant's privilege; (2) the disclosed secret with a better contrast; and (3) shares with size of the original secret. However, Hou et al.'s scheme does not support the concept and the related property of "essential group".

In order to benefit the superiority of visual quality compared to the RG-based VSS [18] and of supporting the property of "essential group", this paper proposes a weighted visual cryptography scheme such that each participant obtains the share with different weight according to the different-privilege group predefined. It is worthwhile to note the proposed scheme achieves progressive-recovery of secret. That is, the higher value of total weight of stacking shares; the more information about the secret revealed from the stacked result. The experimental results demonstrate that the proposed scheme does work.

The rest of this paper is organized as follows. The related works are given in the next section. The present scheme is described in Section 3. Section 4 demonstrates the experimental results, respectively. Further discussions and conclusions are given in Sections 5 and 6.

2 Related Works

This section gives the brief review of traditional VC and weighted RG-based VSS.

2.1 Visual Cryptography

Visual cryptography (VC), proposed by Naor and Shamir [11] in 1995, encodes a secret image into a number of meaningless shares. The secret can be recognized by the human visual system and disclosed by stacking share upon satisfying recovering threshold condition.

Table 1: The codebook of $(2, 2)$ VC scheme and the stacking results















Secret pixel		
Share S_1	 	 
Share S_2	 	 
Stacking result	 	 

Table 1 shows the codebook of a $(2, 2)$ VSS scheme. The dealer uses the codebook to generate two shares, S_1 and S_2 . Each secret pixel is corresponding to the defined 1×2 pixels according the codebook. In such a way, the size of a share is twice as big as the secret. When S_1 and S_2 are stacked together, the secret can be disclosed.

2.2 Weighted Visual Secret Sharing Based on Random Grid

Inspired from Li et al.'s SIS scheme [9], Yan et al. [18] propose a (k_0, n_0, k, n) -essential and non-essential RG-VSS scheme, in which the encoding process is divided into two steps.

Step 1. Encoding a binary secret image into $n_0 + 1$ essential shares by $(k_0 + 1, n_0 + 1)$ RG-based VSS, like $SC_1, SC_2, \dots, SC_{n_0}, \widetilde{SC}_{n_0+1}$. The share \widetilde{SC}_{n_0+1} is further encoded to generate non-essential shares.

Step 2. Encoding \widetilde{SC}_{n_0+1} into $n - n_0$ non-essential shares by $(k - k_0, n - n_0)$ RG-based VSS, like $SC_{n_0+1}, \dots, SC_{n-1}, SC_n$.

Therefore, \widetilde{SC}_{n_0+1} can be restored by stacking some $k - k_0$ or more non-essential shares. The secret image can be disclosed by stacking k or more shares in which containing k_0 or more essential shares.

Note that the VC-based VSS has its superiority of visual quality compared to the RG-based VSS. It benefits to present a VC-based weighted VSS scheme.

3 Proposed Method

The proposed VC-based weighted VSS scheme consists of encoding and decoding phases. An example is given to clear the processes.

Assume there are n participants P_1, P_2, \dots, P_n classified into two sub-group: n_0 *specific* participants and $n - n_0$ *general* participants. And at least k_0 out of n_0 specific participants are essentially asked to take part in the secret disclosing operations. Furthermore, $k - k_0$ or more out of $n - n_0$ *general* participants have the same privilege as one *specific* participant. Note that there are at least k participants asked to disclose the secret.

Encoding process is divided into four steps: pre-processing, temporary-share generation, *specific*-share generation, and *general*-share generation.

Step 1. Pre-processing: According predefined k_0 and n_0 (resp. $k - k_0$ and $n - n_0$), design the codebook CB_A of $m \times (n_0 + 1)$ matrix C_A^0 and C_A^1 (resp. CB_B of $m \times (n - n_0)$ matrix C_B^0 and C_B^1) for decoding the white (resp. black) pixels of a secret image and within each row is presented a sharing method in which a participant is assigned. Tables 3 and 4 show the codebook examples of CB_A and CB_B .

Within Table 2 (Resp. 3) there are two groups: a white group and a black group. If a certain pixel of a secret image is white, participants are assigned codewords by randomly selecting one of the cases in the white group. On the contrary, if the secret pixel is black, the codewords are selected from the black group.

Table 2: The codebook CB_A of 4×3 sharing metrics used for (3,3) VC case

C_A^0	C_A^1
$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}_{4 \times 3}$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}_{4 \times 3}$

Table 3: The codebook CB_B of 4×4 sharing metrics used for (2,4) VC case

C_B^0	C_B^1
$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}_{4 \times 4}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}_{4 \times 4}$

Step 2. Temporary-share generation: A secret image S with size of $w \times h$ is decoded to generate $n_0 + 1$ temporary shares by decoding a secret pixel 0/1 (denoted white/black) according to C_A^0 and C_A^1 by a $(k_0 + 1, n_0 + 1)$ VC scheme. Finally, the $n_0 + 1$ temporary shares of size $4w \times h$ are generated.

Step 3. Specific-share generation: Carry on Step 2. n_0 temporary shares are further expanded into the shares of size $4w \times 4h$ assigned to specific participants. Note that here a pixel is extended into four ones by duplicating a pixel into four.

Step 4. General-share generation: The last temporary share is used to generate $n - n_0$ shares assigned to all general participants. Here, a pixel of the temporary share image is decoding according to C_B^0 and C_B^1 by a $(k - k_0, n - n_0)$ VC scheme. Finally, the $n - n_0$ general shares of size $4w \times 4h$ are generated.

Example 1. Assume the access structure is defined $(k_0, n_0, k, n) = (2, 2, 4, 6)$. There are $n = 6$ participants in which two members have the higher privilege and the others have the general privilege. First, a 512×512 secret image S is encoded into three temporary shares of size 2048×512 by (3,3) VC in Table 2. If a secret pixel is white (black), the sharing matrix C_A^0 (C_A^1) is referred. When the generated two shares of size 2048×2048 are assigned to the two participants of higher privilege. Finally, the third temporary share is encoded below. If a pixel of the temporary share is white (black), the sharing matrix C_B^0 (C_B^1) in Table 3 is referred to generate four shares with size of 2048×2048 by (2,4) VC and, then, assign the generated three shares to the general members.

4 Experimental Results

Carry on the example given in Section 3 and the access structure is defined $(k_0, n_0, k, n) = (2, 2, 4, 6)$. The 512×512 secret image S in Figure 1(a) is encoded into six 2048×2048 shares as $S_1, S_2, S_3, S_4, S_5, S_6$ in Figure 1 (b)-(g), in which S_1, S_2 for specific members with higher privilege, and S_3, S_4, S_5, S_6 for the other general members.

As the access structure is defined $(k_0, n_0, k, n) = (2, 2, 4, 6)$, if stacking any two or three shares, no secret is revealed as shown in Figures 2 and 3.

As the access structure is defined $(k_0, n_0, k, n) = (2, 2, 4, 6)$, if stacking both S_1 and S_2 with at least two shares out from $S_3, S_4, S_5,$ and S_6 , the secret can be disclosed as shown in Figure 4(a)-(f) and Figure 5(a)-(d) and (g). Otherwise, the stacked results are noise-like as shown in Figure 4(g)-(o) and Figure (e)-(f).

The experimental results presented above demonstrate that the proposed scheme does work and the secret can be disclosed and recognized by the human visual system under the predefined privilege policy.

5 Discussions

The proposed scheme presents a new VC-based VSS scheme with the following properties.

- 1) **Privilege:** The participants are classified into different groups. The high-privilege members are asked to essentially participate to disclose the secret.

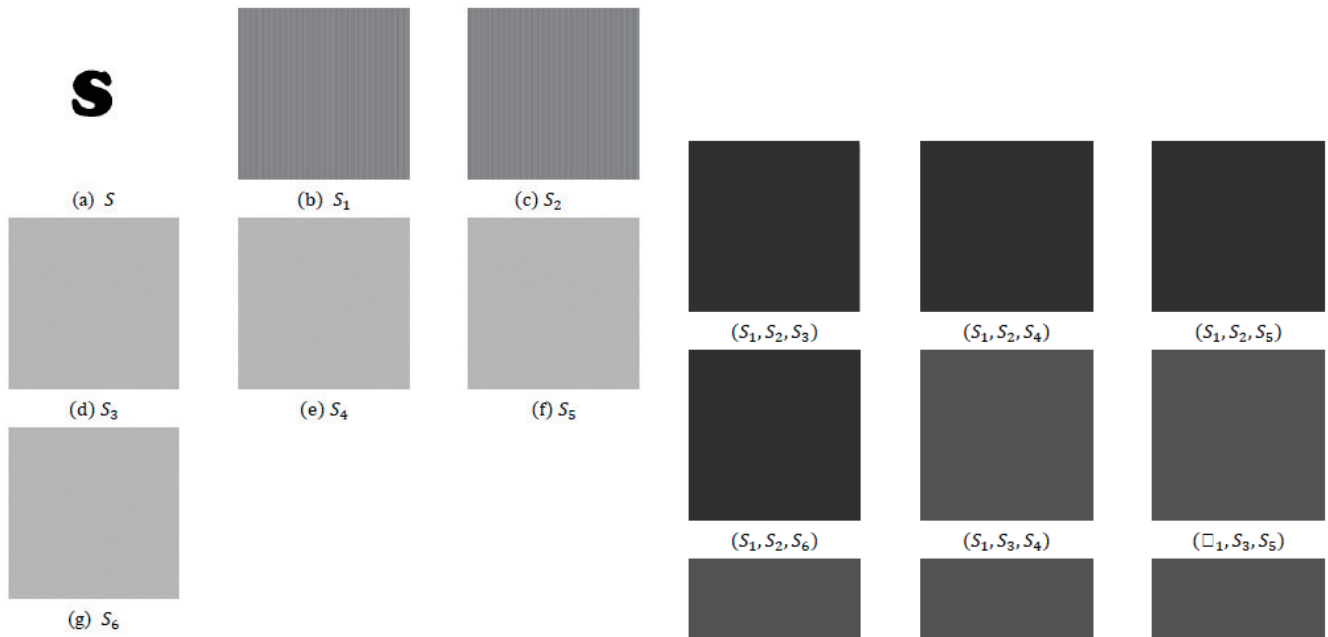


Figure 1: (a) secret image S; (b)-(c) special shares with higher weight; and (d)-(g) general shares

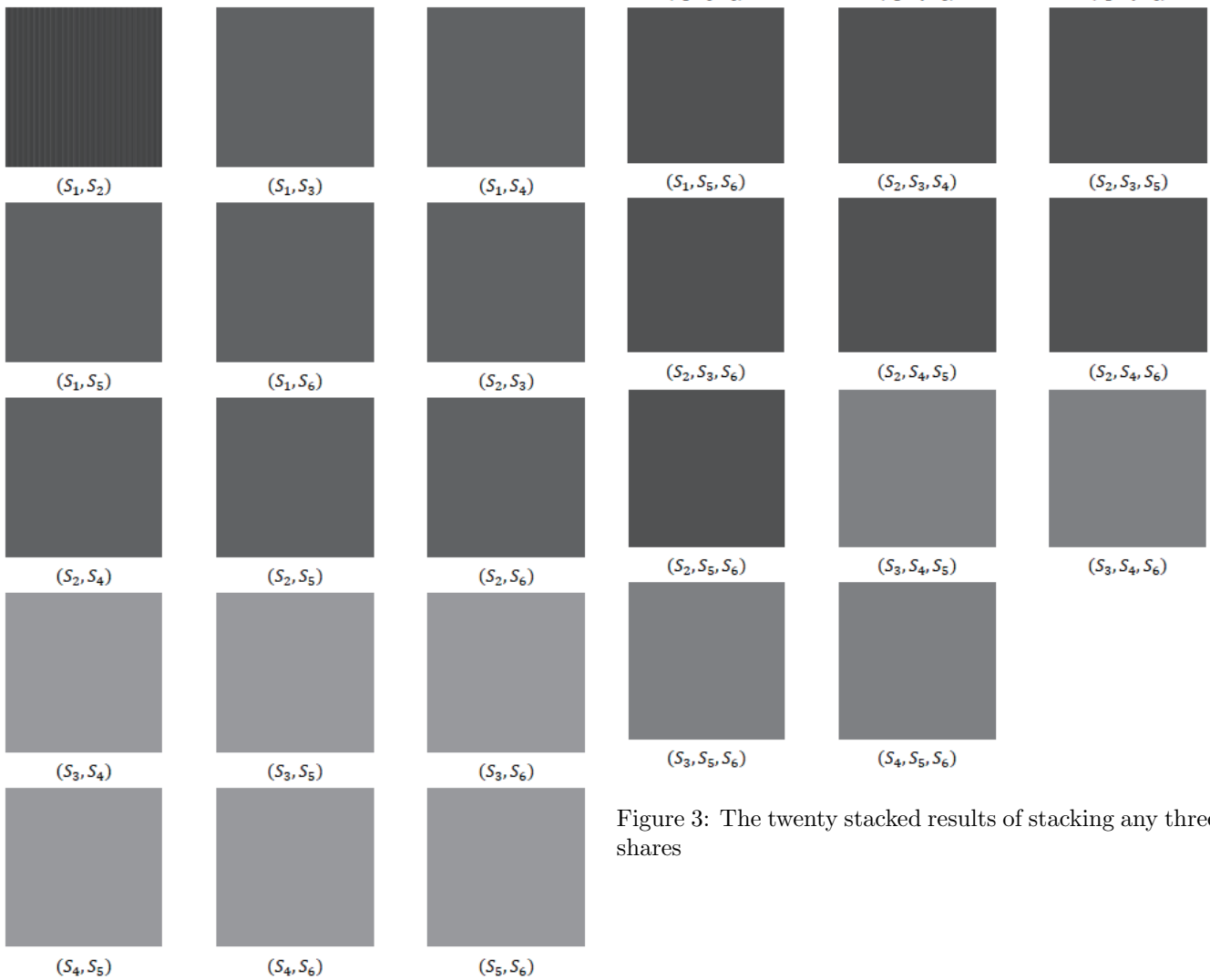


Figure 2: The fifteen stacked results of any two from six shares

Figure 3: The twenty stacked results of stacking any three shares



Figure 4: (a)-(f) the stacked results including two specific shares and two general ones; (g)-(o) the stacked noise-like results

Table 4: The contrast values in the experimental results

Stacked results	Contrast
(S_1, S_2, S_3, S_4)	0.0553059
(S_1, S_2, S_3, S_5)	0.0552645
(S_1, S_2, S_3, S_6)	0.0553177
(S_1, S_2, S_4, S_5)	0.055266
(S_1, S_2, S_4, S_6)	0.0553192
(S_1, S_2, S_5, S_6)	0.0552778
$(S_1, S_2, S_3, S_4, S_5)$	0.117063
$(S_1, S_2, S_3, S_4, S_6)$	0.117122
$(S_1, S_2, S_3, S_5, S_6)$	0.117076
$(S_1, S_2, S_4, S_5, S_6)$	0.117078
$(S_1, S_2, S_3, S_4, S_5, S_6)$	0.186576

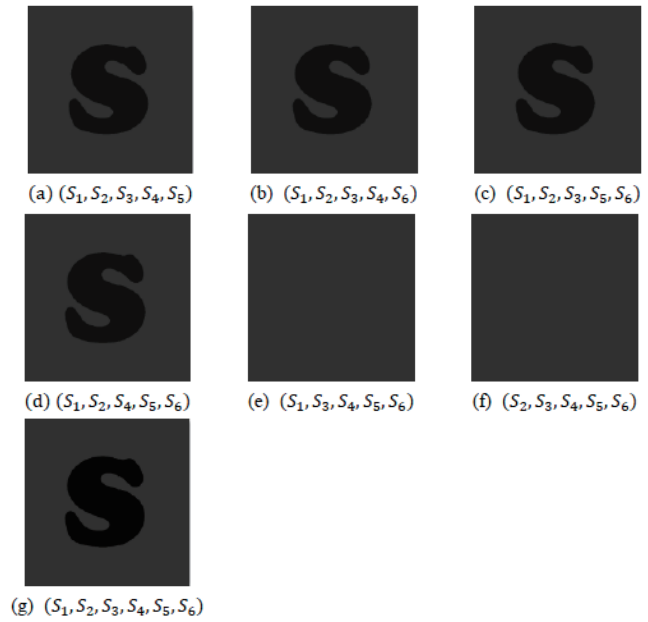


Figure 5: (a)-(d) the stacked results including two specific shares and three general ones; (e)-(f) the stacked noise-like results; and (g) the one by stacking all shares

- 2) **Visual quality:** The disclosed secret can be clearly recognized in the experiments. Furthermore, the contrast is defined as $\frac{H(V_1) - H(V_0)}{m}$, where m is the pixel expansion rate, $H(V_0)$ and $H(V_1)$ are the Hamming weights of all white and all black area in the disclosed image corresponding to the white and black areas in the original image. Table 4 demonstrates the contrast values of all the cases in which the secret can be disclosed in the experimental results.
- 3) **Progressive:** It is obvious by Table 4 that the secret in the proposed scheme can be progressively disclosed.
- 4) **Security:** Any information of the secret cannot be revealed without satisfying the access structure. Here, less than k shares or less than k_0 specific shares cannot be stacked to reveal the secret.

Table 5 gives the comparison between the related works and the proposed.

6 Conclusions

In order to enable the practical end of assigning shares with the specific privilege, this paper proposes a new weighted VC scheme. Each participant in a different group with distinct privilege is delivered a share with specific weight. The disclosed secret is revealed only under the predefined policy of privilege. The experimental results demonstrate the proposed scheme works well.

Table 5: Comparisons of the weighted VSS schemes

Schemes	VC	RG	PVC	SIS	Pixel expansion	Visual quality	Essential
Chen et al. [2]				✓	N/A	N/A	No
Lin et al. [10]				✓	N/A	N/A	No
Shyu et al. [14]				✓	N/A	N/A	No
Li et al. [9]				✓	N/A	N/A	Yes
Yan et al. [18]		✓	✓		No	Low	Yes
Hou et al. [7]	✓				No	Low	No
The proposed	✓				Yes	High	Yes

Acknowledgments

This research was partially supported by Ministry of Science and Technology, R.O.C., under contrast No. MOST 103-2221-E-415 -017.

References

- [1] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol. 129, pp. 86–106, 1996.
- [2] C. C. Chen, C. C. Chen and Y. C. Lin, "Weighted modulated secret image sharing method," *Journal of Electronic Imaging*, vol. 18, pp. 043011-1–043011-6, Oct. 2009.
- [3] T. H. Chen, and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, pp. 1693–1703, 2011.
- [4] T. H. Chen, K. H. Tsao, and Y. T. Yang, "Friendly color visual secret sharing by random grids," *Fundamenta Informaticae*, vol. 96, pp.61–70, 2009.
- [5] W. P. Fang, and J. C. Lin, "Progressive viewing and sharing of sensitive images," *Pattern Recognition and Image Analysis*, vol. 16, pp.632–636, 2006.
- [6] J. B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognition*, vol. 41, pp. 3572–3581, 2008.
- [7] Y. C. Hou, Z. Y. Quan, and C. F. Tsai, "A privilege-based visual secret sharing model," *Journal of Visual Communication and Image Representation*, vol.33, pp. 358–367, 2015.
- [8] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Optics Letters*, vol. 12, pp. 377–379, 1987.
- [9] P. Li, C. N. Yang, C. C. Wu, Q. Kong and Y. Ma, "Essential secret image sharing scheme with different importance of shadows," *Journal of Visual Communication and Image Representation*, vol. 24, no. 7, pp. 1106–1114, Oct. 2013.
- [10] S. J. Lin, L. S. T. Chen and J. C. Lin, "Fast-weighted secret image sharing," *Optical Engineering*, vol. 48, pp. 077008-1–077008-7, July 2009.
- [11] M. Naor and A. Shamir, "Visual cryptography," in *Proceedings of Advances in Cryptography (Eurocrypt'94)*, Lecture Notes in Computer Science, vol. 950, pp. 1–12, 1995.
- [12] B. Schneier, *Applied Cryptography*, 2nd ed, 1996.
- [13] 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, pp. 960–969, 2011.
- [14] S. J. Shyu, C. C. Chuang, Y. R. Chen and A. F. Lai, "Weighted threshold secret image sharing," in *Proceedings of The Third Pacific-Rim Symposium on Image and Video Technology*, LNCS 5414, Springer, Jan. 2009.
- [15] C. C. Thien, and J. C. Lin, "Secret image sharing," *Computers and Graphics*, vol. 26, pp. 765–770, 2002.
- [16] G. Tychiev, "The encryption algorithm GOST28147-89-PES16-2 and GOST28147-89-RFWKPES16-2," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 1–11, 2017.
- [17] X. Wu, and W. Sun, "Improving the visual quality of random grid-based visual secret sharing," *Signal Processing*, vol. 93, pp. 977–995, 2013.
- [18] X. Yan, S. Wang, X. Niu and C. N. Yang, "Essential visual cryptographic scheme with different importance of shares," in *Proceedings of the 21st International Conference on Neural Information Processing*, LNCS 8836, pp. 636–643, Springer, Nov. 2014.
- [19] C. N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters*, vol. 25, pp. 481–494, 2004.

Biography

I-Chun Weng received his M.S. in Department of Computer Science and Information Engineering from National Chiayi University in 2016. Her research interest is visual cryptography and information security.

Tzung-Her Chen was born in Tainan, Taiwan, Republic of China, in 1967. He received the B.S. degree in Department of Information & Computer Education from National Taiwan Normal University in 1991 and the M.S. degree in Department of Information Engineering from Feng

Chia University in 2001. In 2005, he received his Ph.D. degree in Department of Computer Science from National Chung Hsing University. He has been with Department of Computer Science and Information Engineering at National Chiayi University as Professor since August 2011. His research interests include information hiding, multimedia security, digital rights management, network security. He is an honorary member of the Phi Tau Phi Scholastic Honor Society.