An in-depth analysis of strong *t*-consistency on secret image sharing

Anneke Soraya Hidayat and Gil-Je Lee
School of Computer Science and Engineering, Kyungpook National University, Daegu, South Korea
Eun-Jun Yoon
Department of Cyber Security, Kyungil University, Gyenggsan-Si, South Korea, and
Kee-Young Yoo
School of Computer Science and Engineering, Kyungpook National University, Daegu, South Korea

Received 1 September 2015
Revised 19 September 2015
Accepted 1 February 2016

Abstract

Purpose – The detection of an adversary in secret image sharing has been a problematic side in the reconstruction phase. Some of verifiable secret sharing solutions have been proposed to solve the problem. However, there is some computational limitation in the previous schemes. The purpose of this paper is to analyze the importance of consistency for detecting an adversary in a secure reconstruction phase. Strong *t*-consistency assures the correctness of reconstructed secret as long as participants $P \in N$ and $n(P) = t$. Consistency is a solution for preventing the participant to be absent and helps the dealer to easily detect the adversary without an additional verification step.

Design/methodology/approach – This paper focuses on secure reconstruction, and uses two different approaches, namely, single-secret and multi-secret, to experiment the relationship between the given variable (t,m,n) and the adversaries by observing the quality test result, polynomial approach and visualization.

Findings – The results show that t and m are inversely proportional to the image quality without respect to the polynomial approach. The reconstruction phase is declared as securely conducted when $m = 2t - 1$, for both single- and multi-secret approaches.

Originality/value – The application of consistency is a considerable step for securing the secret from an adversary by combining the reconstruction phase and the consistency combination at once, removing the need for additional separate verification steps for decreasing the computational time, especially in secret image sharing.

Keywords Consistency, Adversary detection, Secret image sharing, Secure reconstruction

Paper type Research paper

1. Introduction

In 1979, Shamir (1979) and Blakley (1979) had proposed a secret sharing scheme based on polynomial approach and geometry, respectively. Both approaches have threshold

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (NRF-2015R1D1A1A01060801), and by the Institute for Information & Communications Technology Promotion (IITP) grant,

International Journal of Pervasive Computing and Communications
Vol. 12 No. 1, 2016
pp. 107-126

1742-7371
DOI 10.1108/IJPCC-01-2016-0006

access structure, which allows a qualified subset t or more participants among the total participants n to recover the secret messages. The reconstruction is limited to the subset $t-1$ or less participants. In Shamir's $(t,n)-$ threshold secret sharing, the robustness is guaranteed such that any t honest participants can reconstruct the polynomial back and get the original secret s by using Lagrange interpolation. The secret sharing schemes are useful as a solution for managing the cryptographic keys, in such an environment that need security among the group of participants. The system is assumed that the dealer D and all of the participants are honest. Apart from Shamir's scheme and Blakley's scheme, there are several secret sharing schemes by using different mathematical approaches such as Chinese Remainder Theorem (CRT) (Mignotte, 1983; Asmuth and Bloom, 1983; Dong, 2015), as well as a Boolean-based (Chen and Wu, 2014; Yang *et al.*, 2015; Chao and Lin, 2009) and Hermite interpolation (Tadayon *et al.*, 2014).

The application of secret sharing can not only be applied in data numbers but also in various media, such as documents, images and audio and video presentations. (Thien and Lin, 2002) were first introduced as the application of secret sharing on an image media in 2002. By the given secret image S, the dealer distributes the share images by using a polynomial with degree $t-1$ to n participants, and no less than t participants can reconstruct the secret image back. Instead of using Shamir's secret sharing, they used the multi-secret sharing to put up to $t-1$ secret image pixels in one polynomial; thus, the size of the share image will be reduced to $1/t$.

Most of the secret sharing schemes were declared as unconditionally secure. Especially on Shamir's secret sharing, it is proved that the secret is consistent and secure from $t-1$ participant in the reconstruction phase (Beimel, 2011). The schemes were secure from attacks, such as Bruce force attack, which means that there is no limit to the adversary's computational boundary. However, it is only secure when there are exactly t or less participants present for the reconstruction phase as stated by Tompa and Woll (1989). Meanwhile, if $t-1$ is assured to get nothing about the secret and t participants can get the original secret, there is a possibility of either inside or outside adversary to take the opportunity to get the secret without giving its share. Suppose there are m participants, where $m > t-1$, the adversary A can arrange the order of the share collection; thus, there are exactly t shares collected excluded from the adversary and put its order in the last. This problem is stated as consistency (Harn and Lin, 2009; Tian *et al.*, 2013; Qassim, 2013).

The detection and identification of an adversary are needed during the reconstruction phase to prevent the adversaries from getting the secret without giving their shares. The verifiable secret sharing (VSS) is one of the solutions to detect and identify the adversary in the reconstruction phase. Some VSS schemes are proposed by Harn *et al.* (2014), Liu *et al.* (2015), Chen *et al.* (2015), which are based on CRT. However, the VSS schemes require much computational time, as it performs more calculations for both verification and reconstruction. Meanwhile, we need to ensure that all the m participants are honest when $m > t-1$. To reduce the computation in the VSS, some methods focused on consistency problem which was proposed by Harn and Lin (2010), Harn (2014), Fuyou *et al.* (2015). Lin and Tsai (2004) introduced the first secret image sharing scheme which applied consistency in the parity bit. Other schemes that applies VSS and consistency in secret image sharing have been published (Lin, 2015; Hidayat *et al.*, 2015).

funded by the Korean Government (MSIP) [No. 10041145, Self-Organized Software platform (SoSp) for Welfare Devices].

In this paper, to analyze the problem applied in secret image sharing by considering the problem stated by Tompa and Woll (1989), this experiment is conducted by manipulating the reconstruction's subset combination of collected data by consistency. The consistency experiment of secret image sharing based on Thien and Lin's (2002) scheme over $GF(2^8)$ is proposed. The reconstruction phase will be conducted as follows:

- there are m participants who collect the image shares;
- at least one adversary A in each subset; and
- each of those combinations is iterated according to the increments of threshold value t or total participants n.

This experiment is performed by two methods: single-secret sharing and multi-secret sharing. The reconstruction phase does not use a VSS scheme, as the image shares are the only information that participants have and not protected in the secret reconstruction. We attempt to know the relationship between threshold value t and total participants n by adding the adversary A. Also, we are eager to know in what point does the image start to distort, and the lower the image quality, the better for the dealer to analyze the reconstructed image. By applying the consistency analysis, it proved that consistency is necessary for every reconstruction. Also, consistency can help the dealer D to determine whether there are any adversaries and/or identify which participant is an adversary by simply analyzing the quality of the image. The quality of the image can be observed by both the security parameter and/or the visualization of the reconstructed image.

This paper consists of seven sections. Section 2 shows the related works, including Shamir's secret sharing and secret image sharing. Section 3 states the consistency problem in secret image sharing. Section 4 describes the consistency reconstruction for adversary detection and identification. Section 5 presents the experimental method, tests and results. Section 6 discusses the analysis of the proposed method in three aspects: test results, correlation analysis and visualization. Finally, Section 7 concludes this paper.

2. Related works

2.1 Shamir's secret sharing scheme

Given the secret message s to be shared among n participants, the dealer D generates the polynomial with degree $t-1$, where t is the minimum number of participants to reconstruct the secret. The distribution conducted uses a polynomial equation as shown below:

$$f(x) = s + a_1 x + \cdots + a_{t-1} x^{t-1} \bmod p \tag{1}$$

Where p is a prime number, coefficient $a_i \in Z_p$ and $i = \{1, 2, \ldots, n\}$ and x are participant's ID. The dealer calculates the shares and distributes them to n participants. For the reconstruction, m participants, where $t < m < n$, are required to collect their shares to the dealer, and the dealer can perform the calculation by using the Lagrange interpolation equation below:

$$f(x) = \sum_{j=1}^{n} y_j \prod_{\substack{k=1 \\ k \neq j}}^{n} \frac{x - x_k}{x_j - x_k} \pmod p \tag{2}$$

$$f(0) = s \tag{3}$$

Equation (2) is used for reconstructing the original polynomial, where y_j are the participant's share and x_j are the participant P_j's ID. Finally, the dealer adds the value $x = 0$ to the $f(x)$ as shown in equation (3).

2.2 Multi-secret sharing

The multi-secret sharing scheme is a modification of Shamir's (t,n) − threshold secret sharing. This scheme inserts all of the coefficients and constant as the secret messages. The possible number of secrets to be inserted can be up to t secrets in one session. This scheme can be said to be more effective and smaller than the original secret sharing:

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1}(mod\, p) \tag{4}$$

Different from the (t,n) − threshold secret sharing, all of the coefficients $a_i, i \in \{0, \ldots, t-1\}$ are treated as the secret messages. This scheme can reduce the file size when there are many secret messages to be shared. The reconstruction phase can be done by using the Lagrange interpolation. The step is to calculate the polynomial equation back to its original polynomial form and get all coefficients a_i which are the secret messages.

2.3 Thien and Lin's secret image sharing scheme

The secret image sharing scheme (Thien and Lin, 2002) was first proposed by using the image as the secret message. Here, the secret image S is the secret message to be shared among n participants by the dealer. In a grayscale image, the pixel value range $(0, \ldots, 255)$ is expressed in eight bits. The closest prime number to the 255 is 251 and 257. Because 257 is over 255, risking the overflow, they took 251 as the prime number p. In the preliminary stage, all pixels greater than 251 in the secret image are rounded to 251 to prevent the overflow. Next, the dealer D distributes the secret image S to n participant with threshold value t using the equation (4). Store up to t pixel in one polynomial, and reduce the image size to $1/t$. The reconstruction phase is conducted similarly by using Lagrange interpolation shown in equation (2). The reconstructed polynomial's coefficients present the secret pixels.

However, a drawback of this scheme is the loss pixel value above 251. Even though there are not many pixels above 251 in average, still it violates the original secret image. It is also possible to lower the quality of the reconstructed image. The authors recommend the other solution to store the value into two pixels. However, it requires more computation to detect each pixel which is above 251.

3. Consistency in secret image sharing

The term of consistency is crucial to detect the adversary among the participants. In the reconstruction phase, it is possible that more than t participants gather to reconstruct the secret. The reconstruction will be conducted successfully or not at all when there are exactly t participants present. However, when the number of participants increases to m, $t \leq m \leq n$, the last participants to collect their share can hold their share or present the share without being calculated by Dealer, as it is of no use if there are already t shares. The last participant or adversary A is not necessary to give a real share or a fake share. This problem is stated as consistency by Qassim (2013). The following two present the definition of consistency:

(1) Definition 1. t-*consistency*: A set of n shares is said to be t-consistent, if any subset of t shares reconstructs the same secret.

(2) Definition 2. *Strong t-consistency*: A set of n shares is said to be strong t-consistent if:

- any subset of t or more that t shares can reconstruct the same secret; and
- any subset of $t-1$ of fewer than $t-1$ shares cannot reconstruct the same secret.

By looking at Definition 1, we can conclude that the traditional secret sharing scheme already had this component. The proofs of consistency in Shamir's secret sharing has been stated by Beimel (2011). The scheme already satisfied correctness and privacy. Correctness means that it assures that a pool of t participants can reconstruct the secret by using equation (2), and privacy implies no up to $t-1$ participants can reconstruct the secret. Meanwhile, the correctness also can assure the consistency, where $Pr[s|T] = 1$.

The reconstruction phase in traditional secret sharing uses the Lagrange interpolation which assures that exactly t shares can reconstruct the same secret. However, the reconstruction phase cannot assure the strong t-consistency when there are t or more shares collected as referred in Definition 2. The participants outside of t subset out of m may get the secret message without giving their shares. The classic method to prevent such an action is to put a VSS scheme to verify whether the shareholder presents the true share or not by using additional values and calculations. Nevertheless, without using the VSS scheme, this experiment tries to see the impact in the quality of reconstructed image when there are m participants and several adversaries A. This experiment conducts both the secret sharing and multi-secret sharing. In Thien and Lin's (2002) scheme, there are many numbers of pixel present in one image, every pixel of shared image is presented as t secret pixels in the original secret image.

In this paper, we present our experiment in consistency using the results that were collected from all of the cases when there are m numbers of image shares. The shares are combined by referring to the subset and calculating the outcome of the combination of pixel subset for every m share with several adversaries A among the m participants. Therefore, the impact from those combinations to the reconstructed image can be seen. After the reconstruction phase, the reconstructed secret images will be calculated by the experiment quality test between the pixels in the reconstructed image and the original secret image S. Also, to prevent of image loss when the pixel value is above 251, we compute all of the calculation in $GF(2^8)$.

4. Consistency reconstruction for adversary detection and identification

This paper focused on the reconstruction phase to observe the quality impact of the reconstructed image when there are adversaries among the participants. This section describing the detection algorithm and identification algorithm is shown as follows.

4.1 Adversary detection

The adversary detection algorithm:

Step 1: Given the set M of m participants *ID*, find a subset T from each participant's ID consisting of t elements, where $T \subseteq M$.

Step 2: Determine all the possible subsets T by using the binomial coefficient formula which is defined in the following equation:

$$C(m, t) = \frac{m!}{t!\,(m - t)!} \tag{5}$$

Step 3: Collect all the m share images by putting the adversary $A_j, j \in \{1, \ldots, t-1\}$ among the shares and start the reconstruction phase by following the steps below:

- get all the pixels in the t share images, referencing the participant *ID* which is present in the subset T_r;
- reconstruct the collected pixel from the shares by using the Lagrange Interpolation; and
- repeat the steps progressively by referencing the subset T_r.

Step 4: After all of the subsets in T_r have been computed, repeat the subset elements until all the pixels have been calculated and get the secret image S.

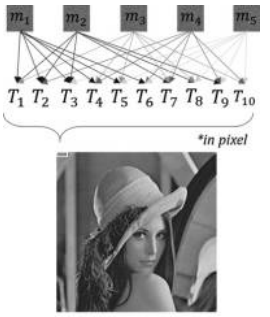
By following these steps, the secret image can be calculated by combining the pixel results from each combination. The example presentation of the experiment is shown in Figure 1. The figure displays the example experiment when (3, 8) − threshold with fixed $n = 8$ and collected share $m = 5$. These experiments use the given controlled variable t and n for each method. Also, in addition, all of the operations are conducted by modulo operation over the $GF(2^8)$, which can calculate the pixel number between 0 and 255. The $GF(2^8)$ can be described by using the irreducible polynomial denote as follows:

$$x\text{^}8 + x\text{^}4 + x\text{^}3 + x + 1 \tag{6}$$

Both the traditional single-secret and multi-secret sharing schemes are represented by applying the consistency scheme above, which computes over $GF(2^8)$ to prevent the loss of pixel value above 251.

4.2 Adversary identification

The identification phase is conducted when the dealer detects an adversary in the reconstruction phase. By simply looking at the quality of the image, presence of an adversary can be determined by the distorted reconstructed image. If the adversary is among the participants pool, then the distorted pixel which does not reconstruct properly will form a pattern of pixels. The identification phase is described below:



Source: http://sipi.usc.edu/database/database.php

Figure 1.
The detection phase conducted in (3,8)-threshold single secret sharing

Step 1: Determine all the possible subsets T from m participant's ID by using the binomial coefficient formula which is defined in equation (5) and index each member of subset T with the r element.
Step 2: Generate an array Y with r elements as a counter.
Step 3: Compare each pixel in the original secret image S and the reconstructed secret image R. Put each comparison result in array Y by the following rule:

$$Y_r(S,R) = \begin{cases} 1 & S_{i_r} \neq R_{i_r} \\ 0 & S_{i_r} = R_{i_r} \end{cases} \tag{7}$$

Step 4: Observe each element with value 1 in array Y and pool the element in the subset T with the same index with array Y.
Step 5: Find the intersection from T_r which determines the adversary's ID:

$$A = \bigcap_{\substack{i \in Y_r \\ Y_r = 1}} T_i \tag{8}$$

Step 6: The dealer halts the procedure.

The procedure above can be repeatedly conducted until all the pixels have been calculated. However, as it forms an identical pattern, it is unnecessary to do all the procedures repetitively. The identification phase is recommended to conduct with the condition $H \times W/2$ pixels to obtain a precise result.

5. Experimental test and results

In this section, the consistency performance for each experiment is shown in the graphs and figures below.

These experiments were conducted using C++ and Library openCV in Windows 7 environment. Figure 2 shows one set consists of three images (Baboon, Lena and Pepper). One set of seven randomly generated adversary images with a size of 256 × 256, where the three image is used as the shared image and other seven adversary

(a) (b) (c)

Notes: (a) Baboon; (b) Lena; (c) Pepper
Source: http://sipi.usc.edu/database/database.php

Figure 2.
Test Image

images which are generated by using a noise proportionally distributed random function $\mathcal{F}$.

There are three variables which applied in this experiment:

(1) The number of adversaries A, where $0 < A < n$;

(2) The total shares n, where $2 \leq n \leq 8$; and

(3) The threshold number of share t, where $2 \leq n \leq 8$.

The experiment collects all the possible reconstruction combinations of subset M within set N, where the elements of each participant are in the range of $t \leq m \leq n$. By gaining the set M, the subset T among those elements of M has to be calculated to put all the possibilities in pixels combination as shown in Section 4. In the reconstruction phase, all the pixels from the shares in the subset T are being calculated. The output of reconstructed images is compared with the original secret image to estimate the image quality. In this experiment, we apply peak signal-to-noise ratio (PSNR), inverse number of pixel change rate (NPCR) and unified averaged changed intensity (UACI) to give better enhancement to our experiments. The method being used in this paper will be described in the following sub-section.

5.1 Experimental test

This section describes the test method to observe the damage in the reconstructed secret image and comparing it with the original secret image. By using the results, we can analyze the relationship between the given variables and the impact made on the image. In the experimental process, we apply three tests: PSNR, inverse NPCR and UACI. Further information regarding the NPCR and UACI can be found in Wu *et al.*'s (2011) study. However, in this paper, it is stated that the NPCR value may vary depending on the image size and the image format. Therefore, in this test, we give the detail of our test image to give precise results in the previous explanation. Also to provide more detail about the impact of our proposed scheme on analysis, we added the correlational analysis test with random samples among the reconstructed images.

5.1.1 Peak signal-to-noise ratio. PSNR is one of the most frequent measurements to observe the quality of either a compressed image or an encrypted image. The computation of PSNR is shown as follows:

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right)dB \tag{9}$$

While, the mean square error with image dimension of $H \times W$ is defined as follows:

$$MSE = \frac{1}{H \times W}\sum_{c=1}^{H}\sum_{r=1}^{W}(p_{cr} - p'_{cr})^2 \tag{10}$$

5.1.2 Inverse number of pixel change rate. To calculate the pixel change rate, NPCR between the reconstructed image and the original secret image is commonly used. However, to ease the visualization of the graph, in this paper, we calculate the image similarity or inverse NPCR as stated below:

$$NPCR^{-1}(S,R) = \frac{\Sigma_{ij} G(i,g)}{H \times W} \times 100\% \tag{11}$$

Where H and W are the width and height of the given reconstructed image, respectively. The value of G is determined as follows:

$$G(i,j) = \begin{cases} 1 & S(i,j) = R(i,j) \\ 0 & S(i,j) \neq R(i,j) \end{cases} \tag{12}$$

While the original NPCR is stated as below:

$$G(i,j) = \begin{cases} 0 & S(i,j) = R(i,j) \\ 1 & S(i,j) \neq R(i,j) \end{cases} \tag{13}$$

As the output, it calculates the average of all inverse NPCR values from all the subset M out of set N reconstruction result in each case; thus, we can see the relationship between the number of adversaries with the combination of threshold value t and the number of all participants n.

5.1.3 Unified averaged changed intensity. UACI is one of the methods to test the randomness of image encryption. Here, it observes the change value between paired images. In this experiment, it will show the difference changed between the reconstructed image and the original secret image. UACI calculation is quite straightforward, which is shown as follows.

$$\sum_{ij} \frac{|S(i,j) - R(i,j)|}{255 \times H \times W} \times 100\% \tag{14}$$

5.1.4 Correlation analysis. The correlation analysis is a method to measure the association between two variables (Anon, 2009). Here, we try to estimate a sample correlation coefficient of pixels in the original secret image and the reconstructed images. The correlation coefficient $\rho_{X,Y}$ varies between $1 \leq \rho_{X,Y} \leq 1$, which indicates the direction and strength of the linear association. The sign indicates the direction of the slope; meanwhile, the coefficient number indicates the strength between the associations. The correlation strength becomes stronger if the correlation coefficient is closer to -1 or $+1$ and vice versa. The correlation analysis computations are shown in the following equations:

$$\bar{X} = \frac{1}{N}\sum_{i=1}^{N} X_i, \quad \bar{Y} = \frac{1}{N}\sum_{i=1}^{N} Y_i \tag{15}$$

$$\sigma_X^2 = \frac{1}{N}\sum_{i=1}^{N} (X_i - \bar{X}), \sigma_Y^2 = \frac{1}{N}\sum_{i=1}^{Y} (Y_i - \bar{Y}) \tag{16}$$

$$cov(X,Y) = \frac{\sum_{i=1}^{N} (X_i - \bar{X})(Y_i - \bar{Y})}{N-1} \tag{17}$$

$$\rho_{X,Y} = \frac{cov(X, Y)}{\sigma_X \times \sigma_Y} \tag{18}$$

Where X_i and Y_i are presenting the pixel values of the secret and share images. $\bar{X}$ represents the mean value of the secret image and $\bar{Y}$ represents the mean value of the share image. *cov*(*x*,*y*) is the covariance between the secret image and the share image. The strength of relationship is considered weak when it reached below +0.30 or above −0.30; meanwhile, it can be considered moderate when it is below +0.50 or above −0.50. When the sample correlation coefficient is below +0.10 or above −0.10 closer to zero, it is considered as none.

5.2 Experimental results

Each test image in the experimental results produces 12 graphs (with a total of 36 graphs) which are divided into four groups: single secret (fixed $t = 2$ and fixed $n = 8$) and multi-secret (fixed $t = 2$ and fixed $n = 8$). Each group consists of three graphs: By PSNR, NPCR and UACI. Figures 3 and 4 show the experimental results from the application of single secret sharing: with given fixed $t = 2$ and fixed $n = 8$. Figures 5 and 6 show the experimental results from the application of multi-secret sharing: with given fixed $t = 2$ and fixed $n = 8$. Meanwhile, each subfigure consists of three graphs which show the image quality result by using PSNR, inverse NPCR and UACI. Three image test methods in the experimental result are conducted with the aim of analyzing the consistency reconstruction in different images.

The value of PSNR and inverse NPCR will be decreased proportionally to the increased number of adversaries among the participants pool, as both of the methods focused on the ratio of the pixels between the reconstructed image and the secret image. Meanwhile, UACI can be observed to increase proportionally to the number of the adversaries. The UACI method uses the number of absolute difference, which makes the value higher when the range of range is getting bigger. An image is considered to have good quality when the PSNR value is more than 30 dB. The inverse NPCR (which is stated in this paper) value is considered as safe when it stated above 50 per cent.

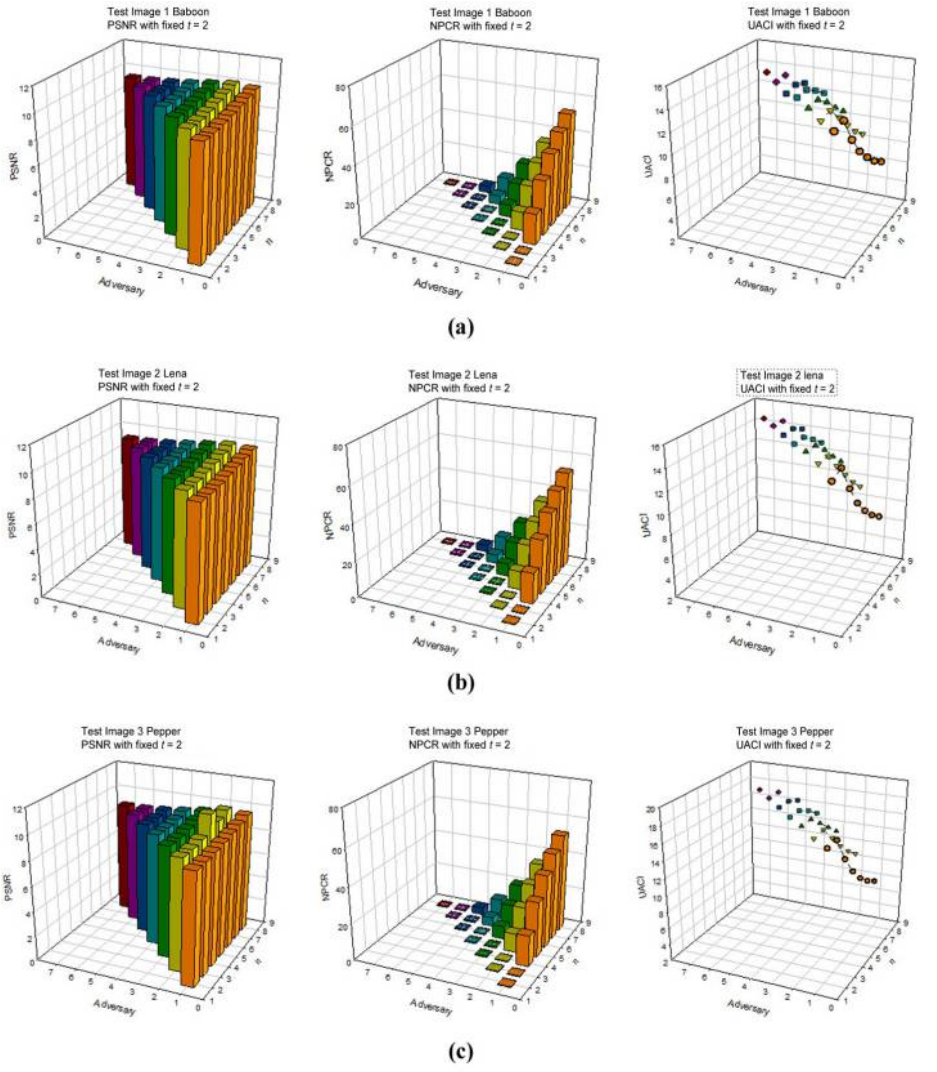
6. Analysis

Based on Shamir's secret sharing method, it is obvious that exact t shares have to be collected in terms of reconstruction by using the Lagrange interpolation method. However, the problem arises when there are m participants, where $t \leq m \leq n$. There is a possibility that the adversary A can get the secret without giving its share, or the adversary does not include in the threshold combination. To observe the impact of image quality and its influence on the method and threshold relationship in the experimental result, the analyses will be given in three subsections: test result, correlation analysis and visualization.

6.1 Test results

6.1.1 Test image. By observing Figures 3-6, there are almost no significant differences among the image tests. Therefore, this experiment is valid without relation to the kind of image it uses.

6.1.2 Method. The result for single-secret (Figures 1 and 2) and multi-secret (Figures 3 and 4) shows the results by the given controlled variable n and variable t. Based on all figures, it is hard for the reader to observe the difference in PSNR, NPCR or UACI.



Notes: (a) Baboon; (b) Lena; (c) Pepper

Figure 3.
Single secret with fixed $t = 2$

However, as the multi-secret sharing scheme contains a lot of pixels in one polynomial [see equation (4)], the results are slightly lower than those of the single-secret sharing scheme but not significant. Thus, we can omit the difference between the methods which has no significant impact to the image quality. Instead, we will focus on the impact of the controlled variable t and variable t in the next paragraph.

6.1.3 (t,n) – threshold relationships. Without considering the methods used in the reconstruction phase, we will observe the impact of variables on the image quality. We assume that the lower the image quality gets, the easier it is for the dealer D to

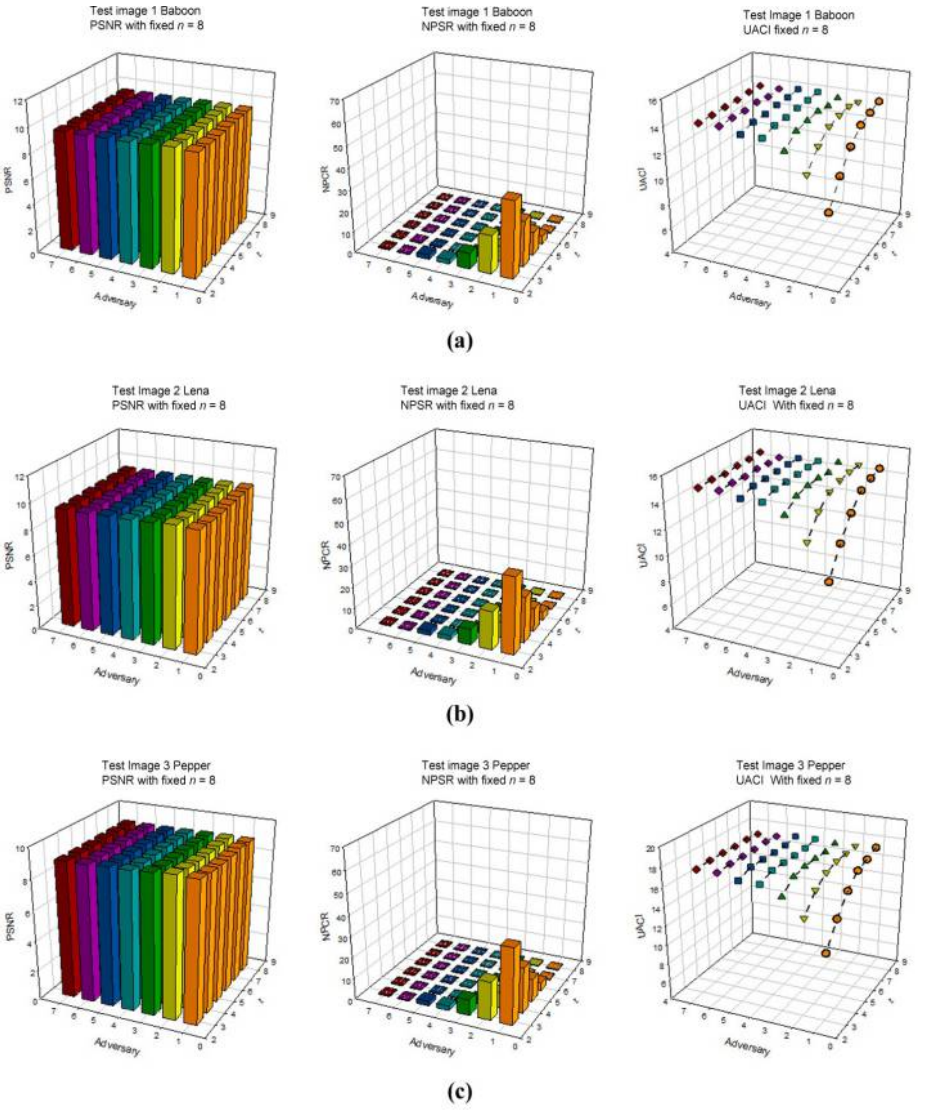
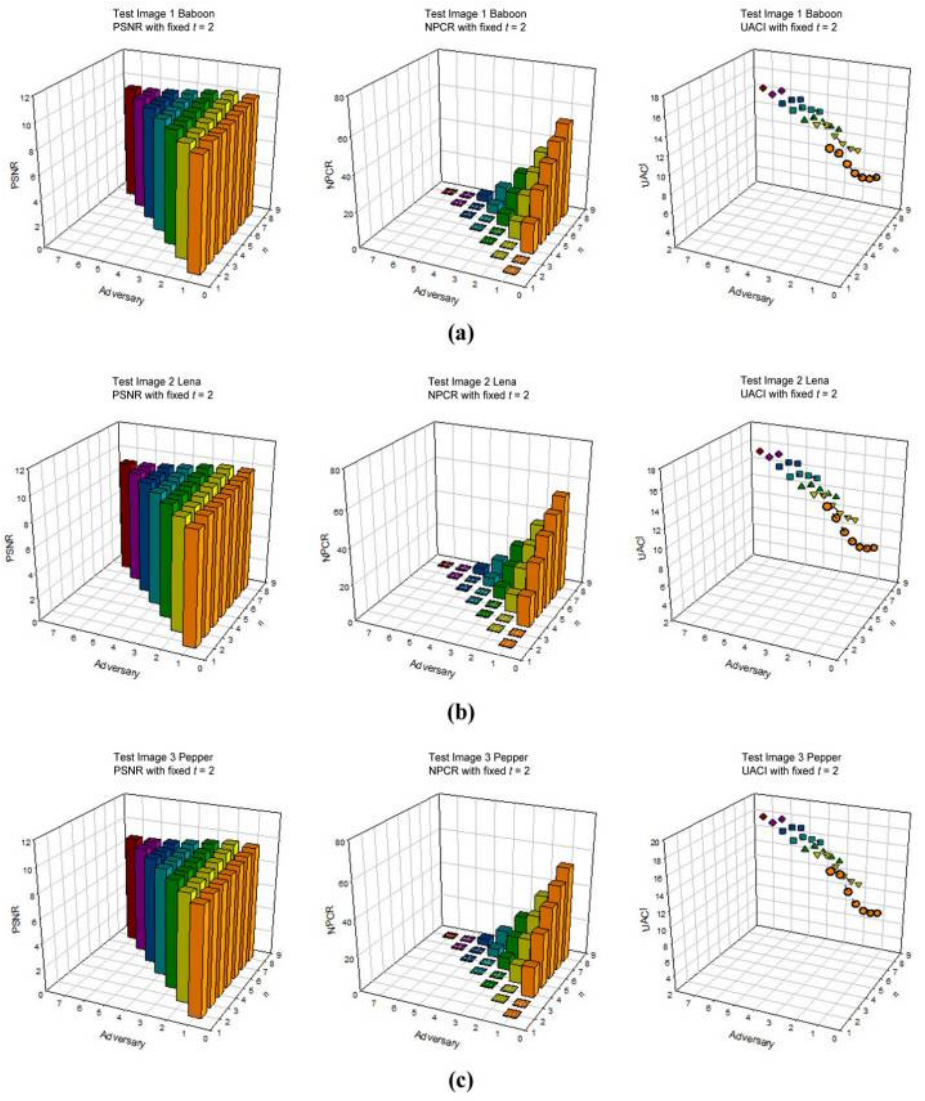


Figure 4.
Single secret with fixed $n = 8$

Notes: (a) Baboon; (b) Lena; (c) Pepper

determine that there are dishonest participants either outside adversaries inside the reconstruction pool. For better observation on the experimental results, we will focus on the results in the Figures 3 and 4.

6.1.4 Experimental results test. The PSNR value in both Figures 3 and 4 is slightly decreased when adversary A is more. When the value of fixed $t = 2$ for both single-secret and multi-secret are conducted, the PSNR value remains stable between 9 and 9.5 dB.



Notes: (a) Baboon; (b) Lena; (c) Pepper

Figure 5.
Multi-secret with fixed $t = 2$

Meanwhile, the PSNR value is gradually decreased when the fixed $n = 8$ condition is being given, started when $A > 3$. It will be decreased by 0.1 dB when the number of adversaries is increased by 1. Nevertheless, the PSNR value is still lower than 10 dB which has a distorted poor-quality output. PSNR may give a great perspective to evaluate the image quality in this experiment; however, the range of PSNR is small that cannot be easily determined by the observer.

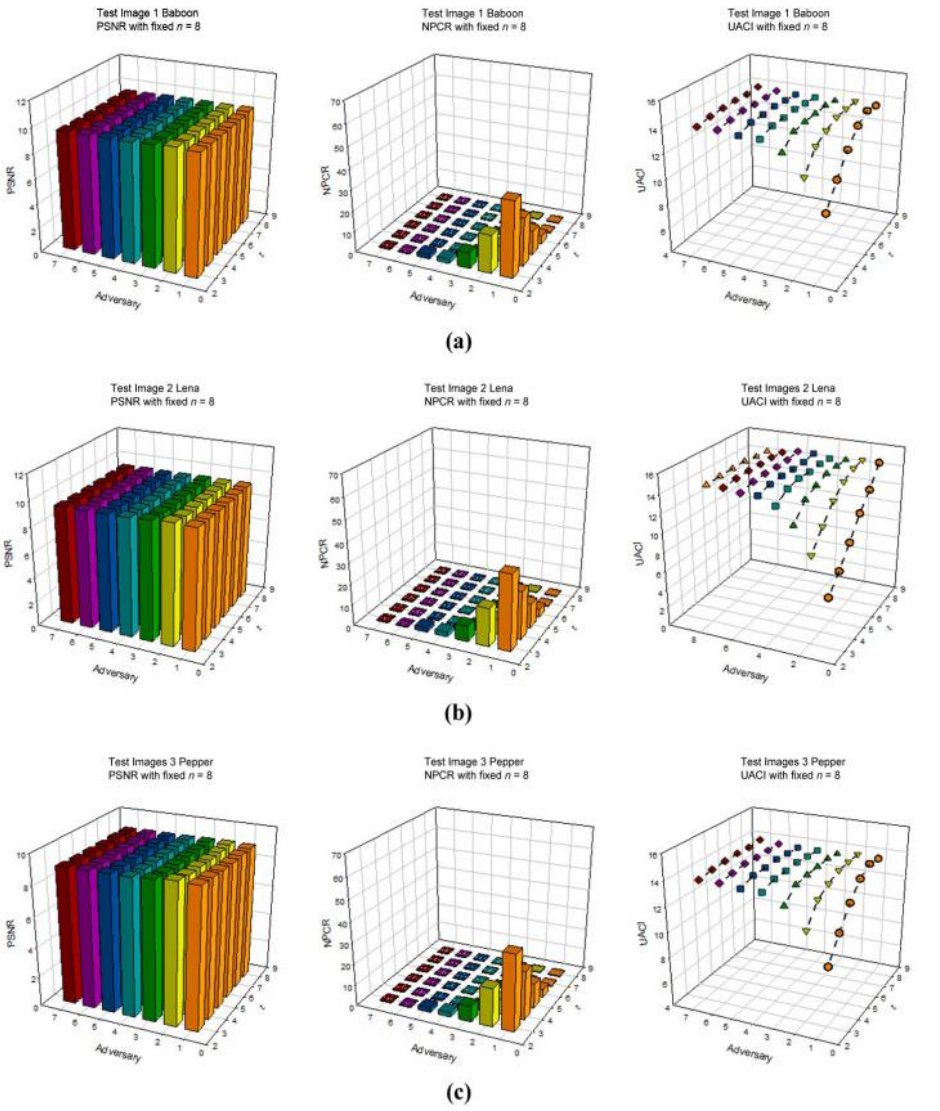


Figure 6.
Multi-secret with fixed $n = 8$

Notes: (a) Baboon; (b) Lena; (c) Pepper

On the other hand, the NPCR graph value gives a contrast result between fixed variables $n = 8$ and $t = 2$ results. The NPCR value goes up when the given fixed $t = 2$ and the number of total participants n increased proportionally as seen in the Figure 3, as there are more subsets $T \in N$. A lower threshold value t can also result in better quality images when there more participants present their shares. However, when it comes to

the fixed $n = 8$, the NPCR value is decreased, as the number of threshold value t showed an inversely proportional increase as shown in the Figure 4.

The UACI value in both Figures 3 and 4 is inversely proportional to the inverse NPCR value. We can also conclude that the UACI is proportional to NPCR. In case of fixed $t = 2$, the UACI value drops significantly when it reaches $n = 3$ which means that the intensity of changed pixel dropped, and the image becomes more identical to each other. From this point of view, the dealer D can determine the number of adversaries A which are included in the pool.

6.2 Correlation analysis

The correlation analysis uses the target between the Lena image as the source original secret image and the reconstructed images from samples provided from the experiment. We adjust the local region size or pixel number, which is three. The correlation analysis results are shown in Tables I and II, which represent the results of both single-secret sharing and multi-secret sharing, respectively. In both Tables I and II, single-secret sharing and multi-secret sharing showed a similar outcome. The correlation coefficient is considered as no relation between two images as it is closer to zero when the threshold value is (2, 8) with three adversaries present during the reconstruction. It can also recognize as an entirely

Adversary	m	(2, 8)	(3, 8)	(4, 8)	(5, 8)
1	2	−0.01			
	3	0.56	0.00		
	4	0.77	0.42	0.02	
	5	0.84	0.67	0.38	0.00
	6	0.80	0.73	0.47	0.31
	7	0.88	0.82	0.68	0.49
	8	0.89	0.85	0.76	0.61
2	2	0.00			
	3	−0.01	0.18		
	4	0.29	0.04	−0.01	
	5	0.53	0.20	−0.01	0.00
	6	0.55	0.37	0.09	0.01
	7	0.69	0.51	0.27	0.08
	8	0.73	0.60	0.38	0.19
3	3	−0.02	0.01		
	4	−0.07	0.01	0.00	
	5	0.18	−0.01	0.00	0.01
	6	0.31	0.08	0.02	0.00
	7	0.47	0.21	0.08	0.01
	8	0.55	0.30	0.15	0.03
4	4	−0.04	0.01	−0.01	
	5	−0.02	−0.02	0.00	0.01
	6	0.09	−0.01	0.01	−0.01
	7	0.25	0.06	0.02	0.02
	8	0.35	0.12	0.03	0.00
5	5	−0.01	0.01	0.00	0.00
	6	−0.01	0.01	0.02	−0.01
	7	0.09	0.03	0.01	0.01
	8	0.18	0.05	−0.01	−0.01

Table I. Single-SS correlation analysis results

Adversary	m	(2, 8)	(3, 8)	(4, 8)	(5, 8)
1	2	−0.01			
	3	0.60	−0.03		
	4	0.78	0.42	0.01	
	5	0.82	0.62	0.36	0.36
	6	0.86	0.75	0.62	0.37
	7	0.84	0.81	0.67	0.52
	8	0.91	0.83	0.67	0.54
2	2	−0.01			
	3	0.08	−0.01		
	4	0.34	0.00	−0.01	
	5	0.52	0.17	0.01	0.00
	6	0.66	0.35	0.18	0.02
	7	0.65	0.47	0.29	0.14
	8	0.80	0.56	0.37	0.20
3	3	0.02	−0.01		
	4	0.01	0.00	0.00	
	5	0.19	0.00	0.00	0.00
	6	0.35	0.08	0.00	0.01
	7	0.45	0.19	0.05	0.05
	8	0.60	0.30	0.05	0.04
4	4	0.01	−0.02	0.00	
	5	0.02	−0.01	0.01	−0.01
	6	0.13	0.00	0.01	0.00
	7	0.26	0.04	0.00	0.00
	8	0.38	0.12	0.02	0.01
5	5	0.00	0.00	0.02	−0.01
	6	0.01	0.03	0.01	0.01
	7	0.09	0.02	0.00	−0.01
	8	0.20	0.03	0.00	0.01

Table II.
Multi-SS correlation analysis results

different image. The secret image sharing system which expect adversary $A \geq 3$ in the same reconstruction phase, the $(2, 8)$ − threshold secret sharing or above for both singles and multi-secret is recommendable, regardless of the number of m participants. When the adversary A is expected to be below three, the $(4, 8)$ − threshold or above is considered safe when $m \leq 6$ for single-secret and $m \leq 5$ for multi-secret. As the higher the m participants, the higher is possibility that the image can be slightly revealed. However, without considering the lowest safe point, it is recommendable to apply $(4, 8)$ − threshold for single-secret and $(5, 8)$ − threshold for multi-secret. Because the secret image is not completely revealed and hard to distinguish when any number of adversary collided in the reconstruction phase. The summary of the threshold point is shown in Table III.

6.3 Visualization

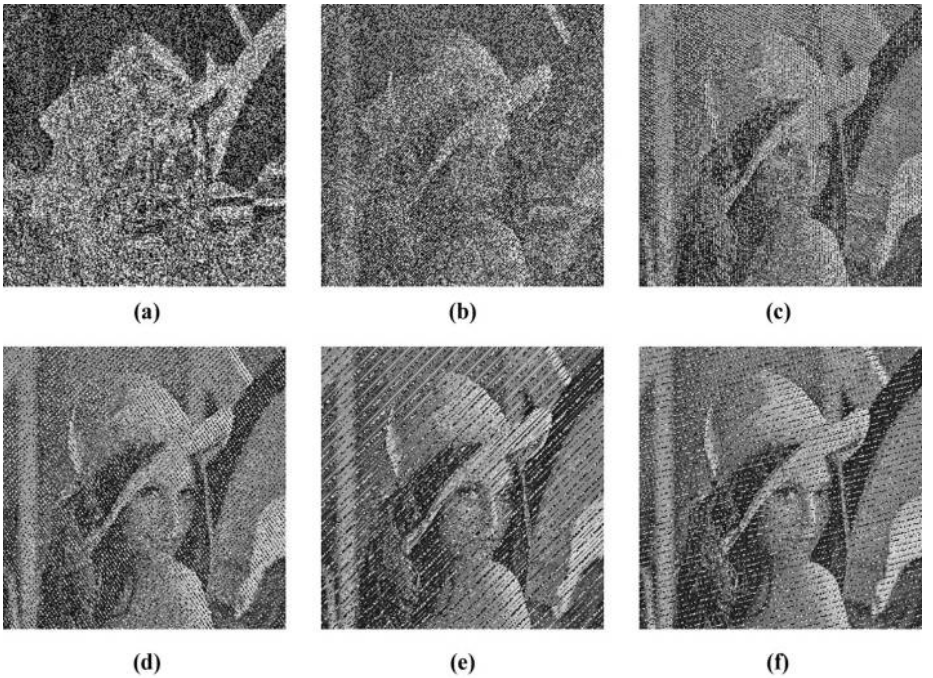
Despite the experimental results and the correlation analysis, both dealer and the participants still can visually distinguish the images whether it has been attacked. According to the number of m participants and the threshold t, the reconstructed images have a visual difference according to the method that the system uses. For a simple

demonstration, we took the $(2, 8)-$ threshold reconstructed images from both single-secret and multi-secret with one adversary among the participants, as shown in Figures 7 and 8.

In Figure 7, the reconstructed images with $2 \leq m \leq 7$ are shown in an ascending order. The reconstructed image is hardly recognized when $m = 3$ or below. Meanwhile, when $m > 3$, the secret image Lena is slightly revealed even not in the high quality. The adversary may know or guess the content visually in this stage. Thus, it can be concluded that it is safe to do the reconstruction when $m \leq 2t - 1$. When $m \geq 2t$, the dealer D or participants can recognize the original secret image even though the image is slightly distorted. The multi-secret reconstruction results are shown in Figure 6. It shows that the reconstructed image quality is slightly lower than the single-secret reconstructed images, due to the increased number of stored pixel in one polynomial. The image is difficult to recognize when $m = 4$ or below. When the $m > 4$, the Lena image can be recognized easily. Thus, the reconstruction with $m \leq 2t$ is considerably safe in multi-secret sharing. Without any restraint to which secret sharing method has been used, we recommend to reconstruct the share images when $m \leq 2t - 1$, considering the visual quality of output images.

Table III. Recommended (t,n)-threshold

	Single-secret	Multi-secret
Safe point **when** $\boldsymbol{A} < 3$	$t = 4, m \leq 5$	$t = 4, m \leq 6$
Recommended point $\forall \boldsymbol{A}$	$t = 4, \forall m$	$t = 5, \forall m$



Notes: (a) m = 2; (b) m = 3; (c) m = 4; (d) m = 5; (e) m = 6; (f) m = 7

Figure 7. (2,8) Single-SS reconstruction image results

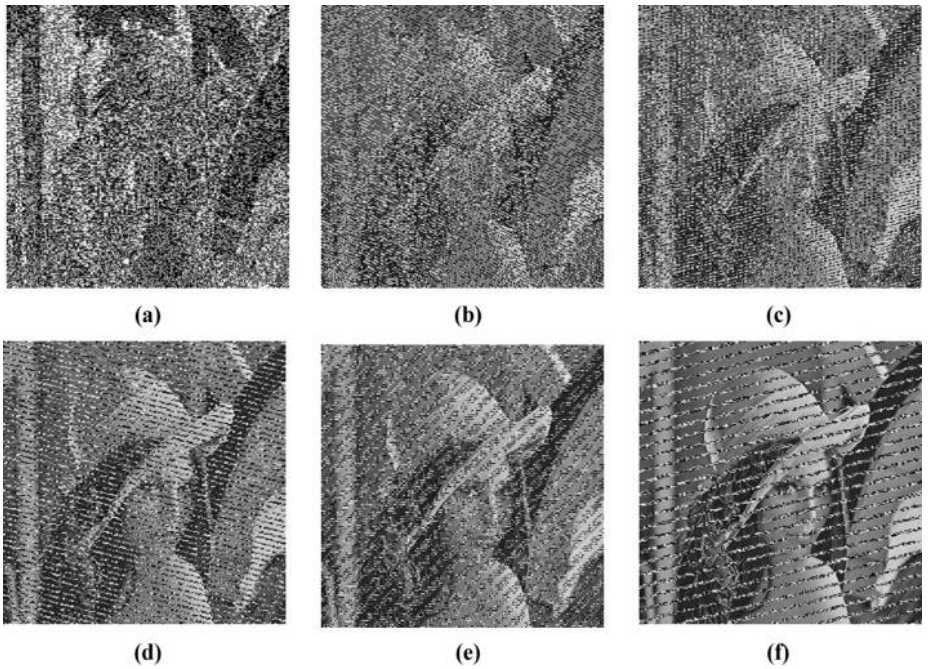


Figure 8.
(2,8) Multi-SS reconstruction image results

Notes: (a) m = 2; (b) m = 3; (c) m = 4; (d) m = 5; (e) m = 6; (f) m = 7

The demonstration shown above is simply applied with (2, 8) − threshold and only one adversary among m participants. However, when the threshold value of either of the adversaries increases, the difficulty to recognize the image also increases for dealer or participant. Thus, the reconstruction phase which is presented in this paper is safe for the given condition above, and it also gives a clearer difference between Shamir's method in secret image sharing and Thien and Lin's secret image sharing.

In general, it is obvious that all of the figures given show similar results to the number of adversary A. The gradual decrease shows that the number of adversaries A can also be determined by looking at the quality of the images. Previously, considered by the Tian *et al.*'s (2013) scheme, the consistency is the variable assistance of fairness. Through this experiment, it is shown that without the utility of fairness, it is sufficient to determine the adversary A by consistency. The combination of pixels in the given set make it possible for the adversary to be discovered when interrupted among the m participants. Because the value of PSNR remains the same without respect to the threshold relationship, the dealer D can reconstruct the image and compare the inverse NPCR and UACI value of both images. Moreover, the dealer D also can visually see the result and determine not to broadcast the secret image. This system assumes that the dealer D is honest.

7. Conclusion

The present paper proposes an in-depth analysis of strong t-consistency in secret image sharing. Two algorithms, detection and identification, can be used as in combination to help

the dealer D in the reconstruction phase. The experiment on detection was conducted by using the difference approach to the number of secret pixels in the polynomial. Single- and multi-secret methods were used in the polynomial equation. The experiment is applied in an image as a media and conducted when there are m participants, and where $t \leq m \leq n$ in one reconstruction session. All of these experiments were computed over $GF(2^8)$ to prevent the pixel value loss. The results show a linear gradual decrease for each adjustment of variable t and n when the number of adversary A is also increasing. Through the experimental results, the method of polynomial did not influence the quality of image; however, the value of t has more impact to the visual quality of the reconstructed image. Here, we gave a recommended threshold value $(4, n)$ for single-secret and $(5,n)$ for multi-secret, where the n values can be a variant for a safe reconstruction. Also the minimum m value, $m \leq 2t - 1$ when the $(2, 8) -$ threshold is applied to the reconstruction phase to easily detect the adversary.

References

Anon. (2009), "Explorable.com: statistical correlation", available at: https://explorable.com/statistical-correlation (accessed 10 August 2015).

Asmuth, C. and Bloom, J. (1983), "A modular approach to key safeguarding", *IEEE Transactions on Information Theory*, Vol. 29 No. 2, pp. 208-210.

Beimel, A. (2011), "Secret-sharing schemes: a survey", *Coding and Cryptology*, Springer, pp. 11-46.

Blakley, G.R. (1979), "Safeguarding cryptographic keys", in *Proceeding of the National Computer Conference*, *Texas A&M University College Station*, *Texas*, pp. 313-317.

Chao, K.-Y. and Lin, J.-C. (2009), "Secret image sharing: a Boolean-operations-based approach combining benefits of polynomial-based and fast approaches", *International Journal of Pattern Recognition and Artificial Intelligence*, Vol. 23 No. 2, pp. 263-285.

Chen, C.-C. and Wu, W.-J. (2014), "A secure Boolean-based multi-secret image sharing scheme", *Journal of Systems and Software*, Vol. 92, pp. 107-114.

Chen, Z., Li, S., Zhu, Y., Yan, J. and Xu, X. (2015), "A cheater identifiable multi-secret sharing scheme based on the Chinese remainder theorem", *Security and Communication Networks*, Vol. 8 No. 18, pp. 3592-3601.

Dong, X. (2015), "A multi-secret sharing scheme based on the CRT and RSA", *International Journal of Network Security*, Vol. 2 No. 2, pp. 69-72.

Fuyou, M., Yan, X., Xingfu, W. and Badawy, M. (2015), "Randomized component and its application to (t,m,n)-group oriented secret sharing", *IEEE Transactions on Information Forensics and Security*, Vol. 10 No. 5, pp. 889-899.

Harn, L. (2014), "Secure secret reconstruction and multi-secret sharing schemes with unconditional security", *Security and Communication Networks*, Vol. 7 No. 3, pp. 567-573.

Harn, L., Fuyou, M. and Chang, C.-C. (2014), "Verifiable secret sharing based on the Chinese remainder theorem", *Security and Communication Networks*, Vol. 7 No. 6, pp. 950-957.

Harn, L. and Lin, C. (2009), "Detection and identification of cheaters in (t, n) secret sharing scheme", *Designs, Codes and Cryptography*, Vol. 52 No. 1, pp. 15-24.

Harn, L. and Lin, C. (2010), "Strong (n, t, n) verifiable secret sharing scheme", *Information Sciences*, Vol. 180 No. 16, pp. 3059-3064.

Hidayat, A.S., Lee, G.-J., Yoon, E.-J. and Yoo, K.-Y. (2015), "Consistency analysis for secure reconstruction in secret image sharing", *Proceeding of the International Conference on Advances in Mobile Computing and Multimedia*, *Belgium*, pp. 357-364.

Lin, C.-C. and Tsai, W.-H. (2004), "Secret image sharing with steganography and authentication", *Journal of Systems and Software*, Vol. 73 No. 3, pp. 405-414.

Lin, P.-Y. (2015), "Double verification secret sharing mechanism based on adaptive pixel pair matching", *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, Vol. 11 No. 3, p. 36.

Liu, Y., Harn, L. and Chang, C.-C. (2015), "A novel verifiable secret sharing mechanism using theory of numbers and a method for sharing secrets", *International Journal of Communication Systems*, Vol. 28 No. 7, pp. 1282-1292.

Mignotte, M. (1983), "How to share a secret", In *Cryptography*, Springer Berlin Heidelberg, pp. 371-375.

Qassim, A.M. (2013), "Polynomial differential-based strong (n, t, n)-verifiable secret sharing", *IER Information Security*, Vol. 7 No. 4, pp. 312-317.

Shamir, A. (1979), "How to share a secret", *Communications of the ACM*, Vol. 22 No. 11, pp. 612-613.

Tadayon, M.H., Khanmohammadi, H. and Sayad Haghighi, M. (2014), "Dynamic and verifiable multi-secret sharing scheme based on Hermite interpolation and bilinear maps", *Information Security, IET*, Vol. 9 No. 4, pp. 234-239.

Thien, C.-C. and Lin, J.-C. (2002), "Secret image sharing", *Computers & Graphics*, Vol. 26 No. 5, pp. 765-770.

Tian, Y., Ma, J., Peng, C. and Jiang, Q. (2013), "Fair (t,n) threshold secret sharing scheme", *Information Security, IET*, Vol. 7 No. 2, pp. 106-112.

Tompa, M. and Woll, H. (1989), "How to share a secret with cheaters", *Journal of Cryptology*, Vol. 1 No. 3, pp. 133-138.

Wu, Y., Noonan, J.P. and Again, S. (2011), "NPCR and UACI randomness tests for image encryption", *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, pp. 31-38.

Yang, C.-N., Chen, C.-H. and Cai, S.-R. (2015), "Enhanced Boolean-based multi secret image sharing scheme", *Journal of Systems and Software*, pp. 1-13, available at: www.sciencedirect.com/science/article/pii/S0164121215000205

About the authors

Anneke Soraya Hidayat is a MS Candidate at the School of Computer Science and Engineering at Kyungpook National University. She received BS in Computer Engineering from Kyungsung University in 2014. Her research interests are in the areas of cryptography and secret sharing.

Gil-Je Lee is currently a PhD Candidate at the School of Computer Science and Engineering at Kyungpook National University. He received BS degree from Kyungil University in 2007 and MS degree from Kyungpook National University in 2010. His current research interests are steganography, digital watermarking, secret image sharing, quantum secret sharing and cloud computing security.

Eun-Jun Yoon is currently an Associate Professor in the Department of cyber security at Kyungil University. He received MSc in computer engineering from Kyungil University in 2002 and PhD in computer science from Kyungpook National University in 2006, South Korea. From 2007 to 2008, he was a full-time lecturer at the Faculty of Computer Information, Daegu Polytechnic College, South Korea. His current research interests are cryptography, authentication technologies smart card security, network security, mobile communications security and steganography.

Kee-Young Yoo is currently a Professor at the School of Computer Science and Engineering at Kyungpook National University. He received BS from Kyungpook National University in 1976, MS from Korea Advanced Institute of Science and Technology in 1978 and PhD from Rensselaer Polytechnic Institute, New York, USA, in 1992. His current research interests are cryptography and information hiding. Kee-Young Yoo is the corresponding author and can be contacted at: yook@knu.ac.kr