Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **1**, January **2016**

An Expandable Essential Secret Image Sharing Structure

Chien-Chang Chen[1] and Yao-Hong Tsai[2]

[1]Department of Computer Science and Information Engineering
Tamkang University
Taipei, Taiwan
ccchen34@mail.tku.edu.tw

[2]Department of Information Management
Hsuan Chuang University
Hsinchu 300, Taiwan

Received May, 2015; revised October, 2015

Abstract. *This study presents an expandable essential secret image sharing structure showing that some important shared images, named essential ones, are necessary when recovering the secret image and the proposed structure must incorporate other secret image sharing scheme to expand to a new secret image sharing scheme with multiple functions. An (s, t, n) essential secret image sharing structure shares a secret image with two kinds of shared images, essential and non-essential ones, and the total number of shared images is n. Two criteria must be met to recover the secret image. Firstly, the number of essential images must be at least s. Secondly, the number of collected shared images, including essential and non-essential ones, must be at least t. An essential participant holds his secret key as a conventional secret key concatenated by a shared essential key. The shared image for a non-essential participant is the XOR result of a correct shared image and a disturbed image generated from the essential key. Experimental results reveal that the proposed method distinguishes essential and non-essential shared images, and keeps the threshold on essential shared images in recovering the secret image.*
Keywords: (s, t, n) secret image sharing structure, Essential shared image, Non-essential shared image.

1. **Introduction.** Nowadays, digital images are popularly used in daily life, and making it important to protect valuable images during storage or transmission. The secret image sharing technique is an efficient way to protect digital images. This technique works by sharing one secret image among shared images (which all look like noise images), and then gathering enough shared images to recover the secret image.

Thien and Lin were the first work to utilize the Shamir-Lagrange method to share and recover secret images [1], and then many researchers later presented other functional secret image sharing schemes, like cheater detection [2], progressive [3, 4, 5, 6], multi-thresholds [7, 8], weighted [9], visual cryptography and secret image sharing [10, 11], scalable [12, 13], and invertible sharing [14, 15, 16]. Excepting the Shamir-Lagrange method, many other methods, like Blakley [17], Boolean [18, 19], and Chinese Remainder Theorem [20, 21], are also used to share important images secretly.

Although numerous secret image sharing methods have been presented, an efficient scheme for distinguishing essential and non-essential participants has not been proposed.

The difference comes from the roles of participants played being important or not. Meanwhile, in recovering the secret image, essential participants should play more important roles than others do. Yang et al. [22] used two-layered hierarchy structure to assign different weight on essential and non-essential shared images.

This paper presents an (s, t, n) essential secret image sharing structure that needs another secret image sharing scheme (*S.I.S.*)[1-22]. The proposed structure generates a secret image sharing scheme with multiple functions. The secret image is shared with n shared images. Two kinds of shared images, essential and non-essential, are generated from the proposed structure. In the sharing algorithm, a disturbed image generated from an essential key is needed. Each essential participant possesses a combined secret key, composed of a secret key in *S.I.S.* and a shared essential key. Each non-essential shared image is the XOR result of the correct shared image and the disturbed image, which is generated from the essential key.

In the recovering algorithm, s essential shared images and totally t shared images are needed to recover the secret image. The essential key is first recovered from the shared essential key possessed by s essential participants. The disturbed image, generated from the essential key, is used to acquire correct shared images. At last, the secret image can be perfectly recovered when the number of essential and non-essential shared images is t.

The rest of this paper is organized as follows. Section 2 describes the proposed essential secret image sharing structure. Algorithms of sharing a secret image among shared images and recovering the secret image from shared images are presented in sections 2.1 and 2.2, respectively. Section 3 presents experimental results and comparisons between the proposed structure and other related works. I draw conclusions in Section 4, and propose future research.

2. Proposed (s, t, n) Essential Secret Image Sharing Structure.

This section introduces the proposed (s, t, n) essential secret image sharing structure. Figure 1 depicts the structure of the proposed structure, in which a secret image sharing scheme is required and named as $S.I.S.\,sharing\,procedure$. The proposed structure generates essential and non-essential shared images with numbers n_e and n-n_e, respectively. Collecting s essential shared images and t shared images recover the secret image. Moreover, the sharing and recovering procedures of an *S.I.S.* can be replaced by any existing secret image sharing scheme, which may be a Shamir-Lagrange or Chinese Remainder Theorem based scheme. The proposed sharing and recovering algorithms are presented in Sections 2.1 and 2.2, respectively.

2.1. Sharing Algorithm.

Another secret image sharing scheme, denoted by (*S.I.S.*) is needed in the proposed sharing structure. The *S.I.S.* scheme can be purely secret image sharing schemes [1, 17, 20] or other functional secret image sharing schemes [2-16]. In an (s, t, n) essential secret image sharing structure ($s \leq t \leq n$), an essential key e_k, the essential key generated disturbed image R, and the Shamir-Lagrange scheme are required. Two kinds of participants, essential and non-essential ones, share the secret image. The difference between these two participants is that each essential participant takes an extra key, and each non-essential participant takes a modified shared image. Assume that the numbers of essential and non-essential participants are n_e and $n - n_e$, respectively. Therefore, without loss of generality, participant i ($1 \leq i \leq n\_e$) is an essential participant and participant j ($n\_e + 1 \leq j \leq n$) is a non-essential participant. The present sharing algorithm is as follows.

1. Share the secret image to n shared images S_i ($1 \leq i \leq n$) and their corresponding secret key k_i by an *S.I.S.* scheme.

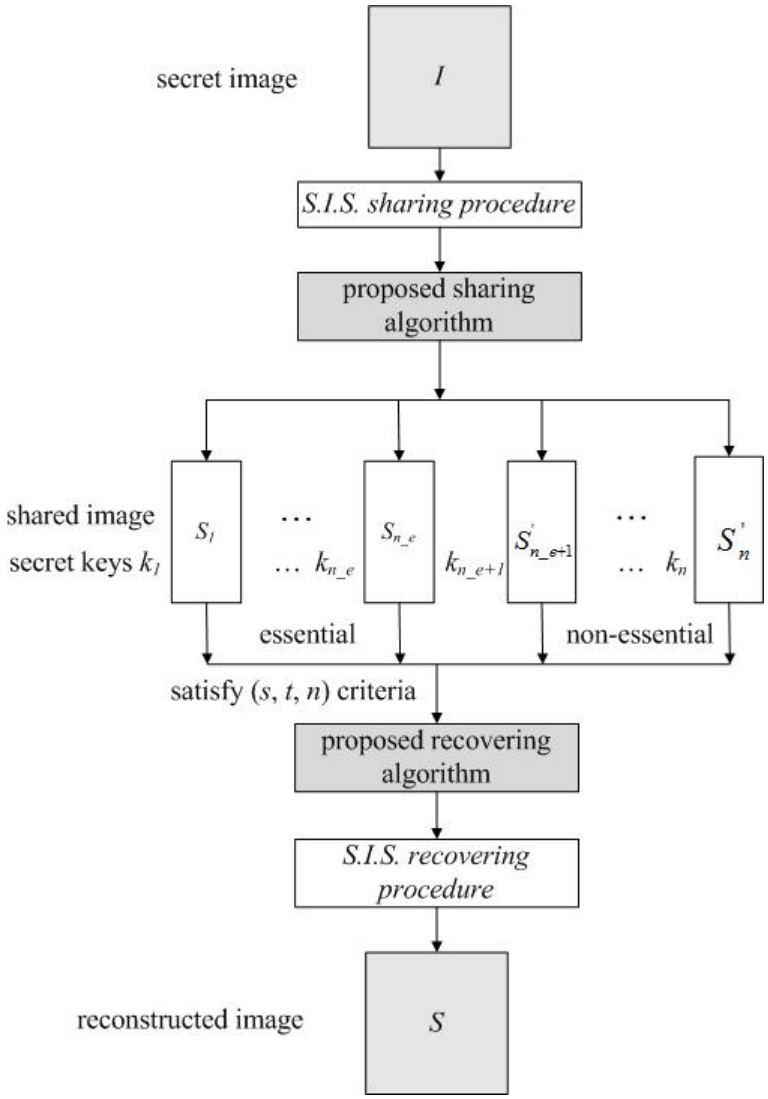

FIGURE 1. Flow of the proposed structure

2. For all non-essential shared images S_j $(n\_e + 1 \leq j \leq n)$, perform the following calculation to acquire modified shared images

$$S'_j = S_j \oplus R \tag{1}$$

where R is the disturbed image generated from the essential key e_k.

3. Randomly select $s-1$ numbers $a_1, \cdots, a_{s-1}$ and calculate shared essential keys $E(k_i)$ by the following calculation

$$E(x) = a_{s-1}x^{s-1} + a_{s-2}x^{s-2} + \cdots + a_1x + e_k (mod\ p) \tag{2}$$

where p denotes a prime number that is larger than each secret key $k_i (1 \leq i \leq n\_e)$.

4. For each essential participant, concatenate each shared essential key $E(k_i)$ corresponding with its secret key k_i to form a new secret key, denoted by $k_i \parallel E(k_i)$, and assign shared image S_i corresponding with the new secret key $k_i \parallel E(k_i)$ to participant $i (1 \leq i \leq n_e)$.

5. For each non-essential participant, assign modified shared image S'_j corresponding with secret key k_j to participant $j (n\_e + 1 \leq j \leq n)$.

Notably, in Step 1 of the sharing algorithm, any *S.I.S.* scheme as a *S.I.S. sharing procedure* block denoted in Figure 2 should be used. The number of essential participants is n_e and it cannot be smaller than threshold s. Figure 2 shows the proposed sharing algorithm, in which grey blocks represent images or shared images.

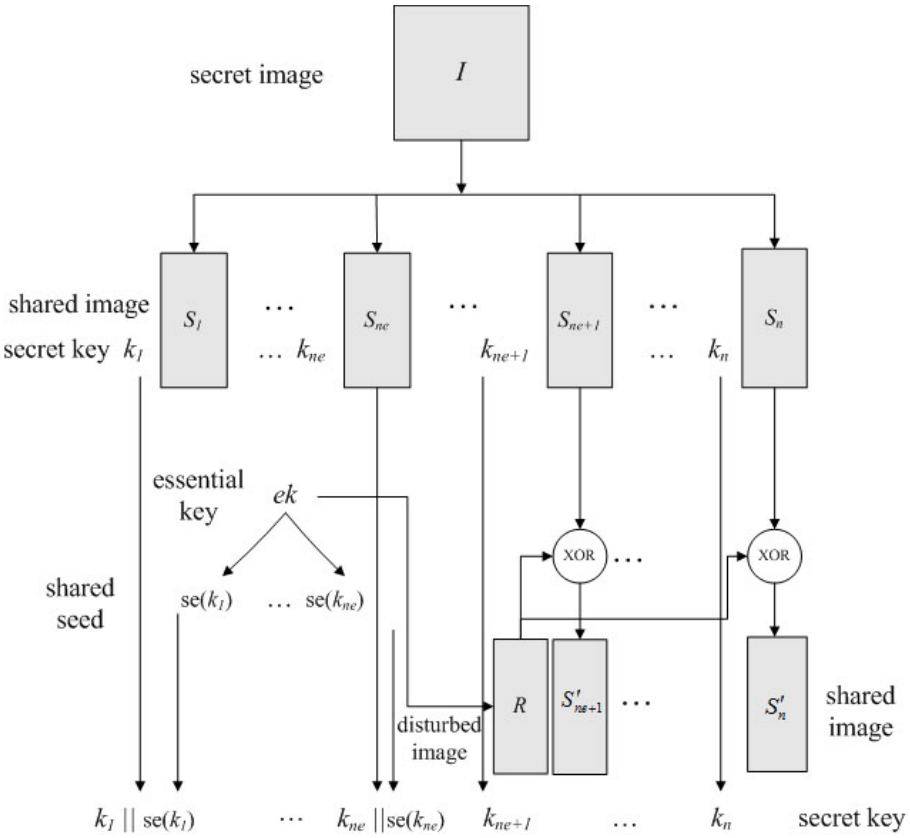

FIGURE 2. The proposed sharing algorithm

2.2. **Recovering Algorithm.** The proposed $(s,\ t,\ n)$ secret image sharing structure ensures that s essential shared images and totally t shared images recover the secret image. The first step in the recovering algorithm is to recover the essential key e_k from s shared essential keys. Then, the disturbed image R, generated from the essential key e_k, is used by performing the XOR operation to all non-essential shared images to obtain correct non-essential shared images. At last, the secret image is recovered from totally t essential and correct non-essential shared images. The recovering algorithm is illustrated as follows.

1. Gather s essential shared keys denoted by $k_b \parallel y_b\{1 \leq b \leq s\}$ to calculate the essential key e_k as the constant term in the following Lagrange Interpolation

$$r(x) = \sum_{b=1}^{s} y_b \prod_{j=1, j\neq b}^{s} \frac{x - k_j}{k_b - k_j} = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + .. + a_1 x + e\_k (mod\ p) \tag{3}$$

where p denotes the same prime number used in Eq. (2).

2. Generate the disturbed image R from the essential key e_k.

3. Perform the XOR operation on the disturbed image R and each non-essential shared image S'_b to acquire correct non-essential shared image S_b by Eq. (4)

$$S_b = S'_b \oplus R \tag{4}$$

4. Rename all essential and correct non-essential shared images with their corresponding secret key by S_i $(1 \leq i \leq t)$ and k_i $(1 \leq i \leq t)$, respectively.

5. Perform the recovering procedure of $S.I.S.$ scheme to acquire the reconstructed image S.

Figure 3 depicts the important steps and notations of the proposed recovering algorithm. This figure shows that s shared secret keys recover the essential key e_k by the Lagrange Interpolation. Then, the disturbed image R, which is generated from e_k, is adopted to acquire correct non-essential shared images. At last, applying t essential and correct non-essential shared images with corresponding secret keys to an $S.I.S.$ recovering procedure acquires the secret image.

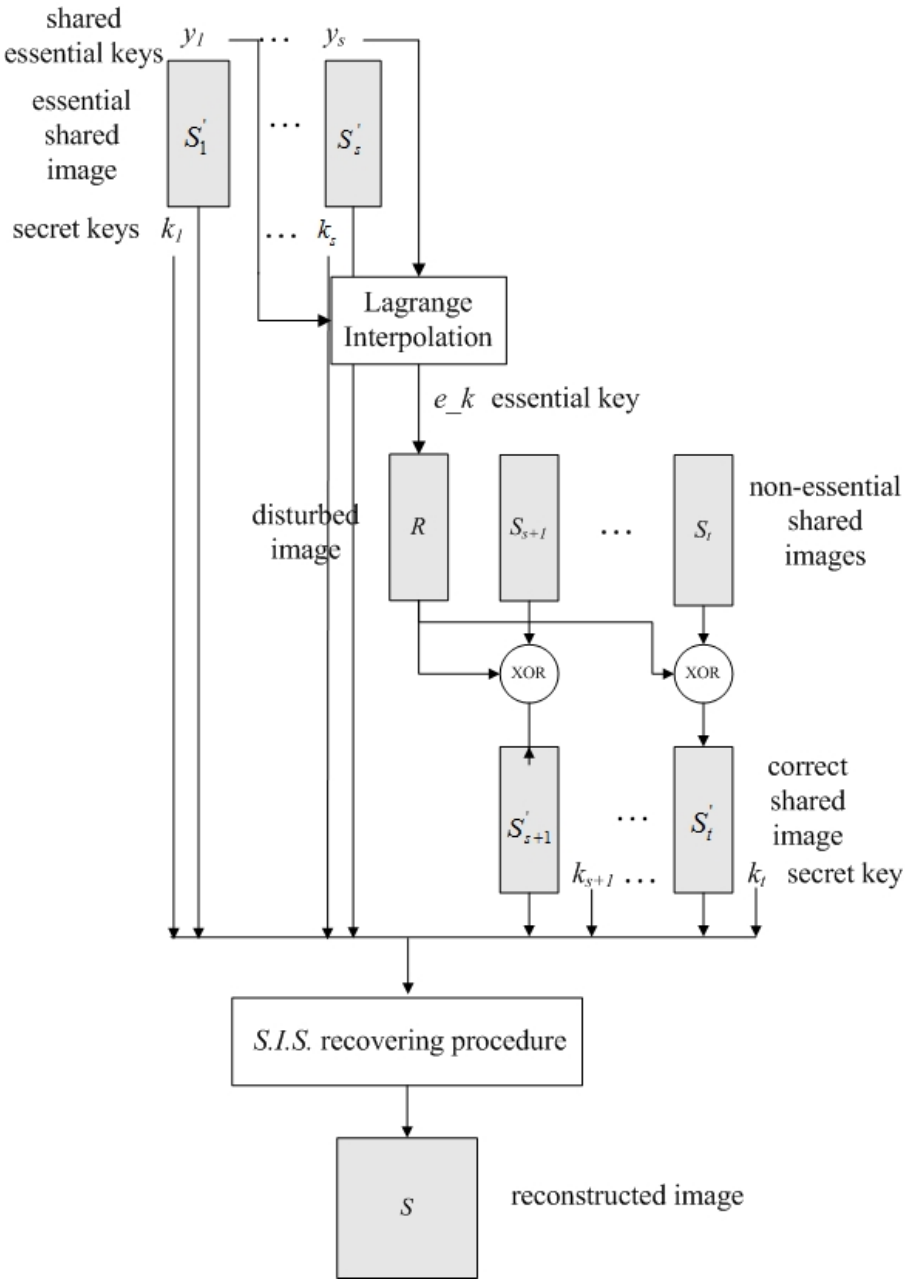

FIGURE 3. The proposed recovering algorithm

3. **Experimental Results and Discussion.**

3.1. **Experimental Results.** This section presents experimental results obtained from the proposed structure. The test image is LENA with size 512×512 and the utilized secret image sharing scheme is literature [20], which is a Chinese Remainder Theorem based secret image sharing scheme. The selected secret prime keys are 211, 227, 233, 241, 251 and the essential key is 399. The thresholds (s, t, n) are selected as (2, 4, 5). This threshold assignment shares the secret image among 5 shared images, including essential and non-essential shared images. In our experiments, the numbers of essential and non-essential shared images are 2 and 3, respectively. Therefore, collecting 2 essential shared images and 2 non-essential shared images recovers the secret image.

Figure 4.(a) presents the secret image LENA and Figs. 4.(b)-4.(f) depict the calculated 5 shared images with size 512×256, in which Figs. 4.(b)-4.(c) depict two essential shared images and Figs. 4.(d)-4.(f) depict three non-essential shared images. For the essential property, Figs. 4.(d)-4.(f) are results obtained by performing the XOR operation on correct non-essential shared images and the generated disturbed image R, which is shown in Figure 4.(g).

Two different recovering experimental results are provided in Figs. 4.(h) and 4.(i). Figure 4.(h) shows the reconstructed image by four shared images, Figs. 4.(c)-4.(f). Although the number of collected shared images is 4, the reconstructed image is not correct because number of essential shared images is less than 2, and the disturbed image R cannot be generated. Therefore, we cannot acquire the correct non-essential shared image to recover the secret image. Figure 4.(i) depicts the reconstructed image by shared images as shown in Figs. 4.(b)-4.(e). In this case, the number of essential shared images satisfies the threshold s and so the essential key e_k can be acquired. The disturbed image R, which is generated by e_k, is then adopted to obtain correct non-essential shared images. Therefore, 4 correct shared images are enough to acquire the correct reconstructed image as shown in Figure 4.(i). We can also conclude that using Figs. 4.(b), 4.(c), 4.(e), 4.(f) or using Figs. 4.(b)-4.(d), 4.(f) can recover the secret image, too.

Figure 5 depicts experimental results of sharing another test image Baboon. Like the results shown in Fig. 4, each shared images as given in Figs. 5.(b)-5.(f) are all random-like images. The false and correct recoveries using Figs. 5.(b), 5.(d)-5.(f) and Figs. 5.(b)-5.(e) are presented in Fig. 5.(h) and Fig. 5.(i), respectively.

The experimental results above show that the proposed (s, t, n) essential secret image sharing structure efficiently ensures that s essential shared images and t shared images are needed to recover the secret image. These two criteria can be more clearly defined as follows. Firstly, s essential shared keys are needed to acquire the essential key e_k for generating the disturbed image R. Secondly, the total number of essential and non-essential shared images must be t. The first criterion ensures that enough essential participant join the recovering procedure, meaning that important persons are needed in the recovering procedure. The second criterion ensures that enough members are needed to recover the secret image. This property prevents few members from acquiring the secret image for the system security.

At last, the proposed structure adopts another scheme to expand to a multi-functions secret image sharing scheme. Therefore, properties in the selected secret image sharing scheme are involved in the proposed structure. For example, our experiment adopts literature [2] to acquire a hybrid secret image sharing scheme with essential property. Therefore, the proposed structure can adopt any secret image sharing scheme to enrich its properties. Comparing with related work [22], our proposed structure can easily combined with other significant secret image sharing scheme rather than only includes essential property. The proposed structure requires little computation load. The sharing algorithm includes four parts as denoted by disturbed image generation, XOR computation, Shamir sharing,

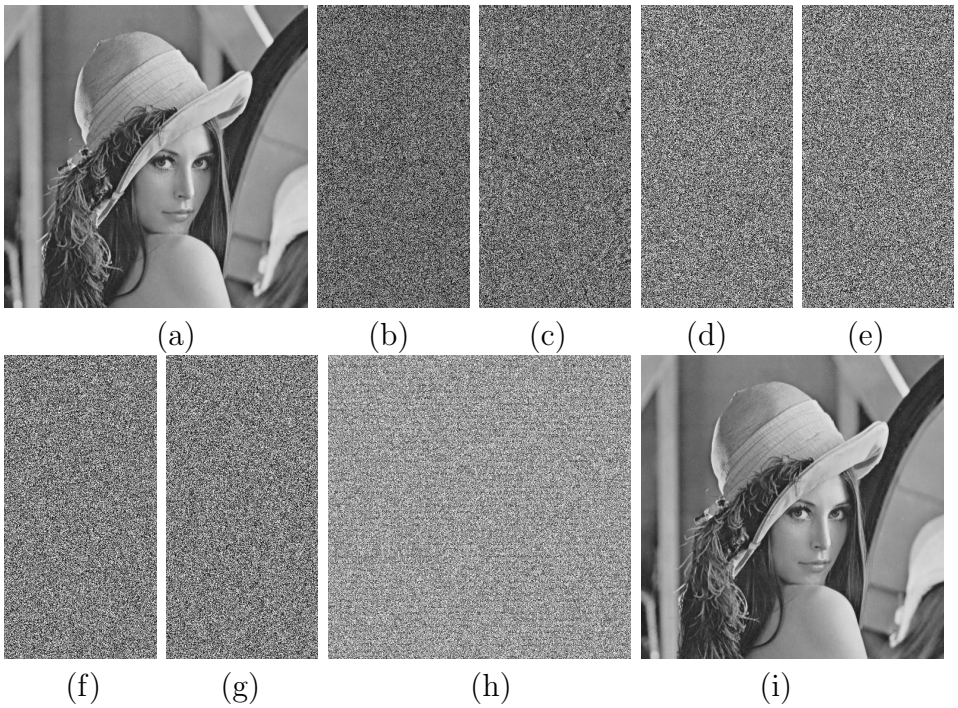

FIGURE 4. (a) secret image LENNA, (b)-(c) two essential shared images, (d)-(f) three non-essential shared images, (g) the disturbed image R, (h) reconstructed image from (c)-(f), (i) reconstructed image from (b)-(e).

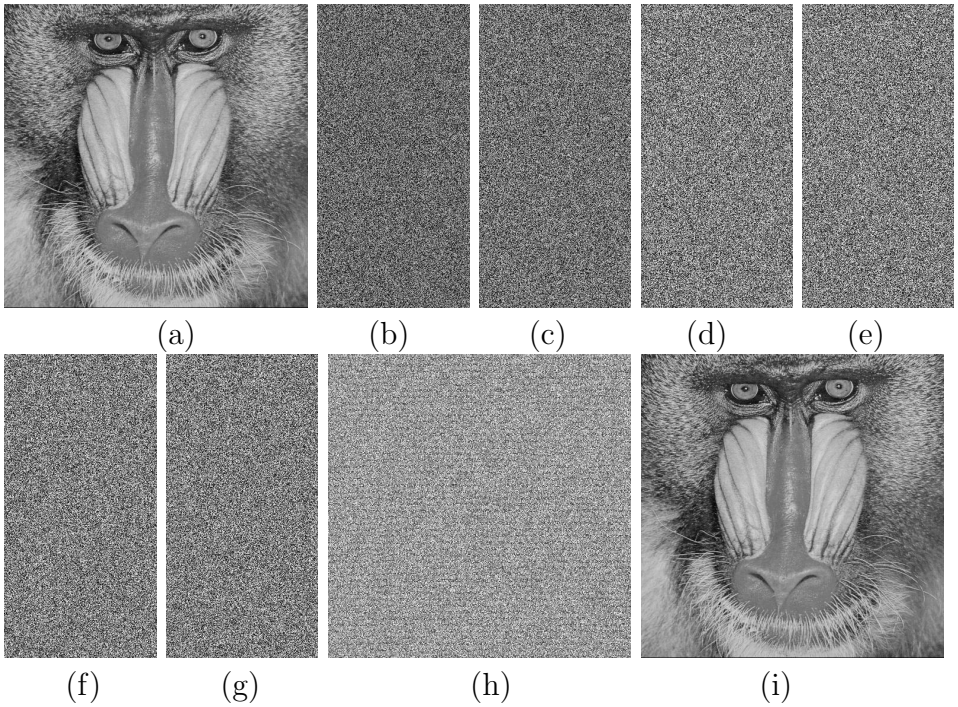

FIGURE 5. (a) secret image Baboon, (b)-(c) two essential shared images, (d)-(f) three non-essential shared images, (g) the disturbed image R, (h) reconstructed image from (c)-(f), (i) reconstructed image from (b)-(e).

and concatenation. The disturbed image generation part acquires the disturbed image R from one essential key e_k and the generation time is proportional to image size as denoted by $O(N)$, where N is the image size. The XOR computation part performs XOR calculations on non-essential shared images and the disturbed image R, which acquires the computation complexity of $O(N)$. The Shamir sharing part shares the essential key e_k among participants and the computation load is proportional to the secret key number n_e as denoted by $O(n_e)$. At last, the concatenation part concatenates the shared essential key with original participant key, respectively. The computation load is quite little and it can be ignored. Therefore, the computation complexity of the proposed sharing structure can be summarized to $O(N)$ since the image size N is quite large than n_e. The sharing algorithm includes three parts as denoted by Lagrange interpolation, disturbed image generation and XOR computation. Since the computation complexity of Lagrange Interpolation is $O(N^2)$ of processing N sets of interpolating data, the computation complexity of Lagrange interpolation part is $O(s^2)$. Like the sharing algorithm, the disturbed image generation part and the XOR computation part also have the time complexity of $O(N)$. Since image size N is far more than essential threshold s, the time complexity of the recovering algorithm is $O(N)$.

3.2. **Characteristics Comparison.** This section compares characteristics between the proposed structure and Shamir-Lagrange based secret image sharing methods. The compared characteristics include scheme feature, combining feasibility, sharing complexity, and recovering complexity, as shown in Table 1. These different characteristics are explained as follows.

Table 1. Characteristics compared between the proposed scheme and important literatures.

Schemes	Scheme Feature	Combination Feasibility	Sharing Complexity	Recovering Complexity
Thien and Lin [1]	secret image sharing	hard	$\approx \frac{N}{k} \times (2k-3) \times n$	$\approx 2 \times k \times N$
Chen and Liu [2]	cheater identification	hard	$\approx \frac{N}{k} \times (2k-3) \times n + \frac{N}{k} \times g_i$	$\approx 2 \times k \times N + \frac{N}{k} \times f$
Huang et al. [5]	progressive	hard	$\approx (2k-3) \times N$	$\approx 2 \times k \times N$
Hung et al. [6]	progressive	hard	$\approx \frac{N}{k} \times (2k-3) \times n + 2 \times N$	$\approx 2 \times k \times N + 2 \times N$
Wu et al. [16]	share to host images	hard	$\approx \frac{N}{k} \times (2k-3) \times n + 7 \times E + \frac{N}{k} \times 3 \times n$	$\approx 2 \times k \times N + E + \frac{N}{k}$
proposed scheme	essential	easy	$\approx (2k-3) \times n$	$\approx 2 \times k^2$

(1) scheme feature: Significant features between the selected secret image sharing schemes are compared. These properties include secret image sharing [1], progressive [5, 6], and share to host images [16].

(2) combining feasibility: Combining feasibility means the difficulty on combining with other secret image sharing scheme. Since all schemes have their property on sharing with some feature. Only the proposed structure is built based on other secret image sharing

scheme. Therefore, the proposed structure has the lowest difficulty to combine with other secret image sharing scheme.

(3) sharing and recovering complexity: These two complexities record the multiplication of sharing and recovering procedures in all schemes. Since all schemes may require other computations like addition, XOR, round-off, and comparison. Therefore, the comparisons used notation to ignore other load. Although, those computations requires fewer CPU computation time than multiplication requires. Furthermore, the defined thresholds are (t, n), meaning to share a secret image to n shared images and collecting t shared images recover the secret image. Some other notations should be introduced. Chen and Liu [2] used g_i to be user selected integer. Wu et al. [16] partitioned the secret image to combination of 1×2 blocks, in which E represents the number of edge blocks.

Figure 4, Figure 5 and Table 1 show that the proposed (s, t, n) essential secret image sharing structure has essential and easily combined characteristics, that is rarely found in previous secret image sharing schemes [1-22]. The most important characteristic in the proposed scheme is that it easily incorporates other secret image sharing schemes to enrich the hybrid scheme for complementing other secret image sharing scheme. Significance of the proposed structure is thus revealed.

4. **Conclusions.** This work presents another secret image sharing scheme-based technique with the properties of essential thresholds. The proposed (s, t, n) essential secret image sharing structure shares a secret image with essential and non-essential shared images with the property that s essential shared images and t shared images recovers the secret image. This property ensures a secure sharing system with the essential property of requiring both important members and enough members to recover the secret image. Experimental results demonstrate that the proposed method exhibits the essential property well, and can be easily incorporated other secret image sharing schemes. Future work will focus on a secure secret image sharing scheme for detecting cheaters in secret keys and shared images.

Acknowledgment. This paper was partially supported by the National Science Council of the Republic of China under contract MOST 104-2221-E-364-002. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] C.C. Thien and J.C. Lin, Secret image sharing, *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[2] C.C. Chen and C.A. Liu, Tamper-Proof secret image sharing scheme for identifying cheated secret keys and shared images, *Journal of Electronic Imaging*, vol.22, no.1, 013008, 2013.

[3] S.K. Chen and J.C. Lin, Fault-tolerance and progressive transmission of images, *Pattern Recognition*, vol.38, no.12, pp. 2466–2471, 2005.

[4] W.P. Fang, Friendly progressive visual secret sharing, *Pattern Recognition*, vol. 41, no. 4, pp. 1410–1414, 2008.

[5] C.P. Huang, C.H. Hsieh, P.S. Huang, Progressive sharing for a secret image, *Journal of Systems and Software*, vol. 83, no. 3, pp. 517–527, 2010.

[6] K.H. Hung, Y.J. Chang, J.C. Lin, Progressive sharing of an image, *Optical Engineering*, vol. 47, pp. 047006, 2008.

[7] C. Guo, C.C. Chang, and C. Qin, A Hierarchical Threshold Secret Image Sharing Scheme, *Pattern Recognition Letters*, vol. 33, pp. 83–91, 2012.

[8] C. Guo, C.C. Chang, and C. Qin, A Multi-threshold Secret Image Sharing Scheme Based on MSP, *Pattern Recognition Letters*, vol. 33, pp. 1594–1600, 2012.

[9] S.J. Lin, L.S. Chen, J.C. Lin, Fast-weighted secret image sharing, *Optical Engineering*, vol. 48, pp. 077008, 2009.

[10] 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 Recognition*, vol. 40, pp. 3652–3666, 2007.
[11] C.N. Yang and C.B. Ciou, Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability, *Image and Vision Computing*, vol. 28, no. 12, pp. 1600–1610, 2010.
[12] C.C. Thien and J.C. Lin, An image-sharing method with user-friendly shadow images, *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, 1161–1169, 2003.
[13] R.Z. Wang, Y.F. Chien, Y.Y. Lin, Scalable user-friendly image sharing, *Journal of Visual Communication and Image Representation*, vol. 21, pp. 751–761, 2010.
[14] M. Ulutas, G. Ulutas, V. Nabiyev, Invertible secret image sharing for gray level and dithered cover images, *The Journal of Systems and Software*, vol. 86, no. 2, pp. 485–500, 2013.
[15] X. Wu, D. Ou, Q. Liang, W. Sun, A user-friendly secret image sharing scheme with reversible steganography based on cellular automata, *The Journal of Systems and Software*, vol. 85, pp. 1852–1863, 2012.
[16] Y.S. Wu, C.C. Thien, J.C. Lin, Sharing and hiding secret images with size constraint, *Pattern Recognition*, vol. 37, pp. 1377–1385, 2004.
[17] C.C. Chen and W.Y. Fu, A Geometry-Based Secret Image Sharing Approach, *Journal of Information Science and Engineering*, vol.24, no.5, pp. 1567–1577, 2008.
[18] C.C. Chen and W.J. Wu, A secure Boolean-based multi-secret image sharing scheme, *The Journal of Systems and Software*, vol.92, no.1, pp. 107–114, 2014.
[19] T.H. Chen and C.S. Wu, Efficient multi-secret image sharing based on Boolean operations, *Signal Processing*, vol. 91, pp. 90–97, 2011.
[20] S.J. Shyu and Y.R. Chen, Threshold Secret Image Sharing by Chinese Remainder Theorem, *IEEE Asia-Pacific Services Computing Conference*, 1332–1337, 2008.
[21] C.C. Chen and J.Y. Huang, Progressive Share of Secret Audio by Chinese Remainder Theorem and Integer Wavelet Transform, *International Journal of Electronic Commerce Studies*, vol.5, no.2, 219–232, 2014.
[22] C.Y. Yang, P. Li, C.C. Wu, S.R. Cai, Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach, *Signal Processing: Image Communication*, vol. 31, pp.1–9, 2015.