International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.259-270
http://dx.doi.org/10.14257/ijsia.2015.9.1.25

A New (*n*, *n*)-threshold Reversible Secret Image Sharing Using Histogram Shifting

Gil-Je Lee, Dae-Soo Kim, and Kee-Young Yoo*

School of Computer Science and Engineering, Kyungpook National University, Daegu, South Korea
vilelkj@infosec.knu.ac.kr, stairways@infosec.knu.ac.kr, yook@knu.ac.kr

Abstract

In this paper, we propose a (*n, n*)*-threshold reversible secret image sharing scheme using histogram shifting. Unlike Shamir's secret sharing, the proposed scheme does not use a polynomial. In the secret image sharing procedure, a histogram is generated by the difference value between the original and copy images. And, the secret image is embedded into original and copy images by using histogram shifting. Lastly, generated shadow images are distributed to each participant. In the experimental results, we measure embedding capacity of secret image and a distortion ratio between original and shadow images. The experimental results show that the embedding capacity and image distortion ratio of the proposed scheme are superior to the previous schemes.*

Keywords: *Reversible secret image sharing, Histogram shifting, Embedding Capacity, PSNR*

1. Introduction

Cryptography is a transformed message where information needs to be protected from other third parties. Modern cryptography focuses on developing cryptographic algorithms that are hard to break against adversary attacks. However, a party has mutually sharing secret key, and the encryption and decryption operations have high computation cost. In additional, if several participants want to share one secret information, then key management has a problem that doesn't know whose access to the secret data. Therefore, the secret sharing scheme proposed to solve these problems [1-3].

Blackey [4] and Shamir [5] first proposed each secret sharing scheme in 1979. Their concept is that encodes a secret data, and distribute to *n* participants, where any *t* or more ~~of the~~ shares can be collected to recover the secret data. However, any *t* - 1 or fewer of them will gain no information about it.

In 2002, Thien and Lin [6] proposed a secret image sharing using steganography and Shamir's scheme. Because a pixel of image is 8-bit (between 0 and 255), this scheme used the prime number *p* be 251 which is the largest prime value less than 255. However, exceed pixel values (251~255) of the secret image change to 250, then recovered secret image occurs to a distortion. In addition, their method generates meaningless (noise) images that attract attention of the malicious users.

In 2004, Thien and Lin [7] proposed to share user-friendly shadow images which are a shrunken version of the secret image. However, the recover image is low quality because the perfect reconstructed image cannot get from the extraction process. At the same year, Lin and Tsai [8] proposed a new type scheme using steganography to embed shared data into a cover image. Their scheme used the parity bits for authentication, and embeds 8 secret bits into a 2×2 pixel of cover block using LSB method. In 2007, Yang et al. [9] used hash functions to authenticate stego images because the parity bit is not an appropriate way for an authentication mechanism. In additional, they use to prevent

* Corresponding author (Tel.:+82-53-950-5553) yook@knu.ac.kr

ISSN: 1738-9976 IJSIA

distortion of the secret image using Galois Fields. In 2008, Chang *et al.*'s [10] scheme proposed to improve a single authentication bit and a poor visual quality of the shadow images. They use the CRT for improving the authentication ability and enhancing the quality of shadow image [11]. In 2010, Lin and Chan [12] proposed a reversible secret image sharing scheme using modulus operation. Their scheme embeds a secret data and the remained value of cover pixel to coefficients of polynomial for improving the embedding capacity.

This paper proposes a new secret image sharing scheme without polynomials and Lagrange interpolation operations. The proposed scheme is to generate a histogram through computes a difference between cover and copy images. The generated histogram decides to peak and zero points pair, and shifts according to a secret bit. *n* shadow images are distributed to *n* participants. In experimental results, we compare the proposed scheme with a previous scheme about embedding capacity and the image distortion.

The rest of this paper is organized as follows. Section 2 introduces histogram shifting, and Lin and Chan's scheme. The new reversible secret image sharing scheme is elaborated in Section 3, followed by the experimental results and performance analyses in Section 4. Finally, Section 5 presents conclusions.

2. Related Works

2.1. Histogram Shifting

Ni *et al.* [13] proposed the histogram shifting using the frequency of a cover image. Their scheme has points which are a peak point (maximum frequency) and a zero point (minimum frequency). The points are shifting from the peak point to a zero point according to a secret bit. If a secret bit is 1, then the peak point is shifting to zero point. Otherwise, the peak point is not moved. In extraction phase, the secret bit gets from a zero point and a peak point. The shifted values are moving 1 bit from a zero point to a peak point. Although the previous data hiding technique is not recover after extraction secret bit, the histogram shifting [14~18] can be recover cover image. However, the embedding capacity is limited by the peak point. Since then, a histogram shifting scheme is to study about improving to the embedding capacity using the difference expansion [19].

2.2. Lin and Chan's Scheme

Lin and Chan (*LC*) scheme is proposed to reversible secret image sharing based on Shamir's scheme. In *LC* scheme, the dealer converts the pixel values of the secret image (*S*) into the p system, and selects to a unique key (K_i) for each participant, where $i = 1, 2, \dots, n$. To increase the embedding capacity, the secret data is to hide the secret digits s_1, s_2, ... , s_{t-1} of the polynomial, and the remainder of pixel value of cover is insert to *d* of polynomial for preserving. It is as following the equation (1).

$$f(x) = (d + s_0 x + s_1 x^2 + \cdots + s_{t-2} x^{t-1}) \bmod p \quad (1)$$

After then, each participants get the shadow image witch add the quantized pixel value of cover image and the hiding data to form a camouflaged pixel.

Given any *t* out of *n* shadow images and the key k_j from the involved participants, the secret image *S* and the lossless cover image can be reconstructed. The pixel value of shadow images is the corresponding pixel value of cover image. To extract the secret data and to recover original image, participants must derive the polynomial. The polynomial $F(x)$ can be reconstructed by Lagrange's interpolation formula as following equation (2).

$$a(x) = \sum_{j=1}^{t} \left(y_j \prod_{1 \le o \le t, o \ne t} \frac{x - x_o}{x_j - x_o} \right) \quad (2)$$

where x_j and x_0 are unique sequence of participants, y_j is a corresponding value at $a(x)$, and p is prime.

However, Lin and Chan's scheme have some problems. First, in general secret image sharing scheme, the number of participants is always less than the prime of polynomial. Therefore, the number of participant is less than 13. The second, the overflow can be occurred sometimes when a modified pixel value is more than 250 (p = 7).

3. The Proposed Scheme

This section proposes a new (n, n)-threshold reversible secret image sharing using histogram shifting. The proposed scheme is divided to two phases. One is embedding secret data and distribute shadow images to n participants. The other is that the secret image S and the lossless cover image can be reconstructed by using n shadow images.

3.1. Distributing Phase

The secret image sharing process is as following. The size of a cover image is $M \times M$, and the embedding capacity is decided by the size of cover image and k-bits. It is the secret bits to embed into a cover image. Therefore, the peak points can shift until 2^k-1.

Input: C, S, and k
Output: n shadow images (Sh_1, $Sh_{2, \ldots,}$ Sh_n)

Step 1: load a cover image and copy n-1 times.

$$C_{n-1(i,j)}{}' = Copy(C_{(i,j)}),$$

where $(0 \le i, j \le M)$, n is the number of participants.

Step 2: Generate a histogram by using difference $d_{(i,j)}$ between $C_{(i,j)}$ and $C_{n\text{-}1(i,j)}{}'$. The peak point of generated histogram is always 0 and the zero point selects 2^k-1.

$$d_{(i,j)} = \left| C_{(i,j)} - C_{n-1(i,j)}{}' \right|$$

Step 3: Convert the pixel value of S into binary system before the embedding. For example, when the pixel values of S are 162 and 165, the binary values are $10100010_{(2)}$ and $10100101_{(2)}$.

Step 4: Embeds the k-bit to the pixel value of l-th column of C_n by using $LSB(k)$ where l is $(1 \le l \le n)$. If the secret bit is same the peak point, then peak point is fixed. In the otherwise, the peak point is shifting to the value of secret bit. The maximum shift value is 2^k-1. Figure 1 shows the example of (3, 3)-threshold proposed scheme.

Step 5: Distribute shadow images (Sh_0, $Sh_{1, \ldots,}$ Sh_n) to n participants.

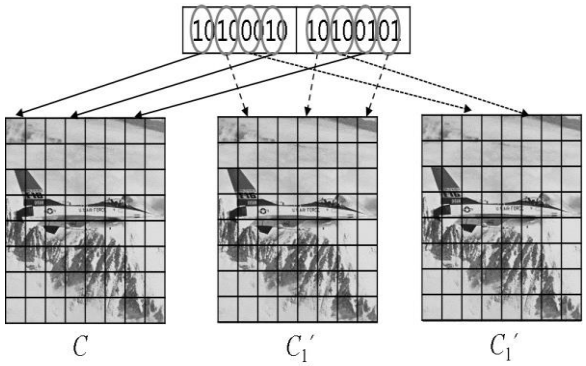


Figure 1. An Example of a Distribution Phase of (3, 3)-*threshold* Proposed Scheme

3.2. Reconstruct Phase

The previous histogram shifting must need to additional information about the peak and zero points. However, the proposed scheme does not need additional information. We can compute the *k* by using difference between shadow images. In addition, it can reconstruct the cover image.

Input: *n* shadow images (Sh_1, $Sh_{2, \ldots,} Sh_n$)
Output: Extracted secret image (S') and reconstructed cover image (C')

***Step* 1**: Generate a histogram by using difference $d_{(i,j)}'$ between *n* shadow images (Sh_1, $Sh_{2, \ldots,} Sh_n$).

$$d_{(i,j)}' = \left| Sh_{1(i,j)} - Sh_{2(i,j)} - \cdots - Sh_{n(i,j)} \right|$$

***Step* 2**: Generate a histogram using $d_{(i,j)}'$. The peak point is always 0 and the zero point can get using histogram. The maximum value of histogram is 2^k-1.

***Step* 3**: Extract the *k*-bit to the pixel value of *l-th* column of Sh_n by using *LSB*(*k*) where *l* is $(1 \le l \le n)$. If the secret bit is same the peak point, then peak point is fixed and extract 0. In the otherwise, 1 extract from the shadow and the value of histogram is shifting to the peak point.

***Step* 4**: Reconstruct a cover image by using unchanged pixel of shadow images.

Figure 2 shows an example of step 2 and step 3. Figure 3 shows an example of a reconstruct cover image.

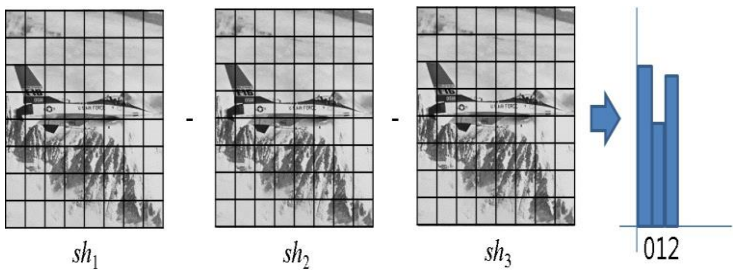


Figure 2. An Example of Step 2 and Step 3 (*k* = 2)

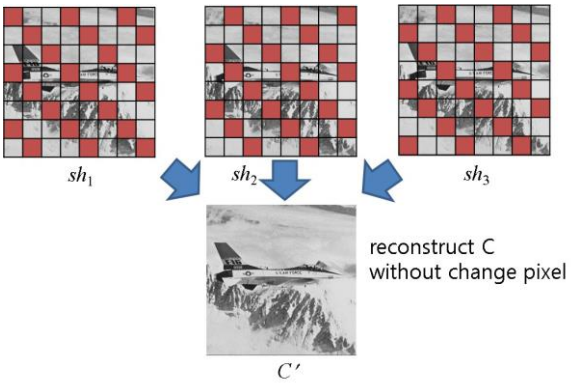


Figure 3. An Example of a Reconstruct Cover Image

4. The Experimental Results

In this section, the proposed scheme is compared with Lin and Chan's scheme in terms of the embedding capacity and image distortion. Peak Significant Noise Ratio (*PSNR*) measures the distortion between the cover image and a shadow image, and defines as follows equation (3).

$$PSNR = \left(10 \log_{10} \left(\frac{255^2}{MSE} \right) \right), \tag{3}$$

where *MSE* is the Mean Square Error between the cover image and ~~a~~ shadow images, and can be calculated by using the following equation (4). The *MSE* of an image with size $M \times M$ pixels is define as

$$MSE = \left(\frac{1}{M \times M} \sum_{i=1}^{M} \sum_{j=1}^{M} \left(I_{(i,j)} - I_{(i,j)}' \right)^2 \right), \tag{4}$$

where $I_{(i,j)}$ and $I_{(i,j)}'$ indicate pixel values of the cover and ~~a~~ shadow images with size $M \times M$. If PSNR was less than 35*dB*, these are difficult to distinguish the distortion in the human visible system (HVS) [20-23].

The embedding capacity is the maximum number of secret bits to hide in a cover image. The embedding capacity of the proposed scheme is determined by *k*-bit. The measurement unit of embedding capacity is defined by bit per pixel (bpp). In the experiment, six gray-scale cover images with size of 256 × 256 as shown in Figure 4 are used. When *k* select 1 to 4, the maximum embedding capacity of secret image is each 128×64, 128×128, 192×128, 256×128 as shown in Figure 5.

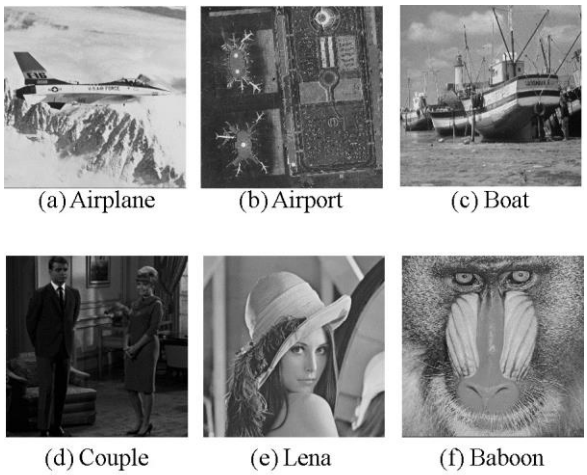


Figure 4. Six Cover Images of 256×256

Figure 5. Four Secret Images: (a) 128×64 (*k* = 1), (b) 128×128 (*k* = 2), (c) 192×128 (*k* = 3), (d) 256×128 (*k* = 4)

4.1. The Estimation of Peak Significant Noise Ratio

In the experiment, the proposed scheme was tested for (3, 3)-threshold. Lin and Chan's scheme was tested for *p* is 7 because of best case. Figure 6 and 7 shows the original secret image and restored secret image, and the original cover image and recovered cover image, respectively. In Figure 6 and 7, each image has the same image quality, that is, the original image exactly was restored. Figure 7 shows PSNR value of generated shadow images in the proposed scheme. Figure 8 shows the shadow images which change according to increase the *k*.

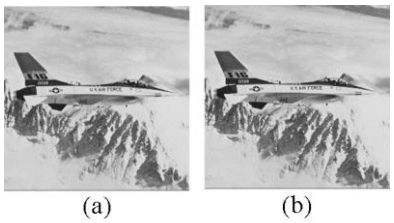


Figure 6. Cover Images: (a) Original, (b) Recovered

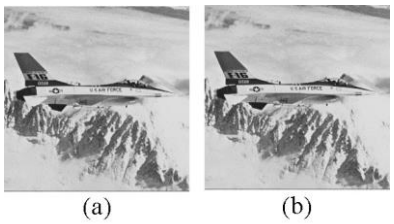


Figure 7. Shadow Images: (a) Sh_1, (b) Sh_2

Figure 8. The Shadow Images which Change According to Increase the *k*

Table 1 shows the comparison of PSNR between the proposed and Lin and Chan's schemes with (3, 3)-threshold. In Table 1, the qualities of shadow images in the proposed scheme are higher than their scheme. Although *n* (that is, the number of participants) was increased, the qualities of generated shadow images in the proposed scheme always are higher than their scheme.

Table 1. The Comparison of PSNR between LC Scheme and the Proposed Scheme with (3, 3)-threshold

Cover	LC	Proposed			
	$p = 7$	$k = 1$	$k = 2$	$k = 3$	$k = 4$
Airplane	40.43	55.85	48.88	42.98	34.19
Airport	40.02	55.9	48.9	42.93	34.19
Baboon	40.17	55.88	48.86	42.92	34.16
Boat	40.31	55.93	48.73	42.92	33.96
Couple	40.4	55.92	48.78	42.97	34.44
Lena	40.45	55.94	48.87	42.94	34.15
Average	40.30	55.90	48.84	42.94	34.18

4.2. The Estimation of Embedding Capacity

The embedding capacity of Lin and Chan's scheme is related by *t*, *p* and a size of the cover image ($M \times M$). If p is increased, then the embedding capacity also is increased. For example p is 7, then the embedding capacity is $((t-1) \times M \times M)/3$. However, PSNR is decreased with the increase of embedding capacity. In addition, n participants cannot be over *p*. In other words, *n* is always less than *p*. If *p* is greater than 11, then PSNR values of shadow images were less than 35dB. Therefore, their scheme has trade-off between the embedding capacity and PSNR according to the number of participants.

In the proposed scheme, the embedding capacity is decided to *k*-bits and a size of cover image. The embedding capacity of the proposed scheme is ($k \times M \times M$) that higher than that those of the LC scheme. Table 2 shows the comparison of embedding capacity between LC and the proposed schemes with (3, 3)-threshold.

Table 2. The Comparison of Embedding Capacity between LC and the Proposed Schemes with (3, 3)-threshold

Cover	LC	Proposed			
	$p = 7$	$k = 1$	$k = 2$	$k = 3$	$k = 4$
128×128	10,923	16,384	32,768	49,152	65,536
256×256	43,691	65,536	131,072	196,608	262,144
512×512	174,763	262,144	524,288	786,432	1,048,576

5. Conclusions

This paper proposed a new (*n*, *n*)-threshold reversible secret image sharing scheme using a histogram shifting. The proposed scheme can reversible cover image using simple operation. In addition, the overflow problem of LC scheme is solved by *LSB*.

In experimental results, we had estimated at (*n*, *n*)-threshold about embedding capacity and a distortion. Lin and Chan's scheme had best result in $p = 7$. However, the proposed scheme was embedding capacity and image quality higher than LC scheme.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (NRF-2012R1A1A2008348) and the IT R&D program of MSIP/KEIT. [10041145, Self-Organized Software platform (SoSp) for Welfare Devices].

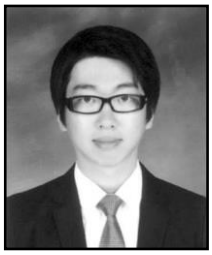
References

[1] J. H. B. Li, J. He and Y. Shi, "A survey on image steganography and steganalysis", Information Hiding and Multimedia signal Processing, vol. 2, no. 2, **(2011),** pp.142-172
[2] P. Li, C.-N. Yang, C.-C. Wu, Q. Kong, and Y. Ma, "Essential secret image sharing scheme with different importance of shadows", Journal of Visual Communication and Image Representation, vol. 27, no. 7, **(2013)**, pp. 1106–1114.
[3] W. Stallings, "Cryptography and Network Security", Prentice Hall, Upper Saddle River, NJ, USA **(2010).**
[4] G. Blakley, "Safeguarding cryptographic keys", In Proc. International Workshop on the National Computer Conference, **(1979)**, pp. 313-317.
[5] A. Shamir, "How to share a secret", Communications of the ACM, vol. 22, no. 11, **(1979)**, pp. 612-613.
[6] C. Thien and J. Lin, "Secret image sharing. Journal of Computers and Graphics", vol. 26, no. 5, **(2002)**, pp. 765-770.
[7] J. C. L. Y.-S. Wu and C.-C. Thien, "Sharing and hiding secret images with size constraint", Pattern Recognition, vol. 37, no. 7, **(2004)**, pp. 1377-1385.
[8] C. Lin and W. Tsai, "Secret image sharing with steganography and authentication", Journal of Systems and Software, vol. 73, no. 3, **(2004)**, pp. 405-414.
[9] K. Y. C. N. Yang, T. S. Chen and C. Wang, "Improvements of image sharing with steganography and authentication", The Journal of Systems and Software, vol. 80, **(2007)**, pp. 1070-1076.
[10] Y. H. C. C. Chang and C. Lin, "Sharing secrets in stego images with authentication", Journal of Pattern Recognition, vol. 41, no. 10, **(2008)**, pp. 3130-3137.
[11] S. Shyu and Y. Chen, "Threshold secret image sharing by chinese remainder theorem", In IEEE Asia-Pacific Services Computing Conference, **(2008)**, pp. 332-1337.
[12] P. Lin and C. Chan, "Invertible secret image sharing with steganography", Journal of Pattern Recognition Letters, vol. 31, no. 13, **(2010)**, pp. 1887-1893.
[13] N. A. Z. Ni, Y. Q. Shi and W. Su, "Reversible data hiding", IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 3, **(2006)**, pp. 354-362.
[14] S. Bae, "A high capacity reversible watermarking using histogram shifting", Journal of Korea Multimedia Society, vol. 13, no. 1, **(2010)**, pp. 76-82.
[15] Y. H. P. Tsai and H. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting", Signal Processing, vol. 89, no. 6, **(2009)**, pp. 1129-1143.
[16] J. L. P.Y. Lin and C. Chang, "Distortion-free secret image sharing mechanism using modulus operator", Journal of Pattern Recognition, vol. 42, no. 5, **(2009)**, pp. 886-895.
[17] J. Tian, "Reversible watermarking by difference expansion", IEEE Transactions on Circuits and System for Video Technology, vol. 13, no. 8, **(2003)**, pp. 890-896.
[18] Y. Lee and J. Kim, "Histogram Rotation-Based Image Watermarking with Reversibility", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 197-202.
[19] Y. H. C. C. Chang and C. Lin, "Sharing secrets in stego images with authentication", Journal of Pattern Recognition, vol. 41, no. 10, **(2008)**, pp. 3130-3137.
[20] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital Watermarking and Steganography", Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, **(2008).**
[21] J. Waleed, H. D. Jun and S. Hameed, "A robust Optimal Zero-Watermarking Technique for Secret Watermark Sharing", International Journal of Security and Its Applications, vol. 8, no. 5, **(2014)**, pp. 349-360.

[22] B. Surekha and G. N. Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications, vol. 5, no. 1, **(2011)**, pp. 1-12.
[23] P. Tsai, Y.-C. Hu, H.-L. Yeh and W.-K. Shih, "Watermarking for Multi-resolution Image Authentication", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 161-166.

Authors

Gil-Je Lee, he is currently a Ph.D. candidate in School of Computer Science and Engineering at Kyungpook National University. He received B.S. degree from Kyungil University in 2007, the M.S. 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.



Dae-Soo Kim is currently a Ph.D. candidate in School of Computer Science and Engineering at Kyungpook National University. He received B.S. degree from Catholic University of Daegu in 2010, the M.S. degree from Kyungpook National University in 2012. His current research interests are steganography, digital watermarking, and data hiding.

Kee-Young Yoo is currently a professor in School of Computer Science and Engineering at Kyungpook National University. He received B.S. degree from Kyungpook National University in 1976, the M.S. degree from Korea Advanced Institute of Science and Technology in 1978 and the Ph.D. degree from Rensselaer Polytechnic Institute, New York, U.S.A., in 1992. His current research interests are cryptography and information hiding.