Secret Sharing Mechanism with Cheater Detection

Pei-Yu Lin*, Yi-Hui Chen†, Ming-Chieh Hsu* and Fu-Ming Juang*
*Department of Information Communication, Yuan Ze University, Chung-Li, Taiwan.
E-mail: {pylin; minghsu; s1016411}@saturn.yzu.edu.tw Tel: +886-3-4638800
†Corresponding author. Department of Applied Informatics and Multimedia, Asia University, Taichung, Taiwan.
E-mail: chenyh@asia.edu.tw Tel: +886-4-23323456

***Abstract*—Cheater detection is essential for a secret sharing approach which allows the involved participants to detect cheaters during the secret retrieval process. In this article, we propose a verifiable secret sharing mechanism that can not only resist dishonest participants but can also satisfy the requirements of larger secret payload and camouflage. The new approach conceals the shadows into a pixel pair of the cover image based on the adaptive pixel pair matching. Consequently, the embedding alteration can be reduced to preserve the fidelity of the shadow image. The experimental results exhibit that the proposed scheme can share a large secret capacity and retain superior quality.**

I. INTRODUCTION

Secret sharing mechanism can distribute secret information among involved participants for reducing the risk of distorted, lost, and stolen [1] [2], [3]. The (t, n)-threshold secret sharing technique was first introduced by Blakely [1] and Shamir [2]. To share a secret among n participants, the secret can be divided and encoded into n shadows by the secret sharing technique. The n shadows thereby can be distributed to the n corresponding participants. That is, each participant possesses a portion of the secret. Note that, a participant who possesses fewer than t shadows is incapable of identifying any knowledge from their own shadow. With any t out of n shadows, the authorized participants can cooperate to reveal the secret correctly.

The (t, n)-threshold secret sharing technique [1] [2], [3], however, assumes that the provided shadows are genuine by the honest participants when cooperation. In [4], Tompa and Woll prove that such assumption is insecure and inapplicable in the real-world. Fraudulent participant may provide a fake shadow to cheat others of their genuine shadows. The fraudulent participant with any t shadows can thereby retrieve the secret himself. Hence, the ability of cheater detection is a critical requirement in the secret sharing system [5], [6], [7].

In additional, the derived shadows by the secret sharing technique [1] [2], [3] [4] are meaningless. The noise-like shadows may attract intruders when communication and storage. The secret sharing schemes [8], [9] conceal the derived shadows into cover images and form the meaningful marked images to reduce attention from malicious intruders.

To achieve the cheater detection, the schemes [10]-[14] embed not only the shadows but also the parity check bits into each 2×2 block of the cover image. The involved participants can validate the genuineness of shadows by the parity check. The qualities of their marked image are satisfactory. The PSNRs of schemes [10][11][12] are around 34 dB to 40 dB, and that of [13] and [14] are 45 dB and 43 dB. To reduce the attention from malicious intruders, the quality of the marked image is an important requirement in the secret sharing system.

To share a large secret payload and preserve the marked image quality is a trade-off issue. In this article, we propose an efficient secret sharing mechanism based on the adaptive pixel pair matching (APPM) function [15]. The new approach can satisfy the essentials of cheater detection, large secret sharing, lossless restore, and marked image quality.

The rest of the article is organized as follows. The proposed verification secret sharing approach is presented in Section II. The experimental results are analyzed in Section III. Finally, conclusions are made in Section IV.

II. THE PROPOSED ALGORITHM

The proposed verification secret sharing (VSS) algorithm offers verifiable mechanism to prevent fraudulent participants and convey larger secret payload. Given a shared secret, the VSS derives shadows from the secret and produce corresponding n meaningful marked images as introduced in Section II-A. The meaningful marked images can avoid attracting attention to the secret shadows. With any t out of n marked images, the involved participants can authenticate the genuineness of the shadows of the provided marked images in order to detect any cheaters. The authorized participants can reveal the secret losslessly. Section II-B introduces the verification and the extraction procedure.

A. Secret Sharing Procedure

In the (t, n)-threshold secret sharing system, the dealer assigns a unique key, K_j, and gray-scale cover image, O_j, with size of $H \times W$ pixels for each participant, where $1 \le j \le n$.

To share the secret S among n participants, S is converted into 7-ary notational system. Here, the length of S is $H \times W/2 \times (t-1)$ digits and the digit value is among [0, 6]. For example, let the pixels in the secret be 66 and 237. The converted digits are presented as $S=\{1, 2, 3, 4, 5, 6\}_7$. For detecting cheaters, a verification stream, V, in an 7-ary notational system is generated by the dealer's key K. The length of V is $H \times W/2$ digits.

To generate the shadows from S with larger capacity, the VSS shares $n \times (t-1)$ secret digits of S into n sharing

polynomial functions in the (t, n)-threshold sharing approach instead of sharing one secret pixel into a polynomial function [10][11]. For the sake of convenience, let the shared $n\times(t-1)$ secret digits of S be s_{il}, where $1\le i\le n$, and $1\le l\le(t-1)$, and the n verification digits of V be v_i. The corresponding n sharing polynomial $f_i(x)$ can be formulated as

$$f_i(x) = (v_i + \sum_{l=1}^{t-1} s_{il}x^l) \bmod 7. \quad (1)$$

The shadows y_{ij} thereby can be generated by feeding the key K_j into $f_i(x)$, $1\le j\le n$,

$$y_{ij} = f_i(K_j), \text{ where } 1\le j\le n. \quad (2)$$

Apparently, the shadow derivation phase can share $n\times(t-1)$ secret digits of S and n verification digits of V into n sharing polynomial functions $f_i(x)$ and thereby generate $n\times n$ shadows y_{ij}. With repeating this phase, the remaining secret digits of S and verification digits of V can be shared and then derive the corresponding shadows.

The VSS conceals the shadows into the corresponding cover image via block-wise manner. The block-wise manner can enhance the cheater detection capability than that of pixel-wise manner. Accordingly, the cover image O_j is divided into non-overlapping blocks with size $(2\times n)$ pixels, $1\le j\le n$. The number of blocks is $H\times W/(2\times n)$. For the sake of convenience, let B_j be a block of the corresponding image O_j and the formula can be expressed as,

$$B_j = \{(a_{ji}, b_{ji}) \mid i=1, 2, \ldots, n\}. \quad (3)$$

Here, the (a_{ji}, b_{ji}) stands for the i-th pixel pair of block B_j, $1\le i\le n$. The derived shadows y_{ij} afterward are concealed into the corresponding pixel pair (a_{ji}, b_{ji}) of block B_j based on the adaptive pixel pair matching (APPM) function [15], where $1\le i, j\le n$. The APPM function is defined as

$$\text{APPM}(g, q)=(g + c\times q) \bmod 7. \quad (4)$$

Here, c is a constant and can be found in [15] for more detail. APPM values are filled with the digits from 0 to 6 and mutually exclusive.

The camouflaged shadow pair (a'_{ji}, b'_{ji}) subsequently can be derived by adjusting the corresponding shadow y_{ij} at the APPM matrix of (a_{ji}, b_{ji}). If $APPM(a_{ji}, b_{ji})=y_{ij}$, the $(a'_{ji}, b'_{ji})=(a_{ji}, b_{ji})$. Otherwise, finding the row at a'_{ji} and the column at b'_{ji} for the remaining neighbors of (a_{ji}, b_{ji}) such that $APPM(a'_{ji}, b'_{ji})=y_{ij}$.

By repeating the phases, the dealer can generate secret shadows and then camouflage the secret shadows into the remaining blocks of corresponding cover images in order to obtain n marked images O'_j, $1\le j\le n$. The marked image O'_j are meaningful and the dealer thereby can distribute the O'_j, and the key K_j to the corresponding participants.

B. Verification and Retrieval Procedure

Given any t out of n marked images O'_j and keys K'_j from the involved participants, where $t\le j\le n$. The participants can verify the genuineness of the provided shadows for detecting dishonest participants before revealing the secret. The authorized participants afterward can reveal the secret S with lossless.

In the beginning, the verification digits V with length $H\times W/2$ in an 7-ary notational system is generated by the dealer's key K. The verification process is based on block-wise manner. Hence, the marked image O'_j is divided into non-overlapping blocks with size $(2\times n)$ pixels, $t\le j\le n$. Here, the block numbers of each O'_j are $H\times W/(2\times n)$.

For the sake of brevity, let B'_j be a block of the corresponding image O'_j, and the block formula can be expressed as $B'_j = \{(a'_{ji}, b'_{ji}) \mid 1\le i\le n\}$. Here, the (a'_{ji}, b'_{ji}) labels the i-th pixel pair of bock B'_j. And let the n verification digits of V be v_i, $1\le i\le n$. Along with v_i, the process of verifying the genuineness of shadows of blocks B'_j, $t\le j\le n$, is described as follows:

Step 1: Compute the shadows y'_{ij} by feeding the pixel pair (a'_{ji}, b'_{ji}) of B'_j into the APPM function, where $1\le i\le n$,

$$y'_{ij} = APPM(a'_{ji}, b'_{ji}) = (a'_{ji} + c\times b'_{ji}) \bmod 7. \quad (5)$$

Here, c is a constant and is computed as the same manner as in the secret sharing procedure.

Step 2: Derive n $(t-1)$-degree polynomials $f'_i(x)$, $1\le i\le n$, by Lagrange's interpolation formula with the shadows y'_{ij} and the participants' keys K'_j, $t\le j\le n$,

$$f'_i(x) = (v'_i + \sum_{l=1}^{t-1} s'_{il}x^l) \bmod 7. \quad (6)$$

Step 3: Compare the value of v'_i from $f'_i(0)$ with the value of verification digit v_i. If $v'_i\ne v_i$, $1\le i\le n$, then the shadows s'_{il} are counterfeit and terminate the retrieval procedure. Otherwise, the provided shadows s'_{il} are valid and follow the next steps.

Step 4: Obtain the secret digits s_{il} by extracting the last $(t-1)$ coefficients of $f'_i(x)$. Here, $s_{il} = s'_{il}$, for $1\le i\le n$ and $1\le l\le(t-1)$.

Repeating the above steps until all blocks of the corresponding image O'_j has been processed. With the $H\times W/2\times(t-1)$ extracted secret digits, the authorized participants finally can reveal the secret S losslessly by converting the secret digits in 7 notational system to decimal system.

III. Experimental Results

The most commonly used gray-scale images, Airplane, Baboon, Lena, and Peppers, are employed as the cover images as shown in Fig. 1. Here, the size of the test images is with 512×512 pixels. To evaluate the quality of the marked

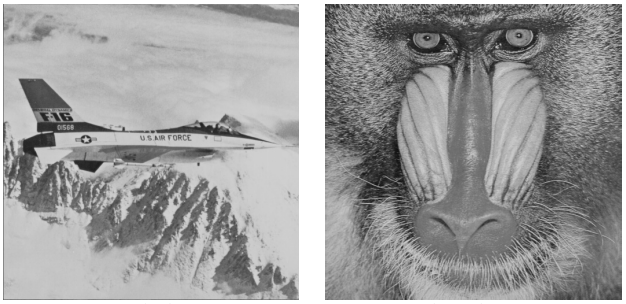
images, the peak signal-to-noise rate (PSNR) is adopted and formulated as

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right)\text{dB}. \quad (7)$$

The mean square error (*MSE*) of an image with $H\times W$ pixels is defined as

$$MSE = \frac{1}{H\times W}\sum_{u=1}^{H}\sum_{v=1}^{W}(p_{uv}-\hat{p}_{uv})^2, \quad (8)$$

where p_{uv} is the host pixel value and p'_{un} is the shadow pixel value.



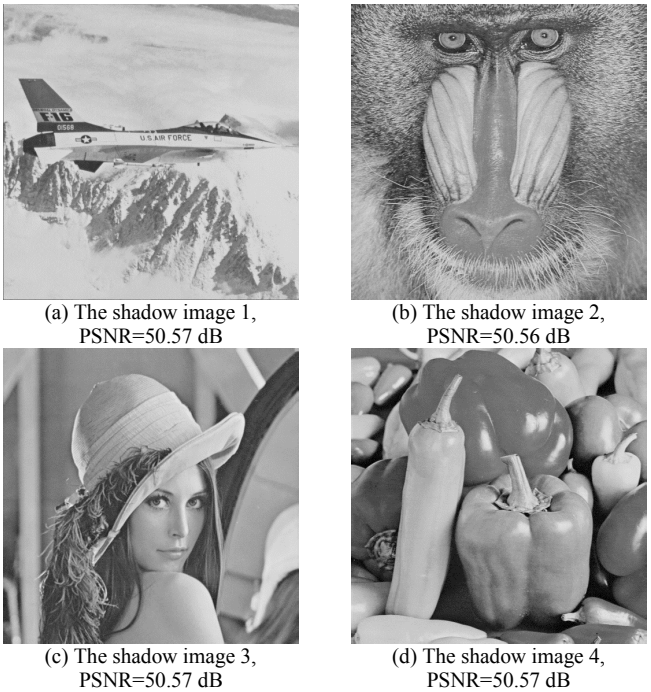
(a) Airplane (b) Baboon

(c) Lena (d) Peppers

Fig. 1 Test images.

Fig. 2 shows the results of the four marked images of the VSS method in (3, 4)-threshold system. The VSS conceals the noise-like shadows into the meaningful cover image for the sake of reducing the attraction risk of intruders. From the human visual perception, the difference between the original cover images and the marked images is imperceptible. The average PSNR value of the marked images is superior and around 50.5 dB.

Fig. 3 illustrates the maximum capacity of the shared media under different settings of *t*. the VSS can embed $367{,}966\times(t-1)$ secret bits into an 512×512 pixels cover image and modify the value of original pixel at most with (±1). It is obvious that the secret capacity can be increased with larger *t*, and the qualities of the marked images preserve similar. The new scheme can achieve the essentials of both high capacity and fidelity.



(a) The shadow image 1, PSNR=50.57 dB (b) The shadow image 2, PSNR=50.56 dB

(c) The shadow image 3, PSNR=50.57 dB (d) The shadow image 4, PSNR=50.57 dB

Fig. 2 The results of the shadow images.

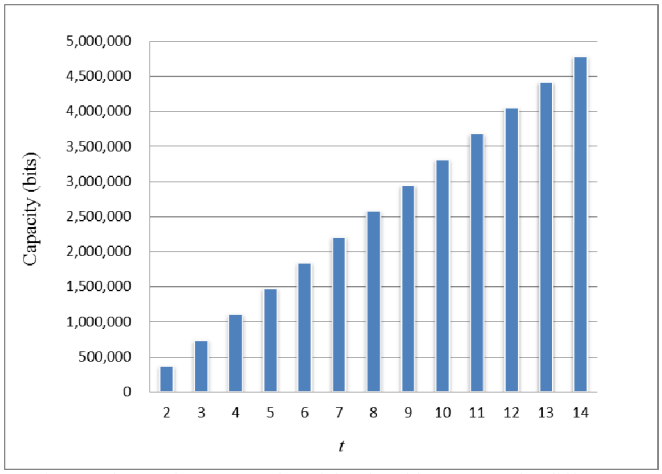
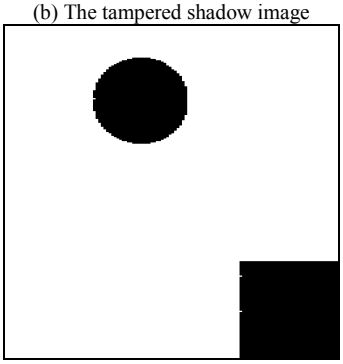


Fig. 3 The maximum capacity of the sharable secret under different *t* setting.

The ability of detecting fraudulent participants during cooperation is critical in the VSS approach. That is, an efficient VSS scheme should allow participants to verify the genuineness of the provided shadow images. Fig. 4(a) displays the original shadow image. Fig. 4(b) demonstrates the tampered marked image by inserting illegal pattern and flower. The black points in Fig. 4(c) indicate the detected results by the verification process from Fig. 4(b). The high density of the black points implies the satisfactory detection ability. Intuitively, the VSS can achieve superior cheater detectability by the verifications.

(a) The genuine shadow image

(b) The tampered shadow image



(c) The first verification result of (b)

Fig. 4 The tampering attack and the verification result.

IV. CONCLUSIONS

To share large secret capacity and preserve the fidelity of the marked image is a trade-off issue. The designed verification secret sharing (VSS) mechanism can share considerable secret payload by increasing the values of t while preserving the fidelity of marked image. The verification of VSS is efficient in authenticate the genuineness of the provided shadows to detect fraudulent cheaters. From the experiments, it is observed that our proposed technique has achieved the better performances of the steganography, secret capacity, lossless secret, high PSNR of marked image, and cheater detection than that of related secret sharing schemes.

REFERENCES

[1] G. R. Blakley, "Safeguarding cryptographic keys," *Proceedings of AFIPS National Computer Conference*, vol. 48, pp. 313-317, 1979.

[2] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[3] M. Naor and A. Shamir, "Visual cryptography," *Advances in Cryptology: Eurocrypt'94*, Spring-Verlag, Berlin, pp. 1-12, 1995.

[4] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 2, pp. 133-138, 1988.

[5] C. M. Hu and W. G. Tzeng, "Cheating prevention in visual cryptography," *IEEE Transactions on Image Processing*, vol. 16, no. 1, pp. 36-45, 2007.

[6] P. Y. Lin, J. S. Lee and C. C. Chang, "Distortion-free secret image sharing mechanism using modulus operator," *Pattern Recognition*, vol. 42, no. 5, pp. 886-895, 2009.

[7] P. Y. Lin and Chi-Shiang Chan, "Invertible Secret Image Sharing with Steganography," *Pattern Recognition Letters*, vol. 31, no. 13, pp. 1887-1893, 2010.

[8] C. C. Thien and J. C. Lin, "Secret image sharing," *Computer & Graphics*, vol. 26, no. 1, pp. 765-770, 2002.

[9] Y. S. Wu, C. C. Thien and J. C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, no. 7, pp. 1377-1385, 2004.

[10] C. C. Lin and W. H. Tsai, "Secret image sharing with steganography and authentication," *The Journal of Systems and Software*, vol. 73, no. 3, pp. 405-414, 2004.

[11] C. N. Yang, T. S. Chen, K. H. Yu and C. C. Wang, "Improvements of image sharing with steganography and authentication," *The Journal of Systems and Software*, vol. 80, no. 7, pp. 1070-1076, 2007.

[12] C. C. Chang, Y. P. Hsieh and C. H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130-3137, 2008.

[13] C. C. Chang, Y. H. Chen and H. C. Wang, "Meaningful secret sharing technique with authentication and remedy abilities," *Information Sciences*, vol. 181, no. 14, pp. 3073-3084, 2011.

[14] M. Ulutas, G. Ulutas and V. V. Nabiyev, "Medical image security and EPR hiding using Shamir's secret sharing scheme," *Journal of Systems and Software*, vol. 84, no. 3, pp. 341-353, 2011.

[15] W. Hong and T. S. Chen, "A novel data embedding method using adaptive pixel pair matching," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 176-184, 2012.