Weighted modulated secret image sharing method

Chien-Chang Chen
Hsuan Chuang University
Department of Information Management
Hsinchu 300, Taiwan
E-mail: cchen34@hcu.edu.tw

Chaur-Chin Chen
National Tsing Hua University
Department of Computer Science
Hsinchu 300, Taiwan

Yun-Cheng Lin
Hsuan Chuang University
Department of Information Management
Hsinchu 300, Taiwan

Abstract. *We present a novel hybrid method that includes a modulated scheme for reducing the distortion of the reconstructed image and a two-layered structure for grouping participants with different weights in a secret image sharing problem. Conventional secret image sharing methods suffer from truncation distortion, which is the difference between a pixel value and its truncated result. We first present a histogram modulation scheme to modulate the truncated pixels to prevent the truncation distortion. A two-layer secret image sharing scheme groups the participants in the first layer and weights them differently in the second layer. The proposed modulated secret image sharing method merges these two schemes. Experimental results reveal that the proposed method efficiently reduces the truncation distortion and groups the participants with different possessing weights.* © *2009 SPIE and IS&T.* [DOI: 10.1117/1.3268362]

1 Introduction

Secret image sharing is essential for protecting digital images. Conventional secret image sharing methods share one secret image to participants, and enough shared images recover the secret image. These approaches can be divided into two categories—namely, *piling up* and *mathematical calculation*. Piling-up methods pile up shared images to obtain a visually similar secret image. Naor and Shamir[1] first introduced the secret image sharing problem, and proposed the piling-up approach for sharing a binary secret image. Blundo *et al.*[2] extended the Naor and Shamir technique to share a gray-level image. Lin and Tsai[3] adopted a dithering technique to acquire a binary image from a gray image, and then shared the binary image by matrices permutation method. Hou[4] applied the halftone and color decomposition methods to share a color image secretly. Nakajima and Yamaguchi[5] presented a method of sharing a secret image with two other images, in which the secret image can be reconstructed by stacking these two images.

Methods in the mathematical calculation group mathematically calculate the reconstructed image from shared images. Thien and Lin[6] first adopted a mapping key to permute the secret image and then generated shared images by the sharing steps of the Shamir method.[7] Thien and Lin[8] also presented a secret image sharing method with fault tolerance and easy-to-manage properties because each shared image looks like a shrunken version of the original image. Chen and Lin[9] presented a progressive secret image sharing approach in which the number of shared images improves the quality of the reconstructed image. Hung *et al.*[10] used discrete cosine transform (DCT) and band partition to progressively share a secret image. Fang[11] adopted DCT to present a progressive secret image sharing method. Fang[12] also presented a progressive method on binary image with fast decoding and lossless and security properties. Lin and Lin[13] presented a method having the preceding piling-up and mathematical calculation properties.

Chen and Chien[14] presented a method of sharing many secret images in which each participant possesses only one shared image. Wu *et al.*[15] used S-E tables to reduce the shared image size and further hid the shared images into natural images to reduce an attacker's notice. Chen and Fu[16] adopted the Blakley geometry sharing method to share images secretly. Tso[17] first quantized the secret image and then shared the quantized image by Blakley's concept. However, these approaches do not discuss the distortion caused by the Shamir method and the difference in weights of shared images. Yang *et al.*[18] authenticated each shared image for cheater detection and then applied GF(2) for acquiring the perfect reconstruction.

Histogram modulation schemes are adopted to hide information into images. Ni *et al.*[19] embedded watermarks into an image using the histogram modulation method, and

Paper 09018RR received Feb. 17, 2009; revised manuscript received Oct. 1, 2009; accepted for publication Oct. 12, 2009; published online Dec. 3, 2009.

1017-9909/2009/18(4)/043011/6/$25.00 © 2009 SPIE and IS&T.

the original image can be acquired after watermark extraction. Lin *et al.*[20] further improved Ni's method from positive number to absolute number and then applied it to the neighboring difference of a 4×4 block to greatly improve the embedded capacity. Tsai *et al.*[21] presented a difference calculation in a 5×5 block and then applied Ni's method to improve the embedded capacity.

Mathematical secret image sharing methods are based on the Shamir method, in which a prime number determines the shared result. A conventional choice of prime number is 251. Errors between 251 and 255, called the truncation distortion, occur when the secret image has pixel gray level larger than 250. Wang and Su[22] used GF(2) to solve the truncation distortion. This paper adopts the concept of histogram modulation to reduce the truncation distortion. Therefore, this study first presents a histogram modulation scheme to reduce the truncation distortion. Although many secret image sharing methods have been proposed, none of them considers different weightings of the shared image. However, since assigning the same weight to all participants is a crude method that does not always fit the real requirements of people in different positions with different importance. A group-based weighting scheme based on a two-layer structure is then presented to assign different weights to shared images.

The rest of this paper is organized as follows. Section 2 describes the proposed improved secret image sharing method, which involves a histogram modulation scheme to reduce the truncation distortion, and a two-layer secret image sharing scheme to share the secret image with different group possessing weights. Section 3 summarizes the experimental results of the proposed method. Section 4 discusses properties of the proposed method. Conclusions are drawn in Sec. 5, along with future research.

2 Proposed Weighted Modulated Secret Image Sharing Method

Conventional secret image sharing methods suffer from two problems, truncation distortion and identical weight. This section presents two methods to solve these two problems. Section 2.1 presents a histogram modulation scheme to improve the reconstructed image quality. Section 2.2 presents a two-layer scheme to share the secret image with different weights. Section 2.3 combines these two schemes to acquire the proposed weighted modulated secret image sharing method.

2.1 *Proposed Histogram Modulation Scheme*

2.1.1 *Histogram modulation algorithm*

In the Thien and Lin[6] secret image sharing method, the usage of Shamir's method[7] requires a prime number, which is practically set to 251. Every calculated number is the modulus result of this prime number. Pixel gray levels between 251 and 255 are always truncated to 250, and this causes the truncation distortion. Therefore, this work presents a histogram modulation scheme to adjust the secret image to a tuned image. The modulation scheme selects at most five zero points in the histogram and reduces all pixel values larger than these selected points. The proposed histogram modulation algorithm is explained as follows.

1. Acquire the histogram $\{h(j)|0\leqslant j\leqslant 255\}$ of the secret image S.
2. Let the largest gray level of S be $250+d$, where $1\leqslant d\leqslant 5$.
3. Select d zero points as $t_1,t_2,\ldots,t_d$, satisfying $t_1<t_2<\cdots<t_d$.
4. For each zero point from t_d to t_1, subtract the levels larger than the zero point 1 value as Eq. (1):

$$x'=x-1\ (x>\text{the zero point}), \tag{1}$$

   where x denotes the original value, and x' denotes the result after modulation.
5. Acquire the tuned image S', and record the zero points $t_1,t_2,\ldots,t_d$.

Note that the preceding histogram modulation is performed when d is larger than 250. This modulation algorithm adjusts the secret image to a tuned image, which eliminates the gray levels larger than 250 to reduce the truncation distortion. If the secret image contains five zero points in the histogram, then the secret image can be losslessly reconstructed from the tuned image. Natural images, like Lena, Jet, and House, contain more than five zero points.

However, a lossy reconstructed image is acquired when an image contains less than d zero points whose gray levels do not exist in the image. Thus, the following lossless modulation method is proposed to modulate a secret image losslessly. First, the lossless modulation method selects $d+1$ zero points as $t_1,t_2,\ldots,t_{d+1}$. Then, pixels of gray levels $t_1,t_2,\ldots,t_{d+1}$ are replaced by pairs of pixels $(t_1,t_{max}),(t_2,t_{max}),\ldots,(t_{d+1},t_{max})$, respectively, where $t_{max}=250+d+1$. The size of the tuned image is larger then the original size, and the increase is the total amount of pixels with gray levels $t_1,t_2,\ldots,t_{d+1}$. Last, step 4 is performed from t_{d+1} to t_1 to acquire the tuned image.

2.1.2 *Histogram demodulation algorithm*

The histogram demodulation algorithm demodulates the tuned image to the reconstructed secret image. The selected zero points t_1 to t_d are applied to the following increasing calculation as shown in Eq. (2) to acquire the reconstructed image S'':

$$x'=x+1\ (x>\text{the zero point}). \tag{2}$$

The following two steps are applied in the lossless demodulation method. First, the preceding demodulation algorithm from t_1 to t_{d+1} is applied to the tuned image. Then, the losslessly demodulation method replaces the pairs of pixels $(t_1+1,t_{max}),(t_2+1,t_{max}),\ldots,(t_d+1,t_{max})$ with pixels $t_1,t_2,\ldots,t_{d+1}$, respectively, to reconstruct the secret image losslessly.

2.2 *Two-Layer Secret Image Sharing Scheme with Different Group Weights*

A conventional secret image sharing method generates the same weight on all participants. However, a secret image sharing method with different weight fits the real-world requirement for people at different levels in a hierarchy. Accordingly, this section presents a two-layer secret image

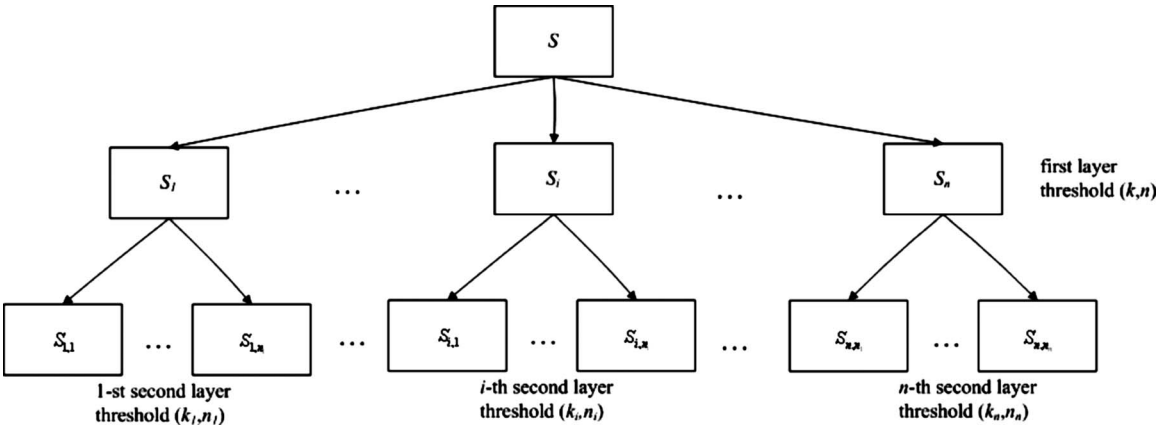

Fig. 1 The proposed two-layer sharing structure.

sharing scheme to weight the shared images differently. Sections 2.2.1 and 2.2.2 show the sharing and recovery algorithms, respectively.

2.2.1 *Two-layer sharing algorithm*

Two secret sharing layers are applied to the tuned image S' in Sec. 2.1 to assign participants different weights. In the first layer, the permuted secret image M is shared to n shared images by threshold (k,n), and each shared image $S_i(1\leqslant i\leqslant n)$ has the same weight $1/k$. The sharing step is performed by Shamir's method.[7] In second layer, each shared image S_i is shared to n_i shared images by threshold (k_i,n_i), and the shared image $S_{i,j}(1\leqslant j\leqslant n_i)$ has the weight $1/k_i$ of the shared image S_i. Thus, in the second layer, shared image $S_{i,j}$ has weight $1/(k\times k_i)$. The sharing algorithm from the tuned image S' to shared images of first layer S_i and from S_i to shared images of second layer $S_{i,j}$ is introduced as follows:

1. Permute the tuned image S' by a user possessing a secret key to acquire permuted image M.
2. Partition M into sets of k pixels. Randomly select n different parameters $x_1,x_2,\ldots,x_n$ with $1<x_i<251$ as the first layer secret key for group i, and then apply the following steps to each set of k pixels:

   a. Allocate k pixels to parameters $a_0,a_1,\ldots,a_{k-1}$ in order.
   b. Calculate $q(x_i)$ from Eq. (3):

$$q(x_i)=a_{k-1}x_i^{k-1}+\ \ldots+a_1x_i+a_0\ (\mathrm{mod}\ 251),\qquad (3)$$

   where $i=1,2,\ldots,n$.
   c. Allocate $q(x_i)$ to shared image S_i of the first layer as one pixel.

3. For each shared image S_i and its corresponding second layer threshold (k_i,n_i):

   a. Partition S_i into sets of k_i pixels. Randomly select n_i different parameters $x_{(i,1)},x_{(i,2)},\ldots,x_{(i,n_i)}$ with $1<x_{(i,j)}<251$ as a secret key for each participant (i,j), and apply steps b to d to each set of k_i pixels.
   b. Allocate k_i pixels to parameters $a_0,a_1,\ldots,a_{k_i-1}$.
   c. Calculate $q(x_{(i,j)})$ from Eq. (4):

$$q(x_{(i,j)})=a_{k-1}x_{(i,j)}+\ \ldots+a_1x_{(i,j)}+a_0\ (\mathrm{mod}\ 251),\qquad (4)$$

   where $j=1,2,\ldots,n_i$.
   d. Allocate $q(x_{(i,j)})$ to shared image $S_{i,j}$ as one pixel.

4. Deliver secret keys $(x_i,x_{(i,j)})$ and shared image $S_{i,j}$ secretly to participant (i,j).

Figure 1 shows the proposed two-layer sharing structure, which requires threshold (k,n) and a set of thresholds (k_i,n_i) in the first and second layers, respectively. Consequently, each participant needs to possess two secret keys x_i and $x_{(i,j)}$ for the first and second layer, respectively. The allocation of k and k_i pixels to Eq. (3) in step 2b, and Eq. (4) in step 3c, reduces the shared image size to $1/k$ and $1/k_i$, respectively. The participant (i,j) denotes the i'th shared image in the first layer and j'th shared image in the second layer.

2.2.2 *Two-layer recovery algorithm*

In section 2.2.1, the secret image is partitioned to $\Sigma_{i=1}^{n}S_{i,n_i}$ shared images belonging to group i in the first layer, and each shared image has weight $1/(k\times k_i)$. Since the weights are different in the second layer, the shared images in the same second layer should be gathered together to acquire the shared image for the first layer, and the permuted image M can be recovered from k reconstructed shared images in the first layer. Therefore, the recovery algorithm uses Lagrange interpolation[6] to perform recovery in the second layer first, followed by the first layer. A reconstructed image is calculated from shared images $S_1,S_2,\ldots,S_k$ with their secret keys, $x_1,x_2,\ldots,x_k$ by the following Lagrange interpolation:

$$q(x)=\sum_{b=1}^{k}y_{k,b}\prod_{j=1,j\neq b}^{k}\frac{x-x_j}{x_b-x_j}\ (\mathrm{mod}\ 251),\qquad (5)$$

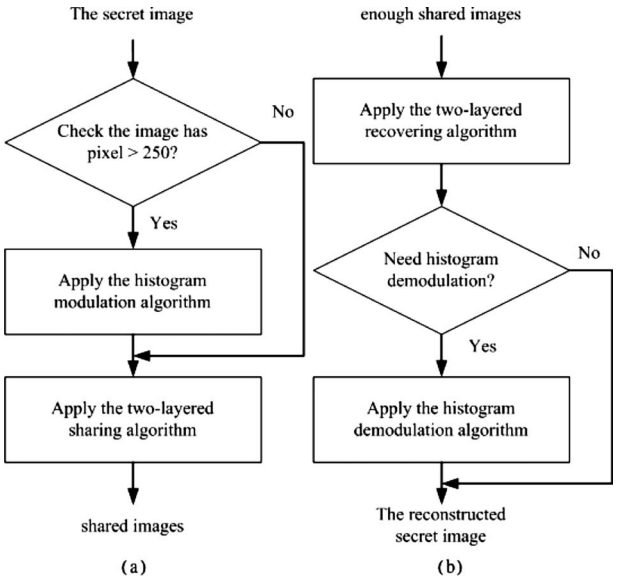

Fig. 2 (a) The proposed sharing algorithm; (b) the proposed recovery algorithm.

where $y_{k,b}$ denotes all pixels of image S_k with $b=1,\ldots,t$ and $1\leqslant t\leqslant$ shared image size. The reconstructed polynomial $q(x)$ has the form $q(x)=a_{k-1}x^{k-1}+\cdots+a_1x+a_0$, and parameter a_i $(i=0,\ldots,k-1)$ denotes one pixel of the reconstructed image S'.

The recovery algorithm is introduced as follows:

1. Select k groups in the second layer, and perform the following steps:
   a. In group i, collect k_i different shared images denoted as $S_1,S_2,\ldots,S_{k_i}$, with their second layer secret keys, $x_{i,1},x_{i,2},\ldots,x_{i,k_i}$, respectively.
   b. Apply Eq. (5) to reconstruct shared image S_i' in first layer.
2. Collect k different shared images in the first layer, denoted as $S_1',S_2',\ldots,S_k'$, with their first layer secret keys, $x_1,x_2,\ldots,x_k$, respectively.
3. Apply Eq. (5) to reconstruct permuted image M'.
4. Reversely permute the image M' by the user's secret key to acquire the reversely permuted image R.

Notably, the reversely permuted image R is consistent with the tuned image S' in Sec. 2.2.1. The proposed histogram modulation scheme in Sec. 2.1 and the two-layer secret image sharing scheme in Sec. 2.2 are combined to form the modulated secret sharing method with different weights, which is described in Sec. 2.3.

2.3 *Proposed Weighted Modulated Secret Image Sharing Method*

Sections 2.1 and 2.2 present schemes that respectively reduce the truncation distortion and share the image to participants with different weights. The proposed method first adjusts the secret image by histogram modulation algorithm and then applies the two-layer sharing algorithm to obtain the shared images. Figure 2(a) depicts the proposed sharing algorithm.

The recovery algorithm first gathers enough shared images and then applies the two-layer recovery algorithm. The histogram demodulation algorithm is then executed if the histogram is modulated in the sharing algorithm. Figure 2(b) depicts the proposed recovery algorithm.

3 Experimental Results

This section presents the experimental results of the proposed modulated weighted secret image sharing method, which reduces the truncation distortion and assigns weights to group participants. The image is Mena with size 256×256, as depicted in Fig. 3(a). Table 1 shows the improved results of applying the proposed histogram modulation scheme, indicating that no truncation distortion occurs because more than five gray levels in the histogram are zero, leading to an infinite peak signal-to-noise ratio PSNR) value or 0 mean square error (MSE) value. In contrast, the first Thien and Lin method[6] has a PSNR value of 47.19 and an MSE value of 1.24, according to Table 1.

Figure 3 shows the experimental results of the proposed method. Figure 3(a) shows the secret image. Figure 3(b) shows the permuted image. The threshold in the first layer is (2,3). Therefore, three shared images are generated, as shown in Figs. 3(c)–3(e). The thresholds selected in the second layer are (1,1), (2,3), and (4,5). The first shared image in the first layer, as shown in Fig. 3(c), performs no further sharing in the second layer with the threshold (1,1), and its weight is also 1/2. Figures 3(f)–3(h) show the shared images of the second layer from the second shared image in the first layer, as depicted in Fig. 3(d). The threshold selection being (2,3) generates the shared images Figs. 3(f)–3(h) that are half the size of Fig. 3(d). The weight of each shared image is $1/2\times1/2$. Figures 3(i)–3(m) show the shared images in the second layer generated from the third shared image in the first layer, which is shown in Fig. 3(e). The shared image in the second layer, shown in Fig. 3(i), is only 1/4 of the size of the image in the first layer, shown in Fig. 3(e). The weight of each shared image is $1/2\times1/4$. Figure 3(n) depicts the reconstructed permuted image based on Figs. 3(f) and 3(g) and Figs. 3(i)–3(l). Figure 3(o) shows the reconstructed shared image, which is consistent with the secret image in Fig. 3(a).

4 Properties Discussion

This section discusses the properties of shared image size, weight of each shared image, and possible weight on shared images in the proposed method. Assume that the first-layer threshold is (k,n), and the i'th second-layer threshold is (k_i,n_i). Then, the shared image size of second-layer shared images from the i'th first-layer shared image is $1/(k*k_i)$ of the secret image size, and the weight is also $1/(k*k_i)$. Last, the possible weights on shared images are determined from the possible forms of $1/(k*k_i)$. If the possible weights are $1/w_1,1/w_2,\ldots,1/w_n$, then $w_1,w_2,\ldots,w_n$ have the greatest common divisor k with $k>1$. Therefore, the first-layer threshold is (k,n), and the second-layer thresholds are $[(w_1/k),n_1],[(w_2/k),n2],\ldots,[(w_n/k),n_n]$. For example, two different weights 1/4 and 1/6 are possible because 4 and 6 have the greatest common divisor 2, resulting in the first-layer threshold $(2,n)$ and second-layer thresholds

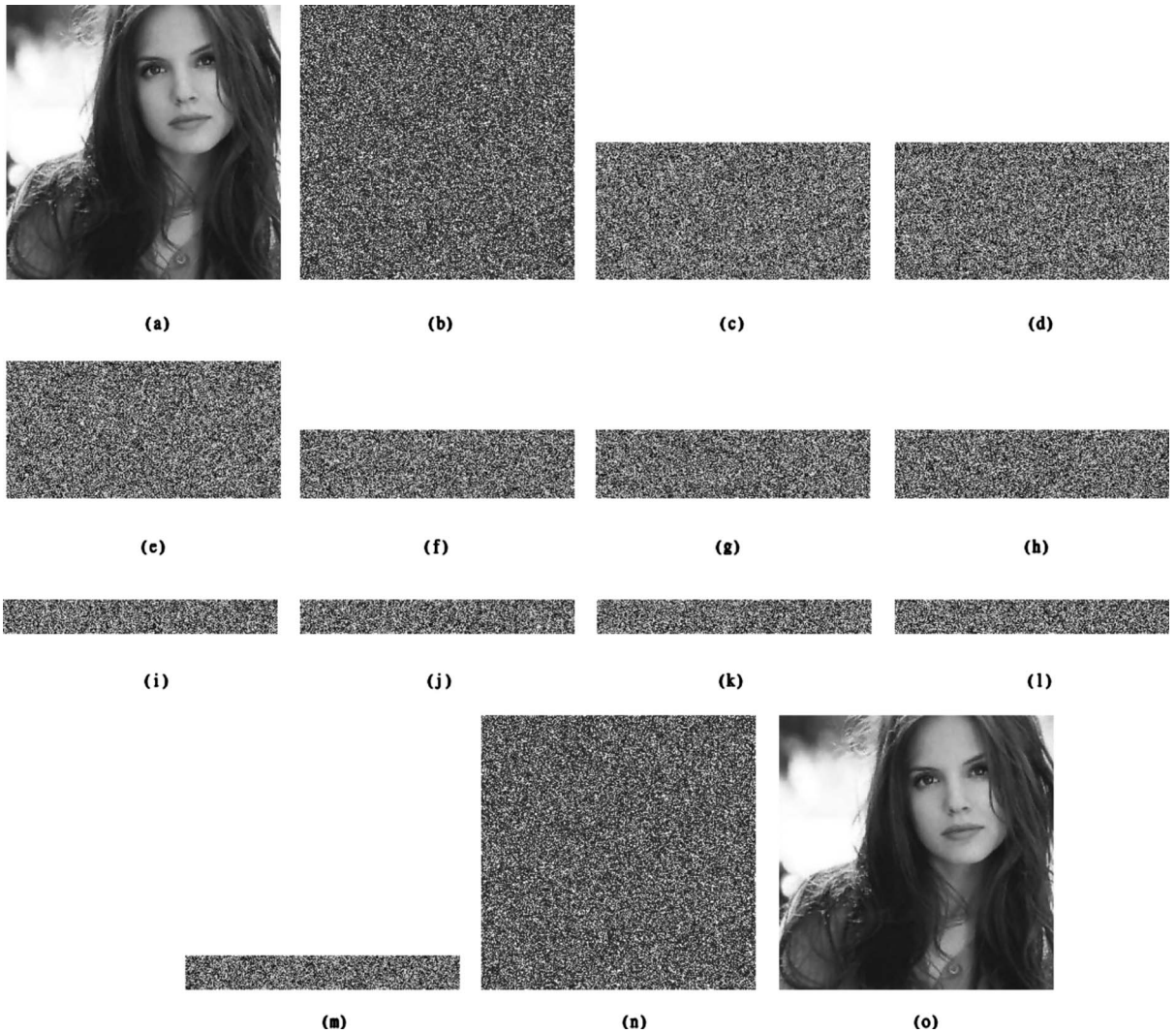

Fig. 3 (a) secret image; (b) permuted image; (c) to (e) three shared images in first layer; (f) to (h) three shared images in second layer from (d); (i) to (m) five shared images in second layer from (e); (n) the reconstructed permuted image; and (o) the reconstructed secret image.

$(2,n_1)$, $(3,n_2)$. However, weights $1/4$ and $1/9$ are infeasible because 4 and 9 have no greatest common divisor larger than 1, which also means that no selection of (k,n) in the first layer and (k_1,n_1), (k_2,n_2) in the second layer may satisfy $1/(k*k_i)=1/4$ and $1/(k*k_j)=1/9$. Significantly, $k=1$ is not a feasible sharing parameter, because it means that only one shared image in the first layer can reconstruct the secret image, thus violating the requirement of secret image sharing. Figure 4 presents the size and weight change in the proposed two-layer method.

In the Thien and Lin method,[6] each shared image and its corresponding secret key has only weight one. Thus, possessing k different shared images and their corresponding secret keys can also have weight k for a participant. Comparing with the Thien and Lin method, the proposed method has the following two advantages. First, each shared image and two secret keys can have any weight in the proposed method. This also means that even if the weight is 90, the proposed method has only two secret keys and one shared image. On the other hand, the Thien and Lin method possesses 90 shared images and their corresponding secret keys. This property reveals the consistency in the possessing load of the proposed method. Second, each secret key must be different and smaller than the prime number 251. Thus, the total sharing weights n in a (t,n) threshold must also be smaller than 251. On the other hand, the proposed two-layer structure provides up to 251×251 total sharing weights.

Table 1 Truncation distortion of image Mena between the proposed and first Thien and Lin methods.

	Proposed method	First Thien and Lin method
PSNR value	∞	47.19
MSE value	0	1.24

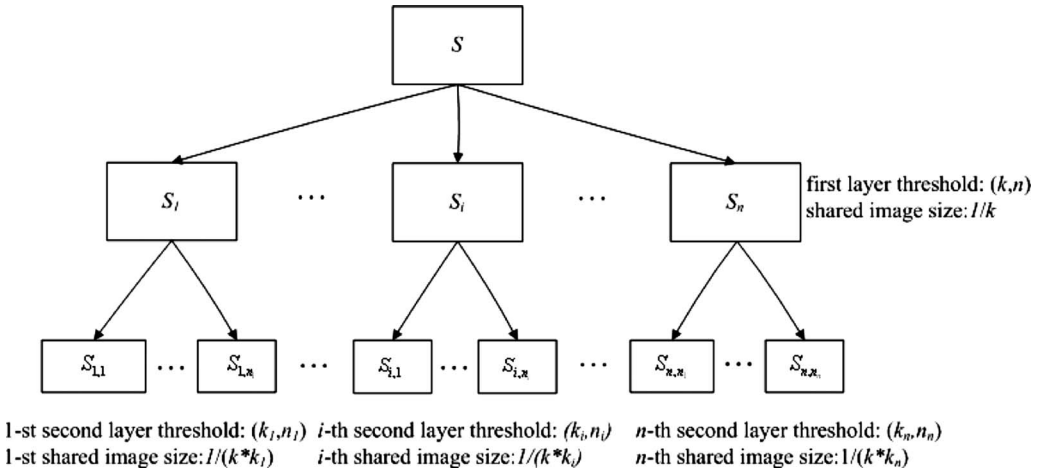

Fig. 4 Size and weight change of shared images in the proposed method.

5 Conclusion

This work presents a weighted modulated secret image sharing method with two components—namely, a histogram modulation and a two-layer structure—which raise the quality of the reconstructed image and provide participants with different weights, respectively. The proposed histogram modulation scheme shifts the image histogram to reduce the truncation distortion. The proposed two-layer structure groups the participants and then assigns participants within each group a particular weight. Enough groups are collected to reconstruct the secret image. Experimental results demonstrate that the proposed method significantly reduces the distortion of the reconstructed image and that participants can have different weights. Future work will focus on improving secret image sharing capabilities.

References

1. M. Naor and A. Shamir, "Visual cryptography, advances in cryptology," in *Eurpocrypt '94*, pp. 1–12, Springer-Verlag, Berlin (1995).
2. C. Blundo, A. D. Santis, and M. Naor, "Visual cryptography for gray level images," *Inf. Process. Lett.* **75**, 255–259 (2000).
3. C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recogn. Lett.* **24**, 349–358 (2003).
4. Y. C. Hou, "Visual cryptography for color images," *Pattern Recogn.* **36**, 1619–1629 (2003).
5. M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *J. WSCG* **10**, 303–310 (2002).
6. C. C. Thien and J. C. Lin, "Secret image sharing," *Comput. Graphics* **26**, 765–770 (2002).
7. A. Shamir, "How to share a secret," *Commun. ACM* **22**, 612–613 (1979).
8. C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images," *IEEE Trans. Circuits Syst. Video Technol.* **12**, 1161–1169 (2003).
9. S. K. Chen and J. C. Lin, "Fault-tolerance and progressive transmission of images," *Pattern Recogn.* **38**, 2466–2471 (2005).
10. K. H. Hung, Y. J. Chang, and J. C. Lin, "Progressive sharing of an image," *Opt. Eng.* **47**, 047006 (2008).
11. W. P. Fang, "Quality controllable progressive secret image sharing—discrete cosine transform approach," *Int. J. Educ. Inf. Technol.* **1**, 43–47 (2007).
12. W. P. Fang, "Friendly progressive visual secret sharing," *Pattern Recogn.* **41**, 1410–1414 (2008).
13. S. J. Lin and J. C. Lin, "VCPSS: a two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches," *Pattern Recogn.* **40**, 3652–3666 (2007).
14. C. C. Chen and Y. W. Chien, "Sharing numerous images secretly with reduced possessing load," *Fund. Inform.* **86**, 447–458 (2008).
15. Y. S. Wu, C. C. Thien, and J. C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recogn.* **37**, 1377–1385 (2004).
16. C. C. Chen and W. Y. Fu, "A geometry-based secret image sharing approach," *ASME J. Comput. Inf. Sci. Eng.* **24**, 1567–1577 (2008).
17. H. K. Tso, "Sharing secret images using Blakley's concept," *Opt. Eng.* **47**, 077001 (2008).
18. C. N. Yang, T. S. Chen, K. H. Yu, and C. C. Wang, "Improvements of image sharing with steganography and authentication," *J. Syst. Softw.* **80**, 1070–1076 (2007).
19. Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.* **16**, 354–362 (2006).
20. C. C. Lin, W. L. Tai, and C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images," *Pattern Recogn.* **41**, 3582–3591 (2008).
21. P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.* **89**, 1129–1143 (2009).
22. R. Z. Wang and C. H. Su, "Secret image sharing with smaller shadow images," *Pattern Recogn. Lett.* **27**, 551–555 (2006).

Chien-Chang Chen received a BS degree from the Department of Computer and Information Science at Tung Hai University, Taichung, in 1991, and a PhD degree in computer science from National Tsing Hua University in 1999. He is currently an associate professor at the Department of Information Management, Hsuan Chuang University. His research interests include secret image sharing, watermarking, and texture analysis.

Chaur-Chin Chen received a BS degree from the Department of Mathematics, National Taiwan University, in 1977, and MS degrees in mathematics and in computer science and a PhD degree in computer science, all from Michigan State University in 1982, 1984, and 1988, respectively. He is currently a professor in the Department of Computer Science, National Tsing Hua University, Taiwan. He teaches courses in computational mathematics, numerical methods, algorithms for image pattern analysis, digital image processing, pattern recognition, discrete mathematics, linear algebra, probability theory, and cryptography. His current research interests include information hiding, watermarking, fingerprint image recognition, face image recognition, and microarray image data analysis. Dr. Chen has coordinated the summer short courses for Honduras UNITEC students in the Institute of Information Systems and Applications, NTHU, from 2006 to 2009.

Yun-Cheng Lin received a master's degree in computer science from Hsuan Chuang University, Taiwan, in 2008. His major research interests include secret image sharing and watermarking.