Appl. Math. Inf. Sci. **8**, No. 5, 2327-2335 (2014)

Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080528

A Secure Visual Secret Checking of Meaningful Sharing Images

Chin-Ling Chen[1,*], *Wen-Hu Chen*[2], *Chih-Cheng Chen*[3], *Yeong-Lin Lai*[4] *and Kuo-Kun Tseng*[5]

[1] Department of Computer Science and Information Engineering, Chaoyang University, 168 Jifeng E. Road, Wufeng District, Taichung, 41349, Taiwan, R.O.C.
[2] Department of Computer Science and Engineering, National Chung-Hsing University, Taichung 40227, Taiwan, R.O.C.
[3] Department of Health Policy and Management, Chung Shan Medical University, Taichung 40201, Taiwan, R.O.C.
[4] Department of Mechatronics Engineering, National Changhua University of Education, Changhua, 50007, Taiwan, R.O.C.
[5] Harbin Institute of Technology Shenzhen Graduate School, HIT Campus of ShenZhen University Town, Xili, Shenzhen 518055, China

Received: 31 Aug. 2013, Revised: 28 Nov. 2013, Accepted: 29 Nov. 2013
Published online: 1 Sep. 2014

Abstract: Visual secret checking refers to the superimposition of one key image and another public sharing image without auxiliary automated computation, in order to recognize the specified secret via human inspection. This paper achieves the goals of: guaranteeing that the related contents of a secret are not revealed after any public sharing image superimposition, confirming the accuracy of any public sharing image, and providing for the ease of management of various types of sharing images. When a user is outside of a computer environment, he/she can utilize the proposed method to discern the contents of the secret independently. Furthermore, the key image and all the sharing images have the same meaning, visible upon inspection, which allows for effective data management and classification. Through an exposition of the relevant theory, as well as experimentation, this paper provides evidence for the above claims.

Keywords: Visual cryptography; Visual secret checking; Pattern dithering; Information security

1 Introduction

Visual cryptography (VC) was first proposed by Naor and Shamir [1]. The main difference between VC and conventional cryptography lies in the deciphering process. Conventional cryptography uses either symmetrical encryption [2] or asymmetrical encryption [3] and must use relevant cryptographic knowledge and computer resources to complete encryption and decryption. However, VC uses the human visual system to respond to the image's chromatic aberration and then utilizes the secret image to propagate several sharing images. The purpose of this division into several sharing images is to protect the content of the secret image. The secret image may be textual, numerical, symbolic, or graphical where a superimposition of the sharing images allows for deciphering. The process of deciphering does not necessitate any complex computation or any knowledge of cryptography insofar as distinguishing the content of the secret image individually. Therefore, in some situations where a computer is not available to the decipherer, a vision-based secret sharing method provides an apt solution. As regards visual secret sharing research, encryption methods may differ between pixel expansion skill [4,5,6,7,8,9,10,11] and pixel non-expansion skill [12,13,14,15,16]. The majority of the sharing images generated by the above two encryption skills is chaotic, but provides meaningful images [4,9,10]. Although the chaotic sharing image may guarantee security, it is subject to suspicion and destruction. Therefore, the secret sharing method regarding the sharing image for the meaningful image holds practical value.

At present, related visual authentication technology mainly covers two issues: one is visual secret sharing [17], which employs the sharing of a visual secret; the other is visual signature checking [18], which focuses on the authentication of a visual secret. The differences are such that visual secret sharing publicizes the sharing

* Corresponding author e-mail: clc@mail.cyut.edu.tw

secret emphatically, while visual signature checking can only allow the public image to be publicized. The technology underlying whether visual authentication is successful depends on two fundamental factors. The first is secret readability; visual authentication is decoded by the human eye. This requires the superimposition of the sharing images to be distinguished by the human eye, revealing the complete secret. The second is secret security; as the sharing images are public, there must be a guarantee such that the superimposition of any public images will not reveal any related content of the secret. A common method is one that joins the primitive secret in fixed ratio noises [19,20] and uses massive noises to prevent one's eyes from being able to distinguish the secret content of the sharing image.

Authentication stems originated from the cryptology in the 1970s, and was further formulated in the following decade. At present, many of the authentication protocols apply to media transmissions within the network [16,21] mostly after a complex deciphering process using a computer for authentication. This raises a question: "If one lacks the computer auxiliary, how can one carry out the deciphering process?" Therefore, the proposed method uses the concept of visual cryptography and coordinates pattern dithering technology and visual secret sharing technology to produce a key image and sharing images which all have the same meaning. If we want to know what belongs in the content of secrets in the future, we may superimpose the key image and the sharing image to obtain the content of the secret directly by looking at it. Our method has the following four advantages: (1) it improves the sharing image security, utilizing the authentication image to add the fixed ratio noises, increasing the readability of the secret; (2) it permits recognition of the hidden message via the human visual system without the use of a computer; (3) it confirms the correctness of the secret sharing image and prevents malicious users from modifying the secret sharing image or changing its secret contents; and (4) all the sharing images have the same meaning such that the superintendent can facilitate the management and classification of all sharing images.

The rest of this paper is organized as follows. Section 2 introduces the related works. Section 3 describes the proposed method. Section 4 provides the experimental results. Finally, conclusions are presented in Section 5.

2 Related works

2.1 Visual secret sharing technology

2.1.1 Naor and Shamir's scheme

In 1944, Naor and Shamir [1] proposed a visual secret sharing technology called visual cryptography. This technology utilizes the mechanism of $m \times m$ pixel expansion and each block size for $m \times m$ is used to process the secret image of $N \times M$ pixels into $mN \times mM$ pixels. We give the definition of the black and white of a block in Table 1. Finally, we refer to the secret image and the definition of the black and white of a block in Table 1 to produce several meaningless binary sharing images. The superimposition of the partial or complete sharing images presents the secret information directly to the human visual system without auxiliary computation.

Naor and Shamir's scheme produces the type of sharing images in which there is no meaning, which is suited to public transmission. However, this causes data (image) management issues.

Table 1: Naor and Shamir's scheme of the black and white definition of a block

Images \ Items	Black (B)[1]	White (W)[2]
Share image[3]	a(B), $m \times m$-a(W)	b(B), $m \times m$-b(W)
Stacking image[4]	p(B), $m \times m$-p(W)	q(B), $m \times m$-q(W)

[1] Black (B) of every block of $m \times m$ size
[2] White (W) of every block of $m \times m$ size
[3] a=b, $\{a, b, m\} \in N$
[4] p>q, $\{m, p, q\} \in N$

2.1.2 Hwang and Chang's scheme

In 2001, Hwang and Chang [10] proposed the visual cryptography technology utilizing the mechanism of $m \times m$ pixels expansion, and each block size for $m \times m$ to process the binary image of size of $N \times M$ pixels becoming the size of $mN \times mM$ pixels. Then, we give the definition of the black and white of a block in Table 2. The camouflaged image matches up with Table 2 to produce sharing images which have the same visual meaning as the input camouflaged image. Finally, we refer to the definition in Table 2 regarding the secret image, to adjust the location of the black dots and white dots of each block. Then, we get the complete sharing images, which have the same visual meaning as the input camouflaged image. The superimposition of the partial or complete sharing images presents the secret information directly to the human visual system.

Hwang and Chang's scheme produces the sharing images in which the visual meaning coordinates the camouflaged image. Therefore, the superintendent facilitates the effective management of all kinds of sharing images. Due to the sharing images in which there is visual meaning, the sharing image expands $m \times m$ times. In other words,

storage space is wasted.

Table 2: Hwang and Chang's scheme of the black and white definition of a block

Items / Images	Black (B)[1]	White (W)[2]
Share image[3]	a(B), $m \times m$-a(W)	b(B), $m \times m$-b(W)
Stacking image[4]	p(B), $m \times m$-p(W)	q(B), $m \times m$-q(W)

[1] Black (B) of every block of $m \times m$ size
[2] White (W) of every block of $m \times m$ size
[3] $a>b$, $\{a,b,m\} \in N$
[4] $p>q$, $\{m,p,q\} \in N$

2.2 Pattern dithering technology

In 1996, Oka et al. [20] proposed a pattern dithering method wherein one can use the black and white dots of a block to simulate one pixel of the gray scale image; the gray scale pixels are presented by the black and white dots of a block with the expended k dots matrix.
If the scope of the complete gray scale pixels value $0 \backsim 255$ will be substituted by t levels, we may obtain t different gray-levels to substitute for original gray scale pixels. Every gray-level represents the scope of gray scale value $\{ n \times \llcorner 256/t \lrcorner + 1 \backsim (n+1) \times \llcorner 256/t \lrcorner, 0 \leq n < t; 2 \leq t \leq k+1; n,k,t \in N$; when $n = 0$, this gray-level contains the gray scale value 0; when $n = t-1$, the maximum gray scale of this gray-level is not larger than 255$\}$. By way of this transformation, we can transfer a gray scale image to a binary image of k times the size. Assuming the expended parameter $k = 4 \times 4$, we can obtain 17 available gray-levels, as shown in Fig. 1.

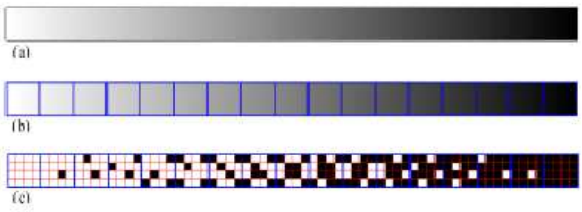

Fig. 1: (a) Gray scale image (b) 17 rank gray-levels substitute gray scale pixels (c) 4×4 dots substitute for one of the kind of chart of 17 rank gray-levels

3 The proposed method

First, we describe the generated images'meanings and the roles of the proposed scheme.
Gray camouflaged image: the camouflaged image of the key image, the secret sharing image, and the authentication sharing image.
Secret image: a secret content which is known by oneself.
Authentication image: an image authenticates if the secret sharing image is correct.
Key image: one binary image, a gray camouflaged image, is used in the pattern dithering method to transform into a binary image.
Secret sharing image: a secret sharing image used to demonstrate belonging to the secret content after superimposition with the key image.
Authentication share image: an authentication sharing image is used to confirm the accuracy of the secret sharing image.
Our method uses the gray camouflaged image and the pattern dithering method to construct one image in which the visual meaning coordinates with the gray camouflaged image, called the key image. This key image refers to the different secret image and coordinates the number of the marked black and white in each block, demonstrating black or white after the superimposition to produce two images in which the visual meaning relates to the gray camouflaged image, called Secret sharing image (1) and Secret sharing image (2). Next, we adjust these two secret sharing images to guarantee that they will not reveal the secret content after the superimposition. Then, the above adjusted Secret sharing image (1) and the Secret sharing image (2) refer to the same authentication image and coordinate the number of the marked black and white of each block, demonstrating black or white after the superimposition to produce two images in which the visual meaning coordinates with the gray camouflaged image, called the Authentication sharing image (1) and the Authentication sharing image (2). The superimposition of the secret sharing image and the authenticating sharing image confirm the accuracy of the secret sharing image. The superimposition of the key image and the secret sharing image demonstrates the secret content. The flowchart of the proposed method is shown in Fig. 2.

3.1 Initial procedure

Step 1:The defined size of a block is $m \times m$ pixels.
Step 2:The definition of the pattern dithering method using the expanded parameter, $k = m \times m$, takes t rank gray-levels to represent the value of the pixels of gray scale image, as shown in Table 3.
Step 3:The number of the marked black and white of each block, demonstrating black or white after the

superimposition, is shown in Table 4. Its definition must conform to the following rules:

(1) p (black)$\geq 2 \times a$ (black), guarantees the number of the marked black and the marked white of each block, demonstrating black after the superimposition.

(2) q (black)$\geq b$ (black), guarantees the number of the marked black and the marked white of each block, demonstrating white after the superimposition.

(3) p (black) - q (black) the disparity is greatly better, guaranteed that the superimposition image can provide for easy identification in the context of human inspection.

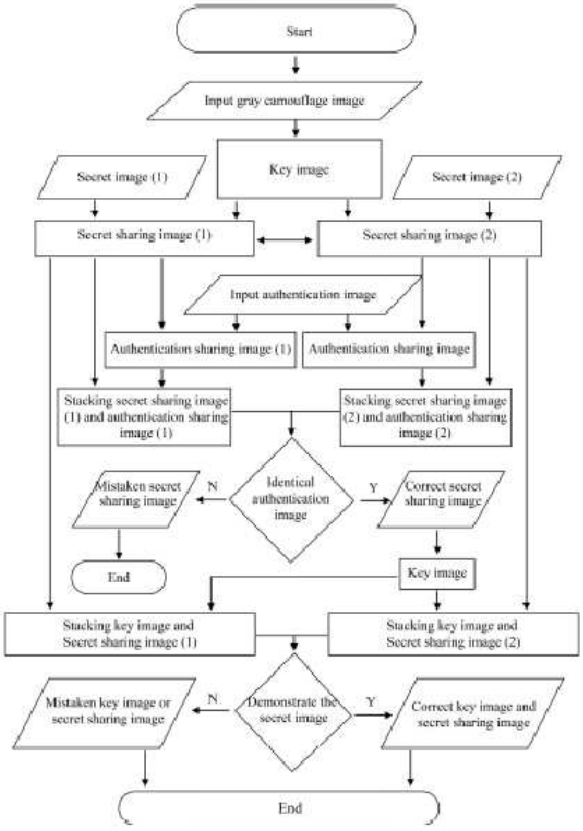

Fig. 2: Flowchart of the proposed method

3.2 Generating key image procedure

Input:

(1) $N \times M$ pixels size of gray camouflaged image.

(2) Following Step 2 of Section 3.1, use the pattern dithering method.

Output:
Key image

Step 1: Use $N \times M$ pixels size of gray camouflaged image to expand $mN \times mM$ pixels size; the expansion image will be divided to $m \times m$ pixels size for each block.

Step 2: Following Step 2 of Section 3.1, each pixel value (in the gray camouflaged image) is substituted with k black and white dots. We can obtain the key image in which a visual inspection renders the same meaning as the input gray camouflaged image after completing all of the blocks.

Table 3: Definition of black and white dots substituting gray-level

Items / Images	Black dots (B) and White dots (W)[1]
Key image[2]	$\{a$(B), $m \times m$-a(W)$\}$ $\backsim\{b$(B), $m \times m$-b(W)$\}$

[1] The number of black dots (B) and white dots (W) of t rank gray-levels of each block of $m \times m$ size

[2] $b>a$ and $b= t+a-1, \{a,b,m,t\} \in N$

Table 4: Definition of black or white after the superimposition

Items / Images	Black (B)[1]	White (W)[2]
Superimposition image[3]	p(B), $m \times m$-p(W)	q(B), $m \times m$-q(W)

[1] Black (B) of every block of $m \times m$ size

[2] White (W) of every block of $m \times m$ size

[3] $p>q$, $\{m,p,q\} \in N$

3.3 Generating secret sharing image procedure

Input:

(1) Secret image (1) and Secret image (2), which have different secret contents, and whose sizes are the same as $N \times M$ pixels.

(2) The $mN \times mM$ pixels size of the key image.

(3) According to Step 3 of Section 3.1, the number of the marked black and white of each block demonstrates black or white after the superimposition.

Output:
Secret sharing image (1) and Secret sharing image (2).

Step 1: Use two secret images whose size is the same as $N \times M$ pixels to expand to $mN \times mM$ and the expanded image will be divided to $m \times m$ for each block.

Step 2: The relative block of each pixel in the secret image superimposes the relative block of the key image and compares it to the secret image until it conforms to the number of black dots and white dots, as in Step 3 of Section 3.1 after superimposition. We will then obtain the preliminary Secret sharing image (1) and the preliminary Secret sharing image (2) after completing all blocks.

Step 3: The preliminary Secret sharing image (1) and the preliminary Secret sharing image (2) from Step 2 can be adjusted according to the following procedures. We will obtain the Secret sharing is a guarantee that the secret content will not be revealed after these two secret sharing images are superimposed.

(1) Secret image (1) and Secret image (2) in the identical position demonstrate the white. The pixel value of Secret sharing image (1) is replaced by the pixel value of the preliminary Secret sharing image (1); the pixel value of Secret sharing image (2) is replaced by the pixel value of the preliminary Secret sharing image (2).
(2) Secret image (1) and the Secret image (2) in the identical position demonstrate the black: The pixel value of Secret sharing image (1) is replaced by the pixel value of the preliminary Secret sharing image (1); this computes the number of black dots of the relative block in the preliminary Secret sharing image (1). If its value is greater than the half of the expended parameter k, then the pixel value of the relative block of Secret sharing image (2) is replaced by the pixel value of the relative block of the preliminary Secret sharing image (1); if its value is not greater than half of the expended parameter k, then the pixel value of the relative block of Secret sharing image (2) is replaced by the pixel value of the relative block of the preliminary Secret sharing image (2).
(3)Secret image (1) and Secret image (2) in the identical position demonstrate the black and white, respectively:

a.The pixel value of the relative block of Secret sharing image (1) is replaced by the pixel value of the preliminary Secret sharing image (1).
b.Each pixel of the relative block of Secret sharing image (2) is set to demonstrate the white.
c.Records the black dots, position of key image, and the preliminary Secret sharing image (1) in the identical block position; the pixel value of the relative block of Secret sharing image (2) sets black dots based on the above record.
d.Records the black dots (position of key image) and the white dots (position of the preliminary Secret sharing image (1)) in the identical block position; the pixel value of the relative block of Secret sharing image (2) set randomly p - q with black dots based on the above record, the p and q are defined in Table 4.
e.Records the white dots (position of key image) and the black dots (position of the preliminary secret sharing image (1)) in the identical block position and assumes that the pre-mentioned record is r; then, the pixel value of the relative block of Secret sharing image (2) is set randomly to r - (p - q) with black dots based on the above record. f. After completing the above *b*, *c*, *d* and *e* steps, complete the pixel value of the relative block of Secret sharing image (2).
f.Secret image (1) and Secret image (2) in the identical position demonstrate the white and the black, respectively.
g.The purpose of the above three adjustments: the overlap of black dots reduces the relative contrast after superimposing Secret sharing image (1) and Secret sharing image (2). This provides a guarantee such that each member of the party will not have access to the other's secret contents.

3.4 Generating authentication sharing image procedure

Input:

(1) The $N \times M$ size of the authentication image.
(2) The The $mN \times mM$ of Secret sharing image (1) and Secret sharing image (2).
(3) Following Step 3 of Section 3.1, the number of the marked black and white of each block demonstrates black or white after the superimposition.

Output:
Authentication sharing image (1) and authentication sharing image (2)

Step 1: Use two secret images whose size is the same as $N \times M$ pixels to expand to $mN \times mM$; the expansion image will be divided to $m \times m$ for each block.

Step 2: The relative block of each pixel in the authentication image superimposes the relative block of the secret sharing and compares the authentication image to adjust until conforming to the number of black and white dots in Step 3 of Section 3.1 after superimposition. We can obtain the Authentication sharing image (1) and the Authentication sharing image (2) which have the same visual meaning as the input gray camouflaged image.

Step 3: The Authentication sharing image (1) and Authentication sharing image (2) of the above Step 2 are marked black which shifted 4 pixels. Thus, we can avoid the confusion of the secret sharing image and the authentication sharing image.

3.5 Confirming accuracy of the secret sharing image procedure

Input:

(1) Secret sharing image (1) and Secret sharing image (2) are produced based on Section 3.3.
(2) Authentication sharing image (1) and Authentication sharing image (2) are produced following Section 3.4.

Output:
Authentication image

Step 1: The superimposed image of A's Authentication sharing image (2) and B's Secret sharing image (2) compares with the superimposed image of B's Authentication sharing image (1) and A's Secret sharing image (1). If both demonstrate the same information as the authentication image, we can confirm the accuracy of the secret sharing image of the opposite party.

3.6 Demonstrating secret image procedure

Input:

(1) The key image produced based on Section 3.2.
(2) Secret sharing image (1) and Secret sharing image (2) are produced based on Section 3.3.

Output:
Secret image (1) and Secret image (2)

Step 1: The key image superimposes Secret sharing image (1) and Secret sharing image (2) and then utilizes human visual recognition. If the key image and the secret sharing image are correct, the content of the secret image can be revealed; otherwise, the content of the secret image will be indiscernible.

Our proposed method produces the key image, Secret sharing image (1), Secret sharing image (2), as well as Authentication sharing image (1) and Authentication sharing image (2) which have the same visual meaning as the input gray camouflaged image. This will allow the superintendent or the user to easily manage the secret sharing images. Furthermore, we utilize the superimposition of the authentication sharing image and the secret sharing image to judge the accuracy of the secret sharing image; this avoids situations where the key image has been revealed and malicious attackers are able to falsify the secret sharing image in order to change its secret content.

4 Experimental results

Input:

(1) Each block of 4×4 substituting one of 5 rank gray-levels based on the definition in Table 5.
(2) The number of the marked black and white of each block demonstrates black or white after the superimposition, as shown in Table 6.
(3) Four images whose sizes are 128×128 pixels, as shown in Fig. 3(a) Gray camouflaged image, Fig. 3(b) Secret image (1), Fig. 3(c) Secret image (2), and Fig. 3(d) Authentication image.

Table 5: The definition of black dots and white dots substituting gray-levels

Items / Images	Black(B) and White(W)[1]
Key image	{5(B), 11(W)} ∽{9(B), 7(W)}

[1] The number of black dots and white dots of 5 rank gray-levels of each block 4×4 size.

Table 6: The definition of black or white after the superimposition

Items / Images	Black(B)[1]	White(W)[2]
Superimposition image	13(B),3(W)	10(B), 6(W)

[1] Black of each block of 4×4 size.
[2] White of each block of 4×4 size.

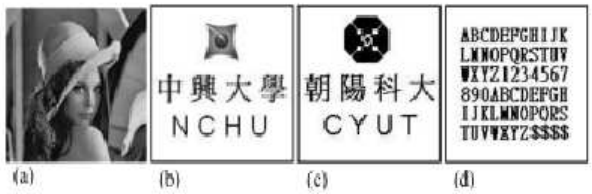

Fig. 3: (a) Gray camouflage image (b) Secret image (1) (c) Secret image (2) (d) Authentication image

4.1 Following Section 3.2, we produce Fig. 4(a) Key image and following Section 3.3, produce Fig. 4(b) Secret sharing image(1). These two images have the same visual meaning as the input gray camouflaged image. It demonstrates correctly as Fig. 4(c) Secret superimposition image (1) after the superimposition.
4.2 Following Section 3.2, we produce Fig. 5(a) Key image and, following Section 3.3, produce Fig. 5(b) Secret sharing image (2). These two images have the

same visual meaning as the input gray camouflaged image. This demonstrates correctly as Fig. 5(c) Secret superimposition image (2) after the superimposition.

4.3 Following Section 3.2, we produce Fig. 6(a) Secret sharing image (1) and, following Section 3.4., produce Fig. 6(b) Authentication sharing image (1). These two images have the same visual meaning as the input gray camouflaged image. This demonstrates correctly as Fig. 6(c) Authentication superimposition image after the superimposition.

4.4 Following Section 3.3, we produce Fig. 7(a) Secret sharing image (2) and, following Section 3.4., produce Fig. 7(b) authentication sharing image (2). These two images have the same visual meaning as the input gray camouflaged image. This demonstrates correctly as Fig. 7(c) Authentication superimposition image after superimposition.

4.5 Tests the superimposition of Secret sharing image (1) and Secret sharing image (2): The result of the superimposition of Fig. 4(b) Secret sharing image (1) and Fig. 5(b) Secret sharing image (2) cannot demonstrate each other's secret content. Fig. 8(c) is the superimposition image of Figs. 4(b) and 5(b).

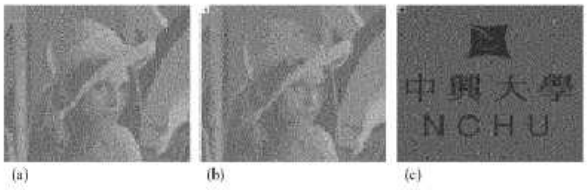

Fig. 4: (a) Key image (b) Secret sharing image (1) (c) Secret superimposition image (1)

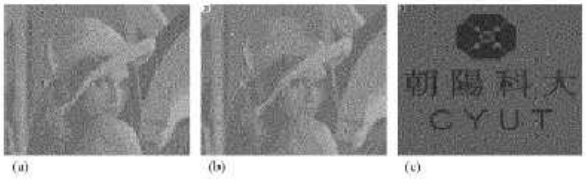

Fig. 5: (a) Key image (b) Secret sharing image (2) (c) Secret superimposition image (2)

5 Conclusions

This paper has proposed a method of visual authentication technology that works effectively when two parties hold the secret image and, alternately, the proposed method avoids negative outcomes when the key image is revealed. Furthermore, in this paper, the key image, the secret sharing image, and the authentication sharing image have the same visual meaning as the camouflaged image, allowing the user to easily manage and classify all kinds of sharing images.

Fig. 6: (a) Secret sharing image (1) (b) Authentication sharing image (1) (c) Authentication superimposition image

Fig. 7: (a) Secret sharing image (2) (b) Authentication sharing image (2) (c) Authentication superimposition image

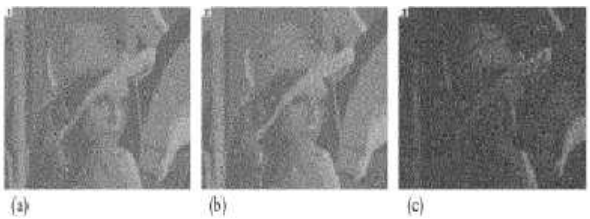

Fig. 8: (a) Like Fig. 4(b) Secret sharing image (1) (b) Like Fig. 5(b) Secret sharing image (2) (c) The superimposition of (a) and (b)

Acknowledgement

This research was supported by the National Science Council, Taiwan, R.O.C., under contract number NSC 101 - 2622 - E324 - 003 - CC3 and NSC 101 - 2221 - E - 324 - 005 - MY2.

References

[1] M. Naor, and A. Shamir, 'Visual cryptography',Advances in Cryptology-EUROCRYPT'94, LNCS 950, 1-12 (1995).

[2] National Bureau of Standards (U.S.): 'DES encryption standard (DES)', Federal Information Processing Standards Publication 46, National Technical Information Service, (1997).
[3] R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital secrets and public-key cryptosystems, Communications of the ACM, **21**,120-126 (1978).
[4] G. Ateniese , C. Blundo, A. De Santis and D. R. Stinson, Extended capabilities for visual cryptography, Theoretical Computer Science, **1-2**, 143-161 (2001).
[5] C. Blundo, A. De Santis and M. Naor, Visual cryptography for grey level images, Information Processing Letters, **75**, 255-259 (2000).
[6] C. Blundo, A. De Santis, and D.R. Stinson, On the contrast in visual cryptography schemes, Journal of Cryptology, **12**, 261-289 (1999).
[7] W.P. Fang, Friendly progressive visual secret sharing, Pattern Recognition, **41**, 1410-1414 (2008).
[8] J.B. Feng, H.C. Wu, C.S. Tsai, Y.F. Chang and Y.P. Chu, Visual secret sharing for multiple Secrets, Pattern Recognition, **41**, 3572-3581 (2008)
[9] T. Hofmeister, M. Krause, and H.U. Simon, Contrast-optimal k out of n secret sharing schemes in visual cryptography, Theoretical Computer Science, **240**, 471-485 (2000).
[10] R.J. Hwang and C.C. Chang, Hiding a picture in two pictures, Optical Engineering, **40**, 342-351 (2001).
[11] W.G. Tzeng, and C.M. Hu, A new approach for visual cryptography, Designs, Codes and Cryptography, **27**, 207-227 (2002).
[12] Y.F. Chen, Y.K. Chan, C.C. Huang, M.H. Tsai and Y.P. Chu, A multiple-level visual secret-sharing scheme without image size expansion, Information Sciences, **177**, 4696-4710 (2007).
[13] W.P. Fang, Non-expansion visual secret sharing in reversible style, International Journal of Computer Science and Network Security, **9**, 204-208 (2009).
[14] Y.C. Hou, C.F .Lin, and C.Y. Chang, Visual cryptography for color images without pixel expansion, Journal of Technology, **16**, 595-603 (2001).
[15] R. Ito, H. Kuwakado, and H. Tanaka, Image size invariant visual cryptography, IEICE Trans. on Fundamentals of Electronics, **10**, 2172-2177 (1999).
[16] T.Y. Kwon and J.S. Song, A study on the generalized key agreement and password authentication protocol', IEICE Trans. Communication, **9**, 2044-2050 (2000).
[17] C.N. Yang, and C.S. Laih, New colored visual secret sharing schemes, Designs, Codes and Cryptography, **20**, 325-336 (2000).
[18] P.W. Wong, and N. Memon,m Secret and public key image watermarking schemes for image authentication and ownership verification, IEEE Transactions on Image Processing, **10**, 1593-1601 (2001).
[19] T. Kawai , Y. Kitayama and M. Okada, An embedding multiplex secret in binary images by using pattern dither method, Proceedings of IEEE Systems, Man and Cybernetics Conference, **2**, 969-974 (1999).
[20] K. Oka, , Y. Nakamura, and K. Matsui, Embedding secret into a hardcopy image using micro-patterns, IEICE Trans. on Info. and Syst., **9**, 1624-1626 (1996).
[21] C.T. Hsu and J.L. Wu, Hidden digital watermarks in images, IEEE Transactions on Image Processing, **8**, 58-68 (1999).

Chin-Ling Chen was born in Taiwan in 1961. He received the B.S. degree in Computer Science and Engineering from the Feng Chia University in 1991; the M.S. degree and Ph.D. in Applied Mathematics at National Chung Hsing University, Taichung, Taiwan, in 1999 and 2005 respectively. He is a member of the Chinese Association for Information Security. From 1979 to 2005, he was a senior engineer at the Chunghwa Telecom Co., Ltd. He is currently a professor of the Department of Computer Science and Information Engineering at Chaoyang University of Technology, Taiwan. His research interests include cryptography, network security and electronic commerce.

Wen-Hu Chen was born in 1967. He received the Master degree in Department of Computer Science and Engineering from National Chung Hsing University, Taichung Taiwan in 2010. His research interests include Information security and Visual cryptology.

Chih-Cheng Chen is an assistant professor in Department of Industrial Engineering and Management in National Chin-Yi Institute of Technology. From 1996 to 2004, he was a senior engineer of Syntegra Tech. Company, which is an integration application software provider for the enterprise. He earned a Master and Ph.D. Degrees in Department of Mechatronics Engineering from National Changhua University of Education in 2005 and 2011 respectively. His research interests include mobile technology and RFID applications.

Yeong-Lin Lai received the Ph.D. degree from the Institute of Electronics, National Chiao Tung University, Taiwan, R.O.C., in 1997. He is currently a professor and the chairman of the Department of Mechatronics Engineering, National Changhua University of Education, Taiwan, R.O.C. His research interests include intelligent systems, RFID, RFIC, NEMS, and optoelectronic technologies. Dr. Lai received the Excellent Ph.D. Dissertation Award for Industries from Ministry of Education, Taiwan, R.O.C., in 1997. In 2001 and 2003, he was the visiting scholar of Communication Research Center, Ottawa, Canada. From 2004 to 2006, he received the Creation and Invention Award of National Changhua University of Education annually. In 2006, he received the Superior Mentor Award and the Superior Professor Award of National Changhua University of Education. In 2007, he received the Academic Research Award and the Outstanding Teaching Professor Award of National Changhua University of Education. In 2008, he received the Outstanding Educator Award from Ministry of Education, Taiwan, R.O.C. Dr. Lai received the Creation and Invention Award and the Outstanding Research Professor Award of National Changhua University of Education in 2010 and 2011, respectively.

Kuo-Kun Tseng received his PhD. degree at Computer Science and Information Engineering Department from Taiwan National Chiao Tung University in year 2007. He is an associate professor at Computer Science and Technology Department in Harbin Institute of Technology Shenzhen Graduate School. His research areas are the pattern matching, image processing, intelligent classification and network algorithms for mobile embedded system, cloud computing and Internet of Thing.