Perceptual Secret Sharing Scheme Based on Boolean Operations and Random Grids

Xuehu Yan(✉), Yuliang Lu, Lintao Liu, Song Wan, Wanmeng Ding, and Hanlin Liu

Hefei Electronic Engineering Institute, Hefei 230037, China
publictiger@126.com

Abstract. In this paper, a new perceptual secret sharing (PSS) scheme is developed based on Boolean operations and random grids. In the developed scheme, the secret image is shared among n shadows using (l, n, n) threshold scheme, while the restored secret image is restored from l out of n shadows. $P(l, n, n)$ threshold is satisfied in this developed scheme, by acquiring this property no information recovery occurs when less than l shares are stacked, imperfect recovery occurs when more than l but less than n shares are presented and perfect recovery occurs when n shares are collected.

Keywords: Visual secret sharing · Perceptual secret sharing
Threshold · Boolean operations · Random grids

1 Introduction

In many applications like Pay- TV/Music and art-work image vending, pay-per-view video on demand (VOD), a feature of "perceptual secret sharing (*PSS*)" is very useful [1]. The *PSS* model is defined as the secret sharing scheme that degrades the quality of media data according to quality or security requirements [1–4] and recovers the secret lossless when sufficient shares are collected.

Secret image sharing technique is one alternative method to protect the secret images. It assigns a secret image among some owners by encrypting the secret image into noise-like shadows (also called shares or shadow images) and restoring the secret image by obtaining sufficient authorized owners (shadows). It attracted more attention of engineers and scientists. Visual secret sharing (VSS) [5,6] (also called visual cryptographic scheme (VCS)) is one primary branch in this domain.

The main properties of traditional VCSs [3,5–7] are free order of the shadows and simple recovery, i.e., the restoration of secret image is only based on human vision system (HVS) with no any cryptographic computation. Unfortunately, these schemes suffer from lossy recovery, pixel expansion or codebook design. Although VCSs by random grids (RG) [8–12] have no pixel expansion or complex codebook, they are lossy recovery. Progressive secret sharing methods, based on the ideas of VCS [13–16], RG [17], and Shamir's polynomial [18] or in transform domain [19], have perceptual quality for the restored secret image when more

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2018
M. Huang et al. (Eds.): WICON 2016, LNICST 214, pp. 80–90, 2018.
https://doi.org/10.1007/978-3-319-72998-5_9

shadows are obtained. Unfortunately, they overall suffer from limitations such as the pixel expansion, poor visual quality of the restored secret image or lossy recovery.

It is noted that the aforementioned schemes could not satisfy the properties of *PSS* that is mentioned previously. Recently, in [1], a (l, k, n) threshold *PSS* model is defined, and a $(1, k, n)$ threshold *PSS* by maximum likelihood estimation (MLE) was developed, which could satisfy $P(1, k, n)$ threshold. Unfortunately, the scheme has complex computation in the recovery phase, and shadows have a little cross interference of the secret which may be not secure in some applications.

In this paper, a new perceptual secret sharing (*PSS*) scheme is developed to improve the security with low computational complexity of traditional PSS [1]. In the new scheme, a (l, n, n) threshold *PSS* scheme is developed based on Boolean operations (Boolean XOR and stacking operations) and RGs through utilizing the random bits to obtain better features, such as threshold and lossless recovery. The secret image is generated into n RGs, then the restored secret image is restored from l *out of* n shadows. The developed scheme has lower computational complexity with no cross interference of secret image. It satisfies $P(l, n, n)$ threshold and by acquiring this property no information recovery occurs when less than l shares are stacked, imperfect recovery occurs when more than l but less than n shares are present and perfect recovery occurs when n shares are collected. In addition, the developed scheme can realize other features such as lower computational complexity, free order of shadows in recovery, no pixel expansion and no codebook design. Experimental results and analyses indicate the feasibility and effectiveness of the developed scheme.

The rest of this article is stated as follows. The basic definitions and preliminaries are illustrated in Sect. 2. The developed (l, n, n) threshold *PSS* scheme is given in Sect. 3. Section 4 focuses on the experimental results and analyses. Finally, Sect. 5 concludes this article.

2 Definitions and Preliminaries

In this section, we illustrate some fundamental definitions and preliminaries for the developed scheme. Symbols $\oplus$, & and $\otimes$ denote the Boolean XOR, AND and OR operations, respectively. $\overline{x}$ indicates a bit-wise complementary operation of any bit x. A binary secret image S is generated among n (generally $2 \leq \text{n} \leq 5, n \in \text{Z}^+$) shadows, and the restored secret image S' is restored from any $t (2 \leq t \leq n, t \in \text{Z}^+)$ shadows based on stacking or Boolean XOR operations.

2.1 Fundamental Definitions [1]

Definition 1 ***(PSS)*:** The original binary secret image is represented by S whose pixel value denoted as $S(i,\ j)\quad (1 \leq i \leq M, 1 \leq j \leq N),\ size\,(S) = (M, N)$, where function *size* tells size of S. For a *P(l, k, n) PSS*, the binary secret

image S is generated into n $(2 \leq n, n \in \mathrm{Z}^+)$ shadows $SC_1, SC_2, \cdots SC_n$ according to generation function (Gf), $(SC_1, SC_2, \cdots SC_n) = Gf(S, l, k, n) 1 \leq l \leq k \leq n$; Then the restored secret image S' is restored from any t $(1 \leq t \leq n, t \in \mathrm{Z}^+)$ shadows by recovery function (Rf), i.e., $S'_t = Rf(SC_{i_1}, SC_{i_2}, \cdots SC_{i_t})$, where $(i_1, i_2, \cdots, i_t)$ demonstrates a subsequence of $(1, 2, \cdots, n)$. $VQ(S'_t)$ means the perceptual visual quality of the restored secret image S'_t. A *P(l, k, n) PSS* satisfies:

$$VQ(S'_t = Rf(SC_{i_1}, SC_{i_2}, \cdots SC_{i_t})) = 0 t < l;$$

$$VQ(S'_{t_2}) \geq VQ(S'_{t_1}) > 0 k \geq t_2 \geq t_1 \geq l; S'_t = Rf(SC_{i_1}, SC_{i_2}, \cdots SC_{i_t}) = S t \geq k.$$

Restoring function Rf is simple.

$S'_{t_m} = Rf(SC_{i_{m_1}}, SC_{i_{m_2}}, \cdots SC_{i_{m_t}}) = S'_t = Rf(SC_{i_1}, SC_{i_2}, \cdots SC_{i_t})$, where $(m_1, m_2, \cdots, m_t)$ denotes a permutation of $(1, 2, \cdots, t)$.

$$size(S') = size(SC_i) = size(S), i = 1, 2, \cdots, n$$

Gf and Rf don't have extra codebook besides the parameters and input images.

Here "1" means white pixel and "0" is black pixel, which is the same as digital multimedia.

Definition 2 (Contrast, denoted as α) [9]: In *PSS*, the visual quality of the restored secret image S'_t, which can decide how well human eyes will recognize the restored image, for the secret image S is evaluated by contrast given as follows:

$$\frac{P_1 - P_0}{1 + P_0} = \frac{P(S'[AS1] = 1) - P(S'[AS0] = 1)}{1 + P(S'[AS0] = 1)} \tag{1}$$

where P_0(resp., P_1) illustrates appearance probability of white pixels in the restored image S' in the corresponding black (resp., white) area of the secret image. $SAS0$ (resp., $AS1$) tells the black (resp., white) area of the secret image S as $S0 = \{(i, j) | S(i, j) = 0, 1 \leq i \leq M, 1 \leq j \leq N\}$(resp., $S1 = \{(i, j) | S(i, j) = 1, 1 \leq i \leq M, 1 \leq j \leq N\}$).

Definition 3 (Visually recognizable and security) [5]: The restored secret image S' will be recognized as the content of the secret image S if $\alpha > 0$. The scheme is secure if $\alpha < 1$ when $l \leq t < k$ which tells part of secret (including content and details) of S can be recognized from S'; $\alpha = 0$ when $t < l$ indicating no any secret (including content and details) of S will be recognized from S'. The restored secret image S' is lossless when $\alpha = 1$ under $t \geq k$, which tells all secret information (including content and details) of S is recognized from S'.

2.2 RG-Based VSS

In RG-based VSS [10], "0" means white pixel, "1" is black pixel. The generation and restoration phases of an original (2, 2) RG-based [10] VSS will be given below.

Step 1: Generate 1 RGSC_1 randomly.

Step 2: Compute SC_2 according to Eq. (2).

Restoration: $S' = SC_1 \otimes SC_2$ as Eq. (3). If a certain pixel $s = S(i,j)$ of S is 1, the restoration result $SC_1 \otimes SC_2 = 1$ will be always black. If a certain pixel is 0, the restoration result $SC_1 \otimes SC_2 = SC_1(i,j) \otimes SC_1(i,j)$ will have half chance to be black or white since SC_1 is random.

$$SC_2(i,j) = \begin{cases} SC_1(i,j) & if\ S(i,j) = 0 \\ \overline{SC_1}(i,j) & if\ S(i,j) = 1 \end{cases} \tag{2}$$

$$S'(i,j) = SC_1(i,j) \otimes SC_2(i,j) = \begin{cases} SC_1(i,j) \otimes SC_1(i,j) & if\ S(i,j) = 0 \\ SC_1(i,j) \otimes \overline{SC_1}(i,j) & = 1\ if\ S(i,j) = 1 \end{cases} \tag{3}$$

The same approach will be extended to (l,n) threshold through applying the above process repeatedly on the first l bits and setting the last $n-l$ bits randomly.

In addition, [12] improves the contrast of [10] through changing the last $n-l$ bits to be equal to the lth bit. However, the schemes in [10,12] are lossy. Besides, the color representation is different from that of digital images, which will not be convenient in digital images applications. Hence, a (2, 2) threshold scheme is used first as an example to show the main idea of the same color representation. The generation and restoration phases are given below, where "1" means white pixel and "0" is black pixel, which are the same as that of digital images.

Step 1: Generate 1 RGSC_1 randomly.

Step 2: Compute SC_2 as Eq. (4).

Restoration: $S' = SC_1 \& SC_2$ as in Eq. (5). If a certain pixel of $S(i,j)$ is 0, the restoration result $SC_1 \& SC_2 = 0$ will be always black. If a certain pixel of $S(i,j)$ is 1, the restoration result $SC_1 \& SC_2 = SC_1(i,j) \& SC_1(i,j)$ will have half chance to be black or white due to SC_1 are random.

$$SC_2(i,j) = \begin{cases} SC_1(i,j) & if\ S(i,j) = 0 \\ \overline{SC_1}(i,j) & if\ S(i,j) = 1 \end{cases} \tag{4}$$

$$S'(i,j) = SC_1(i,j) \& SC_2(i,j) = \begin{cases} SC_1(i,j) \& SC_1(i,j) & if\ S(i,j) = 1 \\ SC_1(i,j) \& \overline{SC_1}(i,j) & = 0\ if\ S(i,j) = 0 \end{cases} \tag{5}$$

Equations (2) and (4) focus on the generation phase of one secret bit $S(i,j)$, and Eqs. (3) and (5) the restoration phase. The difference of Eqs. (2) and (4) lies in the color representation method. Equations (3) and (5) utilize different restored operations.

3 The Developed PSS Scheme

In this section, we introduce a novel *PSS* scheme based on Boolean operations and RG to realize the *PSS* model defined in Sect. 2. Performance analyses are performed to show security of the developed scheme. Here "1" denotes white

pixel, "0" denotes black pixel, which are the same as the color representation method of digital images.

Before giving the details of the developed scheme, the principal of the developed scheme is stated as follows: (l, n) threshold RG-based VSS is applied to obtain (l, n) threshold first. Then the random bits in the n bits are utilized to gain lossless restoration.

3.1 Shadows Generation and Restoration Phases

The shadows generation designed concept is in Fig. 1, whose algorithmic steps are given in Algorithm 1.

The secret restoration algorithmic steps are in Algorithm 2.

The ideas of Algorithms 1 and 2 are discussed precisely as follows:

Some random bits in the n bits corresponding to the n shadows. The random bits will be utilized to obtain better properties, e.g., threshold mechanism, improved visual quality and lossless restoration. In Step 2 of Algorithm 1, the l bits are utilized to achieve threshold mechanism [10], i.e., when less than l shadows are obtained, the secret cannot be restored. Step 2 in Algorithm 1 aims at improving the visual quality of restored secret image [12]. Flipping one of the last $n - l$ bits in step 5 of Algorithm 1 aims at satisfying $S(i, j) = b_1 \oplus b_2 \oplus \cdots \oplus b_n$, i.e., to be lossless restoration in Step 2 of Algorithm 2. Hence, the developed scheme is PSS (*l,n,n*). In step 6 of Algorithm 1, in order to make all the shadows be equal to each other, i.e., owning the same importance, the outputted n bits are randomly rearranged to n shadows bits.

Algorithm 1. The developed *PSS (l, n, n)* scheme.

Input: A binary secret image S with size of $M \times N$, threshold parameters *PSS (l, n, n)*

Output: n generated shadows $SC_1, SC_2, \cdots SC_n$

Step 1: For each position$(i, j) \in \{(i, j)|1 \le i \le M, 1 \le j \le N\}$, i.e., $S(i, j)$, repeat Steps 2–6.

Step 2: Compute $b_1, b_2, \cdots b_l$ one by one repeatedly using Eq.(4), i.e., set $\tilde{b}_1 = S\,(i, j)$ for $p = 1, 2, \ldots, l - 1$, generate b_p randomly by flip-coin function. If $\tilde{b}_p = 0\tilde{b}_{p+1} = b_p$; otherwise, $\tilde{b}_{p+1} = \bar{b}_p$ Set $b_l = \tilde{b}_l$

Where b_x and $\tilde{b}_x$denote the temporary pixels, $x = 1, 2, \ldots, n - 1, n$

Step 3: Set $b_{l+1} = b_l, b_{l+2} = b_l, \cdots b_n = b_l$

Step 4: If $n > l$, go to Step 5; else go to Step 6

Step 5: If $S(i, j) = b_1 \oplus b_2 \oplus \cdots \oplus b_n$ go to Step 6; else randomly select $q \in \{l+1, \cdots, n\}$, flip $b_q = \overline{b_q}$(that is 0→1 or 1→0).

Step 6: The order of the n pixels $b_1, b_2, \cdots b_{n-1}, b_n$ are rearranged and the rearranged n pixels are assigned to $SC_1(i, j), SC_2(i, j), \cdots SC_n(i, j)$

Step 7: Output the n shadows $SC_1, SC_2, \cdots SC_n$

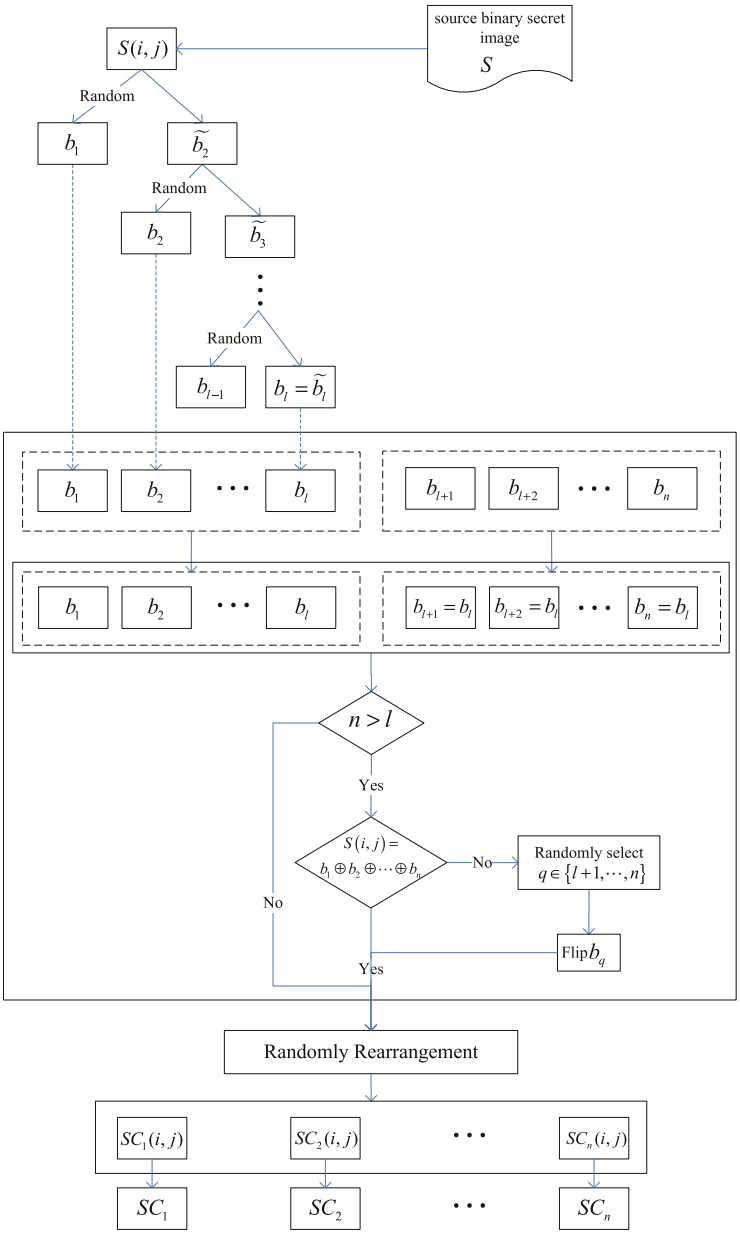


Fig. 1. Shadows generation design concept of our developed scheme

Algorithm 2. Secret image restoration of the developed scheme.
Input: any t shadows $SC_{j_1}, SC_{j_2}, \cdots SC_{j_t}$. **Output**: A $M \times N$ binary restored secret image S'
Step 1: If $t < n$, $S' = SC_{j_1} \& SC_{j_2} \& \cdots SC_{j_t}$ go to Step 3; else go to Step 2. **Step 2:** $S' = SC_{j_1} \oplus SC_{j_2} \oplus \cdots \oplus SC_{j_t}$ If $n = l, l \in 2Z^+$, $S' = \overline{S}'$; else go to Step 3. **Step 3:** Output the restored binary secret image S'.

4 Experimental Results and Analyses

Herein, we will perform experiments and analyses to demonstrate the effectiveness of our developed scheme. In the experiments, binary secret images with size of 512×512, are employed to do the test.

In our experiments, $PSS\ (3, 4, 4)$ (i.e. $l = 3, k = \ n\ = 4$) threshold with secret image1, $PSS\ (2, 5, 5)$ (i.e. $l = 2, k = \ n\ = 5$) threshold with secret image2, and $PSS\ (2, 3, 3)$ with secret image3 are employed.

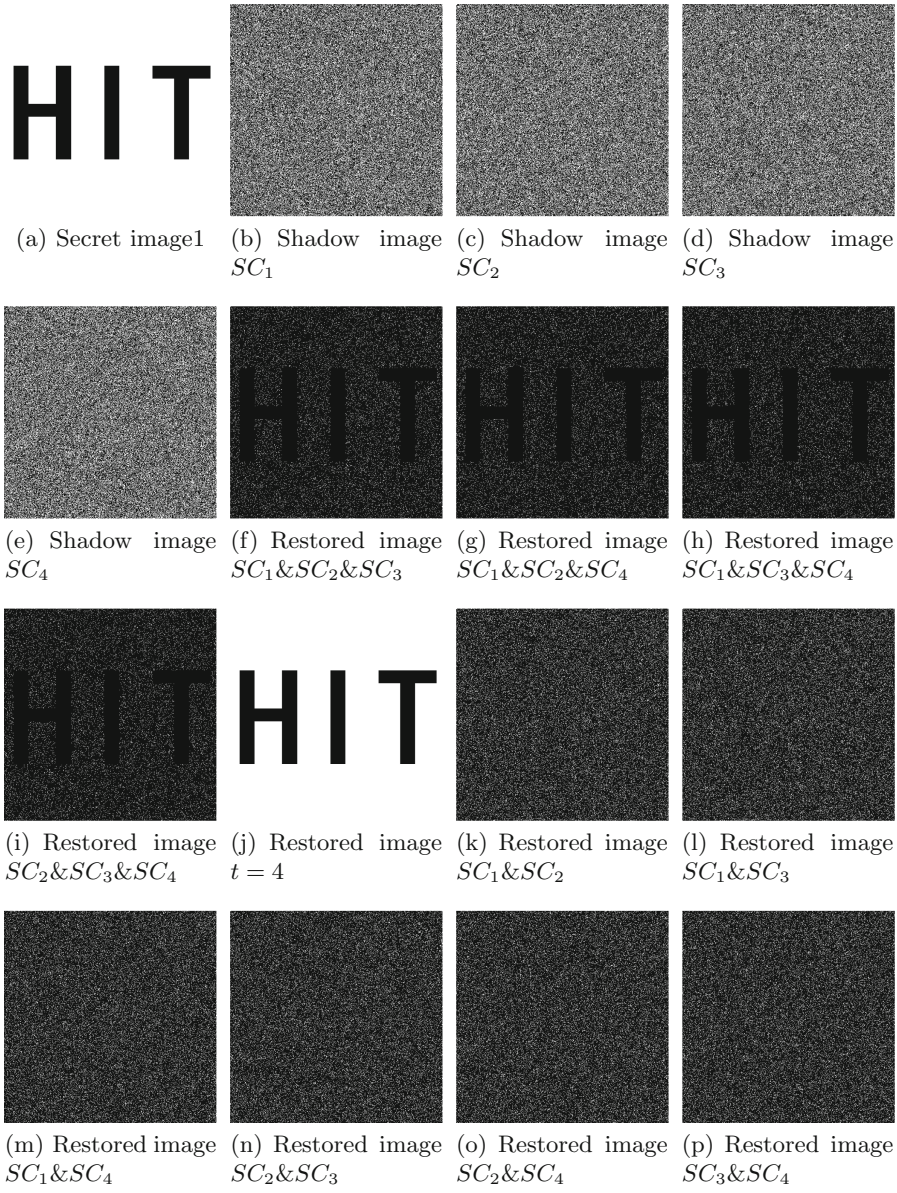
Figure 2(b–e) show the obtained 4 shadows SC_1, SC_2, SC_3 and SC_4 from binary secret image 1, which are noise-like. Figure 2(f–j) show the restored binary secret image with any 3 or 4 shadows, from which the secret image1 restored by $t = l = 3$ shadows can be recognized, and the secret image1 restored by $t = k = n = 4$ shadows is lossless. Figure 2(k–p) demonstrate the restored secret image with any less than l shadows, from which no information can be recognized.

In addition, we analysis the security of the developed $PSS\ (3, 4, 4)$ shown in Fig. 2 in terms of contrast, histogram and information entropy.

Contrast α is defined in Definition 2. Based on Definition 3, when $t < l\alpha = 0$ which means no information of S could be recognized through S'. Entropy is a statistical measure of randomness in information theory. The entropy $H(m)$ is computed as in Eq. (6) where $P(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each level. A good image encryption scheme should always generate a cipher image having uniform histogram for any plain image.

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i) * \log_2 p(m_i) \quad bits \tag{6}$$

The corresponding results for the shares and restored secret by 2 shadow images of Fig. 2 are shown in Fig. 3. Contrast is close to 0 which shows the satisfaction of Definition 3. Entropy of the shares agrees with the theory, while the histogram of shares doesn't which could be explained by Lemma 3. From Lemma 3, the black proportion will be greater than white one, which will not affect the security since the fixed pixel value has no relation with the secret bit. Neither entropy nor histogram of inadequate shadow images satisfies the theory, which are caused by Lemma 3 and the stacking restoration since stacking operation leads to more black ones. From the above results, we know that.



(a) Secret image1 (b) Shadow image SC_1 (c) Shadow image SC_2 (d) Shadow image SC_3

(e) Shadow image SC_4 (f) Restored image $SC_1\&SC_2\&SC_3$ (g) Restored image $SC_1\&SC_2\&SC_4$ (h) Restored image $SC_1\&SC_3\&SC_4$

(i) Restored image $SC_2\&SC_3\&SC_4$ (j) Restored image $t = 4$ (k) Restored image $SC_1\&SC_2$ (l) Restored image $SC_1\&SC_3$

(m) Restored image $SC_1\&SC_4$ (n) Restored image $SC_2\&SC_3$ (o) Restored image $SC_2\&SC_4$ (p) Restored image $SC_3\&SC_4$

Fig. 2. Experiments of our developed PSS(3, 4, 4) scheme for binary secret image1

(a) Histogram of 2(b) $\alpha = 0.001251$, $H = 0.954276$

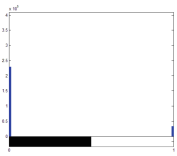
(b) Histogram of 2(c) $\alpha = 0.001114$, $H = 0.955240$

(c) Histogram of 2(d) $\alpha = 0.002910$, $H = 0.953924$

(d) Histogram of 2(e) $\alpha = -0.003670$, $H = 0.953958$

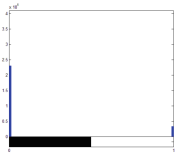
(e) Histogram of 2(h) $\alpha = 0.000365$, $H = 0.543222$

(f) Histogram of 2(l) $\alpha = 0.002406$, $H = 0.541924$



(g) Histogram of 2(m) $\alpha = -0.001580$, $H = 0.544014$

(h) Histogram of 2(n) $\alpha = 0.001338$, $H = 0.543039$



(i) Histogram of 2(o) $\alpha = -0.001429$, $H = 0.544570$

(j) Histogram of 2(p) $\alpha = -0.000238$, $H = 0.543661$

Fig. 3. Histogram analysis of developed *PSS* (3, 4, 4) scheme example shown in Fig. 2

- The shadows are noisy so that our developed scheme has no cross interference of the secret on shadows.
- When $t(l \leq t \leq k = n)$ shadows are obtained, the secret image will be recognized, and the image quality of restored secret image increases as t increases.
- When $t < l$ shadows are inspected, no information of the secret can be recognized, which demonstrates the security of our developed scheme.

5 Concluding Remarks

A simple and efficient perceptual secret sharing (PSS) scheme based on Boolean operations and RG is developed in this article. The developed scheme can satisfy valuable features in secret sharing. It satisfies $P(l, n, n)$ threshold sharing, which can achieve different perceptual quality as well as preserves the same color representation method as digital images. It also inherits conventional VSS

benefits, such as no pixel expansion or codebook. Furthermore, it has lower computational complexity as well as avoids the cross interference of secret on the shadows. Simulations results and analyses demonstrate the effectiveness of our developed scheme.

Acknowledgement. The authors would like to thank the anonymous reviewers for their valuable discussions and comments. This work is supported by the National Natural Science Foundation of China (Grant Number: 61602491).

References

1. Yan, X., Wang, S., El-Latif, A.A.A., Sang, J., Niu, X.: A novel perceptual secret sharing scheme. In: Shi, Y.Q., Liu, F., Yan, W. (eds.) Transactions on Data Hiding and Multimedia Security IX. LNCS, vol. 8363, pp. 68–90. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55046-1_5
2. Liu, F., Chuankun, W.: Embedded extended visual cryptography schemes. IEEE Trans. Inf. Foren. Secur. **6**(2), 307–322 (2011)
3. Wang, D.-S., Zhang, L., Ma, N., et al.: Two secret sharing schemes based on boolean operations. Pattern Recogn. **40**(10), 2776–2785 (2007)
4. Wang, Z., Arce, G.R.: Halftone visual cryptography through error diffusion. In: ICIP, pp. 109–112 (2006)
5. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053419
6. Weir, J., Yan, W.Q.: A comprehensive study of visual cryptography. In: Shi, Y.Q. (ed.) Transactions on Data Hiding and Multimedia Security V. LNCS, vol. 6010, pp. 70–105. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14298-7_5
7. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended capabilities for visual cryptography. Theoret. Comput. Sci. **250**(1/2), 143–161 (2001)
8. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Optics Lett. **12**(6), 377–379 (1987)
9. Shyu, S.J.: Image encryption by random grids. Pattern Recogn. **40**(3), 1014–1031 (2007)
10. Chen, T., Tsao, K.: Threshold visual secret sharing by random grids. J. Syst. Softw. **84**, 1197–1208 (2011)
11. Shyu, S.J.: Image encryption by multiple random grids. Pattern Recogn. **42**, 1582–1596 (2009)
12. Wu, X., Sun, W.: Improving the visual quality of random grid-based visual secret sharing. Signal Process. **93**(5), 977–995 (2013)
13. Jin, D., Yan, W.-Q., Kankanhalli, M.S.: Progressive color visual cryptography. J. Electron. Imaging **14**(3) (2005)
14. Hou, Y.-C., Quan, Z.-Y., Tsai, C.-F.: Block-based progressive visual secret sharing. Inf. Sci. **233**, 290–304 (2013)
15. Fang, W.-P., Lin, J.-C.: Progressive viewing and sharing of sensitive images. Pattern Recogn. Image Anal. **16**(4), 632–636 (2006)
16. Hou, Y.-C., Quan, Z.-Y.: Progressive visual cryptography with unexpanded shares. IEEE Trans. Circ. Syst. Video Technol. **21**(11), 1760–1764 (2011)

17. Chen, S.-K.: Friendly progressive visual secret sharing using generalized random grids. Optical Eng. **48**(11), 117001-1–117001-7 (2009)
18. Chen, S.-K., Lin, J.-C.: Fault-tolerant and progressive transmission of images. Pattern Recogn. **38**(12), 2466–2471 (2005)
19. Huang, C.-P., Hsieh, C.-H., Huang, P.S.: Progressive sharing for a secret image. J. Syst. Softw. **83**, 517–527 (2010)