New Designs for Friendly Visual Cryptography Scheme

Young-Chang Hou, Zen-Yu Quan, and Hsin-Yin Liao

***Abstract*—Different from conventional cryptography, visual cryptography is an image cryptographic technique proposed by Naor and Shamir. It encodes a secret image into *n* pieces of noise-like shares. When *k* or more than *k* pieces of shares are gathered from participants, human visual system will disclose the secret image on the stacked image easily. Neither complicated mathematical computation nor any knowledge of cryptography are needed are the main advantages of visual cryptography. In this paper, we propose a new design for friendly visual cryptography scheme. The secret will be hiding into two meaningful shares. The black-appearing ratio in each block of the shares for the corresponding black (rep. white) secret pixel is the same. Therefore, it is impossible for one to disclose any information related to the secret image on each share, which achieves the goal of improving security. When shares are superimposed, the contours of the cover image will disappear on the stacked image, which will only reveal the secret image. According to our experimental results, the contrasts of the shares or the stacked images are good which can reveal the contents of the cover images and the secret image clearly.**

***Index Terms*—Friendly visual secret sharing, secret sharing, visual cryptography.**

I. Introduction

Digital data have gradually replaced their paper-based form due to the advancement of Internet technology and widespread use of computers. People can surf the Internet for information they want at any time and at any place. Information delivery is easier and faster than ever. But in another aspect, without proper protection of information from being stolen and tampered with, the owner of the property can do nothing to deal with these attacks. To ensure the confidentiality, integrity and availability of data transmission over the Internet, traditional cryptography uses a secret key and complicated computing to convert plain text into meaningless text. The biggest drawback is that a computer is needed for the encryption and decryption processes, resulting in extensive execution time and wastage of computational resources.

Naor and Shamir [1] proposed a visual secret sharing method, namely visual cryptography (VC), which can encode a secret image into *n* noise-like shares. The secret image can be decrypted by the human eye when any *k* or more shares are stacked together. The secret image will be invisible if the number of stacked shares is less than *k*. The greatest advantage of this decryption process is that neither complex computations nor any knowledge about VC are needed. It is a simple and safe secret sharing method for decoding of the secret images when computer-resources are lacking.

Since visual cryptography was proposed, several related works [2]-[9] were presented thereafter. However, traditional VC produced meaningless share-images, which can create some management problems for those who participate in many secret sharing projects because they have to keep track of many different share-images. Moreover, transmission of meaningless image can arouse suspicion of an outsider, who may realize that this image may carry some type of secret message. This attracts attention and could strengthen their desire to uncover the secret image, thus reducing the security of the secret image. Ateniese *et al.* [10] first applied the strategy of steganography to generate meaningful share-images in VC. Following Ateniese, Hou and Wu [11] proposed a method which uses the halftone and color composition/decomposition techniques to generate meaningful grey or color share-images. Zhou *et al.* [12] and Wang *et al.* [13] improved upon Ateniese's method by developing VC algorithms for dealing with halftone images to make the recovered stack-image less unclear. Chang *et al.* [14] found a way to hide a color secret image in two color cover images. Nakajima and Yamaguchi [15] presented a scheme for encrypting a natural image. Fang [16] proposed a progressive VC scheme which could also produce meaningful share-images. Although all of above methods used pixel expansion method to generate meaningful share-images, Chang *et al.* [14] and Nakajima and Yamaguchi [15] made the share images nine times larger than the original image. Thien and Lin [17] proposed a pixel non-expansion method that could produce a meaningful share-image but a computer was needed to decrypt the secret image, losing the advantage of VC in which the decryption of the secret can be done directly by the human eye.

In this study, new designs for friendly visual cryptography scheme are proposed. Although the share-images are generated by some pixels from the secret image and some pixels from the cover images, only the content of the cover image can be recognized on the share-image without disclosing any clue about the secret image. When two share-images are stacked together, the content of the cover image will disappear and the content of the secret image will naturally reveal instead.

Manuscript received April 10, 2014; revised June 20, 2014. This work was supported in part by the National Science Council of the Republic of China under Grant NSC101-2221-E-032-047.

Young-Chang Hou and Hsin-Yin Liao are with the Department of Information Management, Tamkang University, New Taipei City 25137, Taiwan, Republic of China (e-mail: ychou@mail.im.tku.edu.tw, kaite.liao@mail.im.tku.edu.tw).

Zen-Yu Quan is with the Department of Information Management, National Central University, Jhongli City, Taoyuan County 32001, Taiwan, Republic of China (e-mail: zyquan1207 @gmail.com).

DOI: 10.7763/IJIEE.2015.V5.493

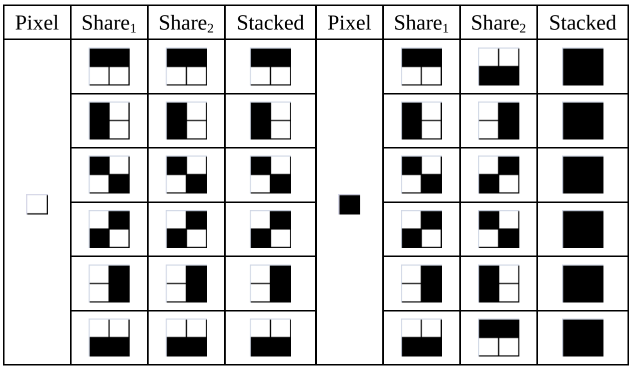
II. Related Works

A. Visual Cryptography

The process of visual cryptography proposed by Naor and Shamir [1] involves the encoding of a secret image into *n* transparencies, where each pixel is expanded *m* times. One transparency is distributed to each participant. The secret image cannot be seen from any transparency, but when *k* or more transparencies are stacked together the image will begin to emerge as the contrast between the black and white pixels becomes sufficient for human eye to recognize the secret image. Neither computational devices nor cryptographic knowledge are required for the decryption process. This approach is called (*k*, *n*)-threshold visual secret sharing.

When encoding a secret image, the dealer designs two $n \times m$ dispatching matrices (C^0, C^1) which represent how to share the white and black pixels in the secret image, where *n* stands for the participant number, and *m* indicates the ratio of pixel expansion. Without loss of generality, we take the case (*k*, *n*) = (2, 2) for example. In this case, each pixel on the secret image will be decomposed into two blocks, 2×2 subpixels each, with two black and two white points inside. When sharing a white pixel, the block content in each share is the same type, otherwise it is the complementary type, as shown in Table I. No matter what the pixel value is on the secret image, the contents in each share will be appeared as two-black-and-two-white blocks. The share's safety is ensured because the interceptor cannot find any secret information from any one share, as seen from Fig. 1.

TABLE I: Sharing and Stacking Scheme of Black and White Pixels



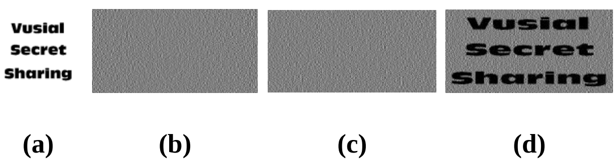
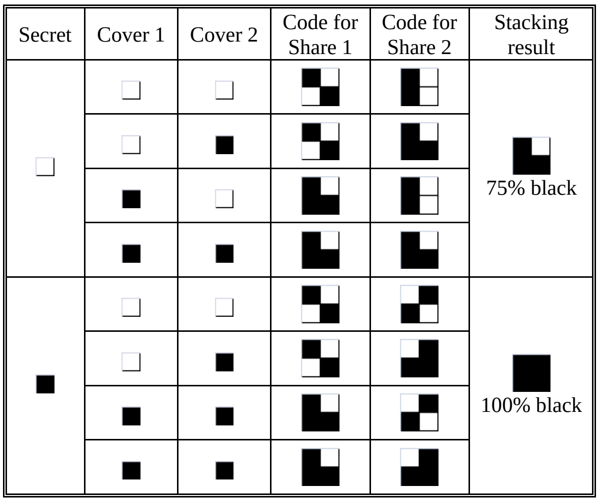


Fig. 1. (a) Secret image; (b) share 1; (c) share 2; (d) restored image.

B. Extended Visual Cryptography

Ateniese *et al*. [10] proposed the Extended Scheme for Visual Cryptography (EVCS) which allowed for meaningful content in the cover-image to appear on the share-image. During the encryption process, a row from a codebook (Table II) is selected according to the colors of the secret-image and two cover images, followed by random permutation of the sub-pixels in each block synchronously. The resultant codes are then assigned to the share-image 1 and the share-image 2. In Ateniese *et al*.'s codebook, regardless of whether the secret image pixel is white or black, in each share-image, a block with two black and two white pixels is represented as a white pixel in the cover-image, and a block with three black and one white pixel is represented as a black pixel. Thus the share-image will not reveal any information about secret image, and the 25% contrast is enough to ensure that we can see the profile of the cover-image. When two share-images are stacked, a block corresponding to a white area in the secret image will have three black and one white pixels within it, and a block corresponding to a black area in the secret image will be fully black. This also creates 25% contrast between the white and black areas, enough to see the content of the secret image with the naked eye.

TABLE II: Ateniese's Codebook



III. The Proposed Scheme

In this paper, we propose a new scheme which can encrypt a secret image into two meaningful share-images. Participants can recognize the contents of the cover-image on each share-image, but nobody can uncover any clue about the secret image on them. If superimposing these two share-images, the contents of the cover-image will be disappeared and, on the contrary, the contents of the secret image will be revealed on the stacked-image. The main concept is that we take some pixels from the secret image and some pixels from the cover image to generate the needed share-images. For example, without loss of generality, the color of the odd (resp. even) locations of the share-image is determined by the color of the cover (resp. secret) image at that corresponding location. In order words, we embed the information of the cover (resp. secret) image into odd (resp. even) locations on the share-images.

Since each 2×2 image block may contain 0 ~ 4 black pixels, it may display 16 different image patterns. If we treat the black pixel as 1 and the white pixel as 0, the image patterns and the corresponding binary/decimal codes are shown in Table III. We classified these patterns into 5 different sets, X_0 = {0}, X_1 = {1, 2, 4, 8}, X_2 = {3, 5, 6, 9, 10, 12}, X_3 = {7, 11, 13, 14}, X_4 = {15}, based on the number of the black pixel in each block.

In order to show a cover-image on the share-image, we need two different types of blocks to produce the contrast between the dark and the light areas corresponding to the odd locations of the cover-image. A block with few (resp. more) black pixels in it is used to represent the white (resp. black) pixel in the cover-image. However, the stacked result of these two types of blocks should reveal no information of the cover image visually (Table IV). It means that the superimposing results of the selected blocks should not display any contrast among the areas of the odd locations of the stacked-image. Except for Table IV, there are many different kinds of blocks, as shown in Table V, which can also be used for this purpose.

TABLE III: OUR CODEBOOK DESIGN

Block	Binary code	Decimal code	Block	Binary code	Decimal code
	0000	0		1001	9
	0001	1		1010	10
	0010	2		1100	12
	0100	4		0111	7
	1000	8		1011	11
	0011	3		1101	13
	0101	5		1110	14
	0110	6		1111	15

TABLE IV: CODEBOOK FOR COVER IMAGE

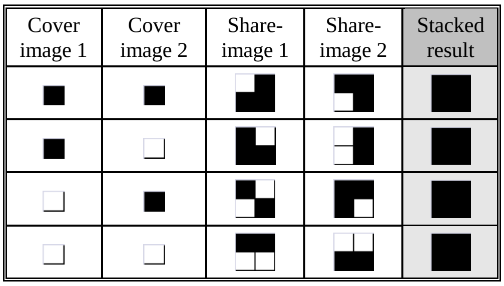
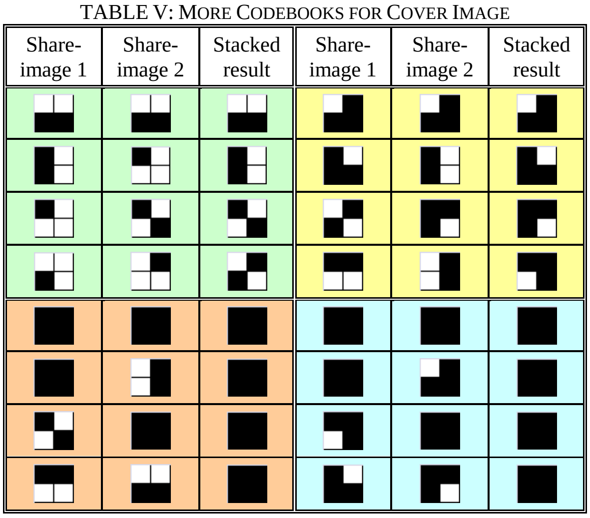


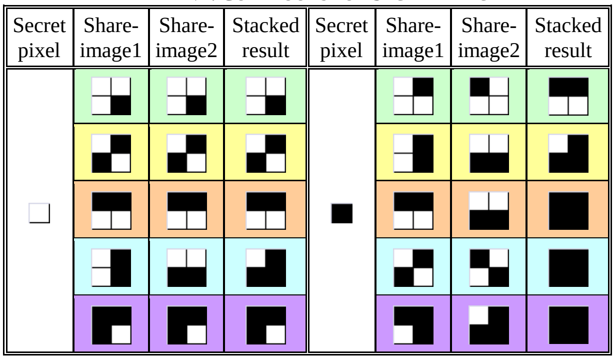
TABLE V: MORE CODEBOOKS FOR COVER IMAGE



On the contrary, it should not reveal any secret information on the share-images. Therefore, only one type of block is enough to represent the areas that are used to embed the secret information. Therefore, blocks corresponding to the even locations on share-image 1 and share-image 2 should have equal number of black pixel to make them noise-like. However, the stacked result of these areas should display necessary contrast and reveal the secret information visually. Some examples are given in Table VI.

In this paper, we use the designs of Table IV, Table V, and Table VI as our building blocks. Any design in Table IV and V, which uses different number of black pixels to make a black area looks darker and a white area looks lighter on the share-image and eliminate the contrast on the stacked-image, can be used as a candidate to represent the black and white pixels on the cover images. On the contrary, any design in Table VI, which uses same number of black pixels to eliminate the contrast on the share-image, but create the necessary contrast on the stacked-image, can be used as a candidate to represent the black and white pixels on the secret images.

TABLE VI: CODEBOOKS FOR SECRET IMAGE



For example, if we select a block with **3** black pixels to represent a black pixel and a block with **2** black pixels to represent a white pixel on the cover image, it will create 25% contrast on the share-image, but the stacked results are all 4 black pixels, the content of the cover image is vanished, which can be treated as a background on the stacked-image (Table IV). If we use a block with 2 black pixels to represent pixels on the secret image (shown in row 3 of the Table VI), it will not disclose any clue about the secret image on the share-images, but the stacked results will be **4** and **2** black pixels respectively. It creates the necessary contrast which helps us to recognize the secret image on the stacked-image. We named this design as (3, 2)/(4, 2) model in which 3 (resp. 2) black pixels represent a black (resp. white) block on the share-images, while 4 (resp. 2) black pixels represent a black (resp. white) block on the stacked-image, respectively.

A. (3, 2)/(4, 2) Model

If the blocks on the share-images are determined by the pixels on the cover image (Table VII, upper part):

1) If corresponding pixels on both cover images are black, we randomly choose two blocks, say S_1 and S_2 from X_3 where $S_2 \neq S_1$, and assign them to share-image 1 and share-image 2 respectively. The black-appearing ratio of these blocks is 75% which makes these areas look darker.
2) If corresponding pixels on both cover images are white, we randomly choose two blocks, say S_1 and S_2 from X_2, where $S_2 \neq S_1$ and $S_2 = 15 - S_1$, and assign them to share-image 1 and share-image 2 respectively. The

black-appearing ratio within these blocks is 50% which makes these areas look lighter.

3) If corresponding pixels on both cover images are not the same, we randomly choose two blocks, say S_b from X_3 and S_w from X_2, where $15 - S_b \subset S_w$, i.e. S_b OR $S_w = 15$. The black-appearing ratios on S_b, and S_w are 75% and 50% respectively.

By doing this way, blocks that are represented for the black regions of the cover image look darker (75% of blackness) than those for the white regions (50% of darkness). This will highlight the content of the cover-images. When the corresponding blocks are superimposed, the stacked result is always a member that belongs to X_4 and the black-appearing ratio will always be 100%. Hence, the contents of the cover-images will disappear on the stack-image.

If the blocks on the share-image are determined by the pixels on the secret image (Table VII, lower part):

1) If the corresponding pixels on the secret image are black, we randomly choose two blocks, say S_1, and S_2 from X_2, where S_1 and S_2 are complement with each other, i.e. $S_2 = 15 - S_1$. The black-appearing ratio within these two blocks is 50%.
2) If corresponding pixels on the secret image is white, we randomly choose a block, say S_1, from X_2 and assign it to both share-images, i.e. $S_2 = S_1$. The black-appearing ratio within these two blocks is also 50%.

In a result, the black-appearing ratio on the share-image will always be 50%. Therefore the appearances of the blocks that are represented for the secret image are meaningless. However, blocks that are represented for the black regions of the secret image look darker (100% of blackness) than those for the white regions (75% of darkness) when these blocks are stacked together. It will emerge the content of the secret image while the content of the cover-image will disappear on the stack-image. This part of blocks causes the desired effect of visual cryptography.

TABLE VII: (3, 2)/(4, 2) MODEL

Cover image 1	Cover image 2	Share image 1	Share image 2	Stacked result
■	■	$S_1 \in X_3$	$S_2 \in X_3$ $S_2 \neq S_1$	$(S_1$ OR $S_2) \in X_4$
■	□	$S_1 \in X_3$	$S_2 \in X_2$ $15 - S_1 \subset S_2$	$(S_1$ OR $S_2) \in X_4$
□	■	$S_1 \in X_2$	$S_2 \in X_3$ $15 - S_2 \subset S_1$	$(S_1$ OR $S_2) \in X_4$
□	□	$S_1 \in X_2$	$S_2 \in X_2$ $S_2 = 15 - S_1$	$(S_1$ OR $S_2) \in X_4$

Secret image	Share image 1	Share image 2	Stacked result
■	$S_1 \in X_2$	$S_2 \in X_2$ $S_2 = 15 - S_1$	$(S_1$ OR $S_2) \in X_4$
□	$S_1 \in X_2$	$S_2 = S_1$	$(S_1$ OR $S_2) \in X_2$

B. Other Models

Except for (3, 2)/(4, 2) model, any combination from of Table IV, Table V, and Table VI which makes a black area looks darker and a white area looks lighter on the share-image while eliminates the contrast when they are stacked and eliminates the contrast on the share-images but creates the necessary contrast on the corresponding areas on the stacked-image can be used to form a new model. Other possible models are (2, 1)/(2, 1), (2, 1)/(3, 2), (3, 2)/(3, 2), (3, 2)/(4, 3), (4, 3)/(4, 3), (2, 1)/(4, 2), (4, 2)/(4, 3), (4, 2)/(4, 2).

(4, 2)/(4, 2) will be the best design among all these nine possible designs. It uses 4 (resp. 2) black pixels to represent the black (resp. white) pixels of the cover images. It will create 50% contrast on the share-images. On the stacked-image, 4 (resp. 2) black pixels are also used to represent the black (resp. white) pixels of the secret image. It also creates 50% contrast on the stacked-image. 50% contrast on the share-image or the stacked-image are good enough to reveal the contents of the cover images and the secret image clearly (Table VIII and Table IX).

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In this study, we ran our experiments under the Microsoft Windows XP with service pack 3 on a personal computer with Intel Core 2 Duo processor and 2GB memory, and we also used Java SE 6.0 SDK as our program development tools. We tested (2, 1)/(3, 2), (3, 2)/(4, 2), (4, 2)/(4, 3) and (4, 2)/(4, 2) models in Table VIII and Table IX. Images used in Table VIII are 256×256 binary images while images used in Table IX are 256×256 grayscale images. From the experimental results, the black area is darker than the white area, so the contents of the cover image are displayed clearly on the share-images. After share-images are superimposed, the contents of the cover-images disappear, only the contents of the secret image revealed on the stacked-image. From Table VIII and Table IX, we can find that the (4, 2) model can get 50% contrast which is better than (2, 1), (3, 2) or (4, 3) models in which only 25% contrast will be gained.

V. CONCLUSIONS

In this study, some pixels from the secret image and some pixels from the cover image are taken to generate the needed share-images. Pixels from the secret image are encrypted to make the appearance on each share-image meaningless, but the content of the secret image will become clear when two share images are stacked together. On the other hand, pixels from the cover-image are encrypted to make the black area dark and the white area bright to highlight the contents of the cover-image, but the contents of the cover-image will disappear; only the encrypted secret image will reveal when they are stacked together.

The advantages of our friendly visual secret sharing include: (1). design concept is simple and easy to implement; (2). in (4, 2)/(4, 2) model, the contrast can reach 50% on both the share-images and the stacked-image which will reveal the contents of the cover images and the secret image clearly; (3). meaningful share-images will benefit for the share management problem.

TABLE VIII: EXPERIMENTS WITH BINARY IMAGES

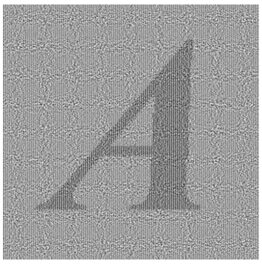
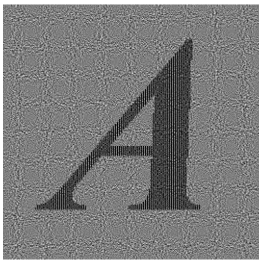
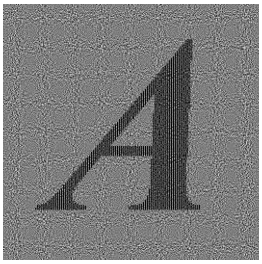
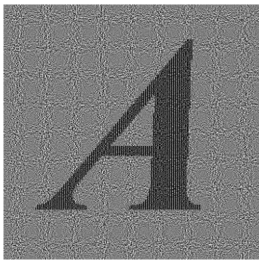
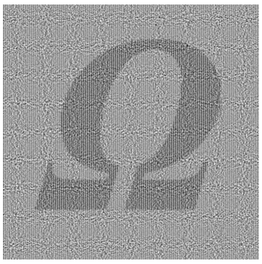
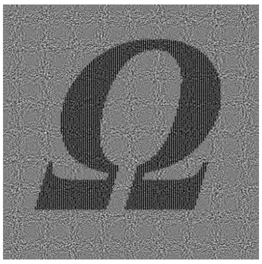
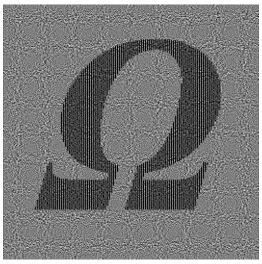
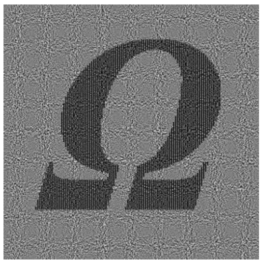
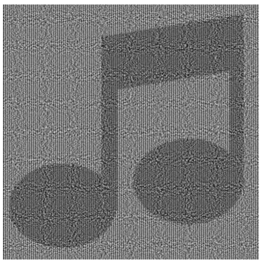
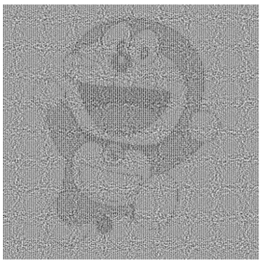
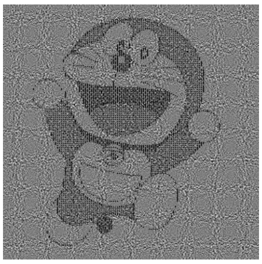
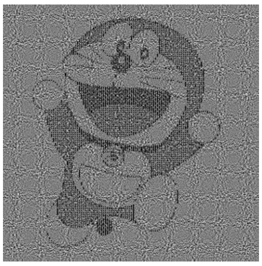
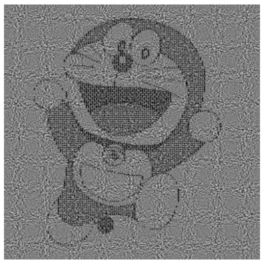
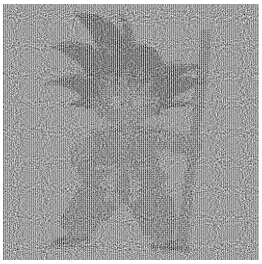
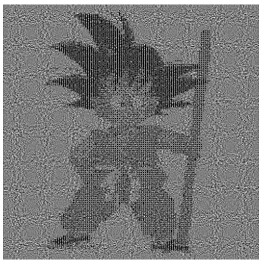
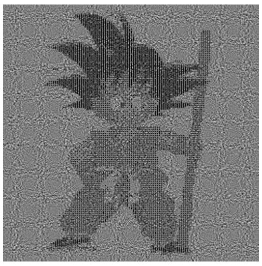
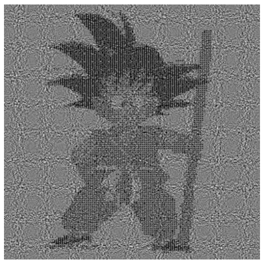
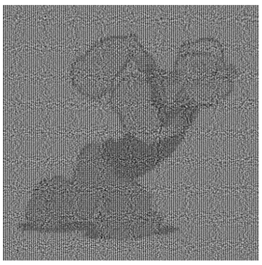
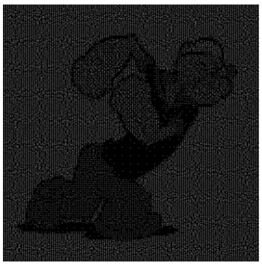
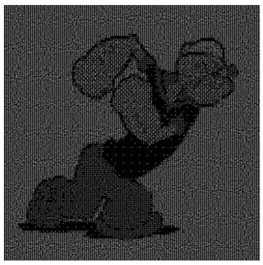
	(2, 1)/(3, 2)	(3, 2)/(4, 2)	(4, 2)/(4, 3)	(4, 2)/(4, 2)
Share image 1				
Share image 2				
Stacked result				

TABLE IX: EXPERIMENT FOR GREY-LEVEL IMAGES

	(2, 1)/(3, 2)	(3, 2)/(4, 2)	(4, 2)/(4, 3)	(4, 2)/(4, 2)
Share image 1				
Share image 2				
Stacked result				

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," *Lecture Notes in Computer Science*, vol. 950, pp. 1-12, 1995.

[2] T. H. Chen and K. C. Li, "Multi-image encryption by circular random grids," *Information Sciences*, vol. 189, no. 15, pp. 255 – 265, 2012.

[3] Y. C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, issue 7, pp. 1619-1629, 2003.

[4] Y. C. Hou and Z. Y. Quan, "Progressive visual cryptography with unexpanded shares," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, issue 11, pp. 1760-1764, 2011.

[5] Y. C. Hou and P. H. Huang, "An ownership protection scheme based on visual cryptography and the law of large numbers," *International Journal of Innovative Computing, Information and Control*, vol. 8, issue 6, pp. 4147-4156, 2012.

[6] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E82-A, no. 10, pp. 2172-2177, 1999.

[7] T. H. N. Le, C. C Lin, C. C. Chang, and H. B. Le, "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images," *Digital Signal Processing*, vol. 21, issue 6, pp. 734-745, 2011.

[8] S. J. Shyu, "Image encryption by multiple random grids," *Pattern Recognition*, vol. 42, issue 7, pp. 1582-1596, 2009.

[9] D. Wang, F. Yi, and X. Li "Probabilistic visual secret sharing schemes for grey-scale images and color images," *Information Sciences*, vol. 181, issue 11, pp. 2189 – 2208, 2011.

[10] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended schemes for visual cryptography," *Theoretical Computer Science*, vol. 250, pp. 143-161, 2001.

[11] Y. C. Hou and J. H. Wu, "An extended visual cryptography scheme for concealing color images," *in Proc. The 5th Conference on Information Management and Police Administrative Practice*, Taoyuan, Taiwan, 2001, pp. 62-69.

[12] 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.

[13] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 383–396, 2009.

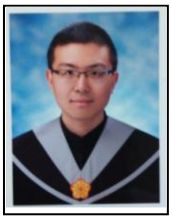
[14] C. C. Chang, W. L. Tai, and C. C. Lin, "Hiding a secret color image in two color images," *IMAGING SCI J - Imaging Science Journal*, vol. 53, no. 4, pp. 229–240, 2005.

[15] M. Nakajima and Y. Yamaguchi, "Enhancing registration tolerance of extended visual cryptography for natural images," *Journal of Electronic Imaging*, vol. 13, no. 3, pp. 654–662, 2004.

[16] W. P. Fang, "Friendly progressive visual secret sharing," *Pattern Recognition*, vol. 41, no. 4, pp. 1410-1414, 2008.

[17] C. C. Thien and J. C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765-770, 2002.

Young-Chang Hou received his B.S. degree in atmospheric physics from National Central University, Taiwan in 1972, his M.S. degree in computer applications from Asian Institute of Technology, Bangkok, Thailand in 1983, and his Ph.D. degree in computer science and information engineering from National Chiao-Tung University, Taiwan in 1990. From 1976 to 1987, he was a senior engineer with Air Navigation and Weather Services, Civil Aeronautical Administration, Taiwan, where his work focused on the automation of weather services. From 1987 to 2004, he was on the faculty at the Department of Information Management, National Central University. Currently he is a professor with the Department of Information Management, Tamkang University, Taiwan. His research interests include digital watermarking, information hiding, fuzzy logic, genetic algorithms, and visual cryptography.



Zen-Yu Quan received his B.S. degree in information management from Tatung University, Taiwan in 2007, his M.S. degree in information management from Tamkang University, Taiwan in 2009. He is currently a PhD student at the Department of Information Management, National Central University, Taiwan. His research interests cover secret sharing, digital watermark, and image retrieval.

Hsin-Yin Liao received her B.S. degree in information management from Chaoyang University of Technology Taiwan in 2005, her M.S. degree in information management from Tamkang University, Taiwan in 2009. Her research interests include digital image processing, digital watermarking, and visual cryptography.