Analysis of an Image Secret Sharing Scheme to Identify Cheaters

Jung-San Lee leejs@fcu.edu.tw
Department of Information Engineering and Computer Science Feng Chia UniversityTaichung, 40724, Taiwan

Pei-Yu Lin pagelin3@gmail.com
Department of Information Communication Yuan-Ze University Chung-li, 32003, Taiwan

Chin-Chen Chang alan3c@gmail.com
Department of Information Engineering and Computer Science Feng Chia University Taichung, 40724, Taiwan

Abstract

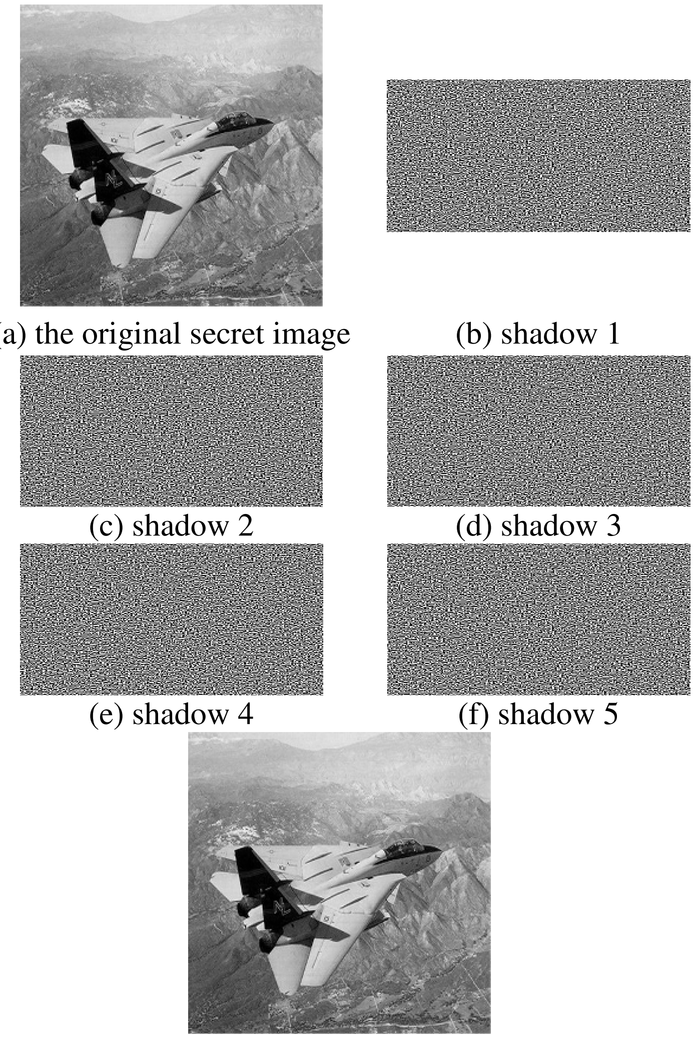
Secret image sharing mechanisms have been widely applied to the military, e-commerce, and communications fields. Zhao et al. introduced the concept of cheater detection into image sharing schemes recently. This functionality enables the image owner and authorized members to identify the cheater in reconstructing the secret image. Here, we provide an analysis of Zhao et al.'s method: an authorized participant is able to restore the secret image by him/herself. This contradicts the requirement of secret image sharing schemes. The authorized participant utilizes an exhaustive search to achieve the attempt, though, simulation results show that it can be done within a reasonable time period.

Keywords: Analysis, Secret image sharing, (t, n)-threshold, Cheater detection

1. INTRODUCTION

Shamir first introduced the concept of secret sharing in 1979 [10]. Given a set of participants $P = \{P_1, P_2, \ldots, P_n\}$, each of them possesses a secret shadow generated from the secret S. Hereafter, any t out of n members can reveal S by collecting t secret shadows, i.e. (t, n)-threshold mechanism. In such a system, participants with fewer than t shadows have no more knowledge of the secret than the one with nothing. This can effectively enhance the security of communications in an insecure network.

Engineers extend this concept to protect confidential images. Due to its practicability, secret image sharing mechanisms have been widely applied to the military, e-commerce, and communications fields [2, 3, 4, 5, 6, 8, 12, 13]. As illustrated in Fig. 1, in a (2, 5)-threshold scheme, while delivering a secret image F-14 to five authorized members, an image owner constructs several shadows from the original image in advance. Then, the owner issues each member a distinct shadow. No one who possesses fewer than two shadows can learn anything about the secret image. Only when two authorized members provide their shadows can the secret image be restored.



(a) the original secret image (b) shadow 1

(c) shadow 2 (d) shadow 3

(e) shadow 4 (f) shadow 5

(g) the reconstructed image

FIGURE 1: Secret image sharing: F-14

Recently, based on Thien and Lin's method, Zhao et al. proposed a novel secret image sharing scheme that introduces the concept of cheater identification [5, 7, 14]. This enables the image owner and authorized members to detect the cheater while reconstructing the secret image. It is claimed in [14] that their (t, n)- threshold method can confirm the following properties:

i. Involved participants can detect cheaters no matter who they are;
ii. At least t authorized participants can cooperate to reveal the secret image;
iii. Participants can join in recovering different original secret image as long as they possess a secret shadow;
iv. No secure channel is needed between the image owner and authorized participants;
v. The size of shadow image is smaller than that of original secret image.

Unfortunately, we find that there exists a design weakness in Zhao et al.'s method: an authorized participant is able to figure out a congruent number of the private key of the image owner using the exhaustive search. Later, the participant can utilize this number to restore secret images simply; this contradicts Property ii. Employing the exhaustive search, though, experimental results show that this can be done within a reasonable time period.

The rest of this article is organized as follows. We briefly introduce Zhao et al.'s mechanism in Section 2. The design weakness of the method is proven in Section 3. We make conclusions in Section4.

2. REVIEW OF AN IMAGE SECRET SHARING SCHEME TO IDENTIFY CHEATERS

Zhao et al.'s method consists of three phases: initialization phase, construction phase, and verification phase. Assume that $P = \{P_1, P_2, \ldots, P_n\}$ is the set of participants and any t out of n participants can cooperate to recover the secret image. Details of these phases are described as follows [14].

2.1 Initialization phase:

To begin with, the gray values of the secrete image from 251 to 255 shall be truncated to 250 since 251 is the greatest prime not larger than 255. The image owner *O* selects two large primes (p, q) and computes $N = p \times q$. *O* picks a generator $g \in [N^{1/2}, N]$ and constructs an RSA-based public and private key pair (e_0, d_0) satisfying $e_0 \times d_0 = 1 \bmod \varphi(N)$. *O* publishes (e_0, g, N) [9,11].

Each participant $P_i \in P$ chooses a random number s_i ranged within [2, N] as its secret shadow. Pi computes $\alpha_i = g^{s_i} \bmod N$ and proves it to *O*. *O* shall ensure $\alpha_i \neq \alpha_j$ for $P_i \neq P_j$.

2.2 Construction phase:

Step 1: *O* computes $\alpha_0 = g^{d_0} \bmod N$ and $\beta_i = \alpha_i^{d_0} \bmod N, i = 1, 2, ..., n.$ *O* publishes α_0.

Step 2: According to lexicography order, *O* divides the secret image *I* into several sections. For each section *k* containing *t* pixels, *O* constructs a (t-1)th-degree polynomial as follows,

$$f_k(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1} \bmod 251, \quad (1)$$

where $a_0, a_1, ..., a_{t-1}$ are the *t* pixels of section *k*.

Step 3: O computes $y_i = f_k(\beta_i)$, (2)

for i = 1, 2, …, n, and publishes y_1, y_2, …, y_n.

2.3 Verification phase:

Step 1: P_i utilizes its own secret shadow s_i to generate sub-secret $\beta_i = \alpha_{0.}^{s_i} \bmod N.$

Step 2: Anyone can verify β_i by checking whether $\alpha_{i.} = \beta_i^{e_0} \bmod N$ holds or not. If it holds, β_i is valid; otherwise, P_i may be a cheater.

Step 3: By collecting *t* pairs of (β_i , y_i)'s and the Lagrange interpolating polynomial, the participants can determine a (t-1)th-degree polynomial as follows,

$$f_k(x) = \sum_{j=1}^{t} y_j \prod_{i=1, i \neq j}^{t} \left(\frac{x - \beta_i}{\beta_j - \beta_i} \right) \bmod 251$$

$$= a_0 + a_1 x + ... + a_{t-1} x^{t-1} \bmod 251.$$

Hence, the secret image *I* is restored.

3. SECURITY ANALYSIS

In this section, we demonstrate that Zhao et al.'s (t, n)-threshold secret image sharing mechanism does not comply with Property ii. We first describe the system scenario. O possesses two secret images I_1 and I_2. P_i keeps a secret shadow s_i and publishes $\alpha_i = g^{s_i} \bmod N$. For I_1, according to Equation (1), O has to construct the polynomial

$$f_{k1}(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1} \text{ mod } 251,$$

where $a_0, a_1, ..., a_{t-1}$ are the t pixels of section k. Furthermore, O must compute $\beta_i = \alpha_{i.}^{d_0} \bmod N$ and publish $y_{i1} = f_{k1}(\beta_i)$, for $i = 1,2,...,n.$

By the same manner, O computes the following polynomial for I_2:

$$f_{k2}(x) = b_0 + b_1 x + ... + b_{t-1} x^{t-1} \text{ mod } 251,$$

where $b_0, b_1, ..., b_{t-1}$ are the t pixels of section k. Moreover, O computes and publishes $y_{i2} = f_{k2}(\beta_i)$, for $i = 1,2,...,n,$ according to Equation (2).

Assume that P_i has joined in recovering the secret image I_1 and obtained the unique polynomial $f_{k1}(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1}$ mod 251. We employ the following proposition to show the design weakness in [14].

Proposition: P_i can restore the secret image I_2 by itself.

Proof: Applying β_i to $f_{k1}(x)$, P_i yields the following:

$$\begin{aligned} y_{i1} &= a_0 + a_1(\beta_i \bmod 251) + ... + a_{t-1}(\beta_i^{t-1} \bmod 251) \bmod 251 \\ &= a_0 + a_1(\alpha_0^{s_i} \bmod 251) + ... + a_{t-1}((\alpha_0^{s_i})^{t-1} \bmod 251) \bmod 251 \\ &= a_0 + a_1(\alpha_i^{d_0} \bmod 251) + ... + a_{t-1}((\alpha_i^{d_0})^{t-1} \bmod 251) \bmod 251 . \end{aligned}$$

According to Fermat's Theorem [11] and the equation $\alpha_i^{d_0} \bmod 251$, P_i can fabricate d_0' satisfying

$d_0' = d_0$ mod 250.

That is, $0 \le d_0' \le 249$. Using the exhaustive search, P_i can find an d_0' answering to

$$\begin{aligned} &\alpha_i^{d_0'} \bmod 251 = \beta_i \bmod 251, \\ &\alpha_i^{2d_0'} \bmod 251 = \beta_i^2 \bmod 251, \\ &\vdots \\ &\alpha_i^{(t-1)d_0'} \bmod 251 = \beta_i^{(t-1)} \bmod 251 . \end{aligned}$$

For the section k in I_2, P_i collects $y_{12}, y_{22}, ..., y_{t2}$, and constructs

$$\begin{aligned} y_{12} &= b_0' + b_1'(\alpha_1^{d_0'} \bmod 251) + ... + b_{t-1}'((\alpha_1^{d_0'})^{t-1} \bmod 251) \bmod 251, \\ y_{22} &= b_0' + b_1'(\alpha_2^{d_0'} \bmod 251) + ... + b_{t-1}'((\alpha_2^{d_0'})^{t-1} \bmod 251) \bmod 251, \\ &\vdots \\ y_{t2} &= b_0' + b_1'(\alpha_t^{d_0'} \bmod 251) + ... + b_{t-1}'((\alpha_t^{d_0'})^{t-1} \bmod 251) \bmod 251. \end{aligned}$$

Since $d_0', \alpha_1, \alpha_2, ...,$ and α_t are known to P_i, P_i can obtain the following system of equations.

$$y_{12} = b_0' + b_1'\delta_1 + ... + b_{t-1}'\delta_1^{t-1} \bmod 251,$$

$y_{22} = b'_0 + b'_1\delta_2 + ... + b'_{t-1}\delta_2^{t-1} \bmod 251,$

$\vdots$

$y_{t2} = b'_0 + b'_1\delta_t + ... + b'_{t-1}\delta_t^{t-1} \bmod 251,$

where $\delta_1 = \alpha_1^{d'_0} \bmod 251, \delta_2 = \alpha_2^{d'_0} \bmod 251, ..., \delta_t = \alpha_t^{d'_0} \bmod 251.$ Hence, P_i has the (t-1)th degree Vandermonde matrix:

$$A = \begin{bmatrix} 1 & \delta_1 & \delta_1^2 & \cdots & \delta_1^{t-1} \\ 1 & \delta_2 & \delta_2^2 & \cdots & \delta_2^{t-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \delta_t & \delta_t^2 & \cdots & \delta_t^{t-1} \end{bmatrix}.$$

As $\alpha_i \neq \alpha_j$, it implies $\delta_i \neq \delta_j$, for $i = 1,2,...,n,$ and

$$\det(A) = \prod_{1 \le i \le j \le t} (\delta_j - \delta_i) \neq 0 .$$

That is, A is a non-singular matrix. Thus, P_i can obtain a unique solution $\{b'_0, b'_1, ..., b'_{t-1}\} = \{b_0, b_1, ..., b_{t-1}\}$ from the system of equations. Eventually, P_i is able to restore the pixels of the secret image by itself. □

The proposition shows that Zhao et al.'s method violates Property ii. Even though P_i applies the exhaustive search, this attempt can be completed in 250 tries at most. We conduct experiments in the VC 6.0 language to confirm the feasibility of figuring out d'_0. Simulators were performed on a PC with Intel L2300 CPU; the RSA algorithm was implemented according to the public OpenSSL library [1]. Since $g \in [N^{1/2}, N]$, the input size is set to 1024 bits. The length of module N is set to 256, 512, and 1024 bits, respectively. The running time of 250 tries is illustrated in Table 1. It is clear that P_i is able to imitate d'_0 within a very short time period under these cases.

	Module length (bit)		
	256	512	1024
Running time (second)	0.268151	0.411303	1.0416215

TABLE 1: Running Time under Different Module Length.

4. CONCLUSIONS

In this article, we have proven that an authorized participant can restore the secret image without the help of others in Zhao et al.'s (t, n)-threshold. Even if the compromise has been done by the exhaustive search, the simulation shows that it is completed within a rather short time interval.

ACKNOWLEDGMENT

This research is partially supported by the National Science Council, Taiwan, ROC, under contract No. NSC 98-2218-E-035-001-MY3. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

5. REFERENCES

[1] The openSSL project, http://www.openssl.org

[2] T. S. Chen and C. C. Chang. "*New method of secret image sharing based on vector quantization*". Journal of Electronic Imaging, 10(4): 988-997, 2001

[3] C. C. Chang and R. J. Hwang. "*Sharing secret images using shadow codebooks*". Information Sciences, 335-345, 1998

[4] C. C. Chang, C. Y. Lin and C. S. Tseng. "*Secret image hiding and sharing based on the (t, n)-threshold*". Fundamenta Informaticae, 76(4): 399-411, 2007

[5] C. Thien and J. Lin. "*Secret image sharing*". Computer & Graphics, 26(1): 765-770, 2002

[6] J. B. Feng, H. C. Wu, C. S. Tsai and Y. P. Chu. "*A new multi-secret images sharing scheme using Lagrange's Interpolation*". The Journal of Systems and Software, 76: 327-339, 2005

[7] R. J. Hwang, W. B. Lee and C. C. Chang. "*A concept of designing cheater identification methods for secret sharing*". The Journal of Systems and Software, 46: 7-11, 1999

[8] R. Lukac and K. Plataniotis. "*Colour image secret sharing*". Electronics Letters, 40(9): 529-531, 2004

[9] R. Rivest, A. Shamir and L. Adleman. "*A method for obtaining digital signatures and public key cryptosystem*". Communications of the ACM, 21(2): 120-126, 1978

[10] A. Shamir. "*How to share a secret*". Communications of the ACM, 22(11): 612-613, 1979

[11] W. Stallings. "*Cryptography and Network Security – Principles and Practices*", Pearson Education Inc., Fourth Edition, pp. 238-241 (2006)

[12] C. S. Tsai, C. C. Chang and T. S. Chen. "*Sharing multiple secrets in digital images*". The Journal of Systems and Software, 64(2): 163-170, 2002

[13] R. Wang and C. Su. "*Secret image sharing with smaller shadow images*". Pattern Recognition Letters, 27: 551-555, 2006

[14] R. Zhao, J. J. Zhao, F. Dai and F. Q. Zhao. "*A new image secret sharing scheme to identify cheaters*". Computer Standards & Interfaces, 31(1): 252-257, 2009