Partial Secret Image Sharing for (n, n) Threshold Based on Image Inpainting

Xuehu Yan[1(✉)], Yuliang Lu[1], Lintao Liu[1], Shen Wang[2], Song Wan[1], Wanmeng Ding[1], and Hanlin Liu[1]

[1] Hefei Electronic Engineering Institute, Hefei 230037, China
publictiger@126.com
[2] School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China

Abstract. Shamir's polynomial-based secret image sharing (SIS) scheme and visual secret sharing (VSS) also called visual cryptography scheme (VCS), are the primary branches in SIS. In traditional (k, n) threshold secret sharing, a secret image is fully (entirely) generated into n shadow images (shares) distributed to n associated participants. The secret image can be recovered by collecting any k or more shadow images. The previous SIS schemes dealt with the full secret image neglecting the possible situation that only part of the secret image needs protection. However, in some applications, only target part of the secret image may need to be protected while other parts may be not in a full image. In this paper, we consider the partial secret image sharing (PSIS) issue as well as propose a PSIS scheme for (n, n) threshold based on image inpainting and linear congruence (LC). First the target part is manually selected or marked in the color secret image. Second, the target part is automatically removed from the original secret image to obtain the same input cover images (unpainted shadow images). Third, the target secret part is generated into the pixels corresponding to shadow images by LC in the processing of shadow images texture synthesis (inpainting), so as to obtain the shadow images in a visually plausible way. As a result, the full secret image including the target secret part and other parts will be recovered losslessly by adding all the inpainted meaningful shadow images. Experiments are conducted to evaluate the efficiency of the proposed scheme.

Keywords: Secret image sharing · Partial secret image sharing
Image inpainting · Linear congruence · Color image · Lossless recovery
Meaningful shadow images

1 Introduction

Through splitting the secret image into noise-like shadow images (also called shadows or shares), secret image sharing (SIS) distributes a secret image among multiple participants. The secret is recovered by collecting sufficient authorized

Y. Zhao et al. (Eds.): ICIG 2017, Part III, LNCS 10668, pp. 527–538, 2017.
https://doi.org/10.1007/978-3-319-71598-8_47

participants(shadow images). SIS can be applied in not only information hiding, but also access control, authentication, watermarking, and transmitting passwords etc. Shamir's polynomial-based scheme [1] and visual secret sharing (VSS) [2] also called visual cryptography scheme (VCS), are the primary branches in this field.

In Shamir's original polynomial-based (k, n) threshold SIS [1], the secret image is generated into the constant coefficient of a random $(k-1)$-degree polynomial to obtain n shadow images distributed to n associated participants. The secret image can be losslessly recovered by collecting any k or more shadow images based on Lagrange interpolation. Following Shamir's scheme and utilizing all coefficients of the polynomial for embedding secret, Thien and Lin [3] reduced share size $1/k$ times to the secret image. The advantage of Shamir's polynomial-based scheme [4–6] is lossless recovery. Shamir's polynomial-based SIS requires more complicated computations, i.e., Lagrange interpolations, for reconstructing and known order of shares, although the scheme only needs k shares for recovering the distortion-less secret image.

In (k, n) threshold VSS [7–13], the generated n shadow images are printed onto transparencies and then distributed to n associated participants. The beauty of VSS is that, the secret image can be revealed by superposing any k or more shadow images and human visual system (HVS) with no cryptographic computation. Less than k shares will reveal nothing about the secret except the image size. Inspired by Naor and Shamir's VSS work, the associated VSS physical properties and its problems are extensively studied, such as contrast [14], threshold [15], different formats [16], multiple secrets [6], noise-like patterns [11,17–20], pixel expansion [8,9,21,22] and so on [23,24].

In most of the existing SIS schemes, the full (entire) secret image is directly generated into the shadow images. The previous SIS schemes dealt with the full secret image neglecting the possible situation that only part of the secret image may need protection. However, there are many examples that only part of the secret image may need to be protected while other parts may be not in the same image, such as improving part design, sensitive information in part of a image and so on. One possible scenario is described as follows. On the basis of multiple traditional design modules in a product, a company improves one module design of them, while the other modules continue to use the traditional original design. At this point for the overall design drawing of this product, the improved module is needed to be protected and the other original modules can be public. Due to business privacy and access control, this product design drawing is kept by the company's n managers. Each manager can display the traditional modules in public display to facilitate the product introduction and other activities. In accordance with business needs, k or more managers together have the right to losslessly recover the full product design drawing including the improved module. In this scenario, we need protect target part of the secret image other than the full secret image as well as need access control with (k, n) threshold.

Thus, in some applications we may only need to encrypt part of the secret image rather than the full secret image for some reasons. However, the previous SIS schemes have not considered this issue. In order to deal with the partial secret image sharing (PSIS) issue, in this paper, we will introduce PSIS problem as well as propose a novel PSIS scheme for (n, n) threshold based on image inpainting [25,26] and linear congruence (LC) [27], where (n, n) threshold is a special case of (k, n) threshold under $k = n$. The target secret part of the color secret image is first manually selected and then automatically removed from the original color secret image to obtain the same input cover images (unpainted shadow images). Then, the target secret part is generated into the pixels corresponding to shadow images by LC in the processing of shadow images texture synthesis (inpainting), so as to obtain the shadow images in a way that looks reasonable to the human eye. As a result, the full secret image including the target secret part and the other parts will be recovered losslessly by adding all the inpainted meaningful shadow images. Experiments are conducted to evaluate the efficiency of the proposed scheme.

The rest of the paper is organized as follows. Section 2 introduces some basic requirements for the proposed scheme. In Sect. 3, the proposed scheme is presented in detail. Section 4 is devoted to experimental results. Finally, Sect. 5 concludes this paper.

2 Preliminaries

In this section, we give the PSIS problem description and some preliminaries as the basis for the proposed method. The original secret image S is shared among original total n shadow images, while the reconstructed secret image S' is reconstructed from t $(k \leq t \leq n, t \in \mathrm{Z}^+)$ shadow images.

2.1 Problem Definition

As show in Fig. 1, for the given secret image S in Fig. 1(a), Fig. 1(b) indicates the same input cover image C obtained by manually selecting and removing the target part from the original secret image S, where the notations of different parts and their edge are presented in Fig. 1(c). The region Ω is the target secret part (object), part Φ illustrates the untouched part, and $\partial\Omega$ denotes the edge of the 2 parts. Shadow images covered secret after sharing are denoted as $SC_i, i = 1, 2, ..., n$ for (k, n) threshold.

The PSIS problem can be described as follows: From the selected target part Ω and the associated cover images $C_1, C_2, \cdots C_n$, the PSIS scheme may generate n meaningful shadow images $SC_i, i = 1, 2, ..., n$ distributed to n associated participants, where each shadow image looks like a nature image. When any k or more shadow images are collected, the full secret image including the secret target part can be reconstructed. Whereas even if infinite computational power is available, less than k shadow images will reveal nothing about the secret target part.

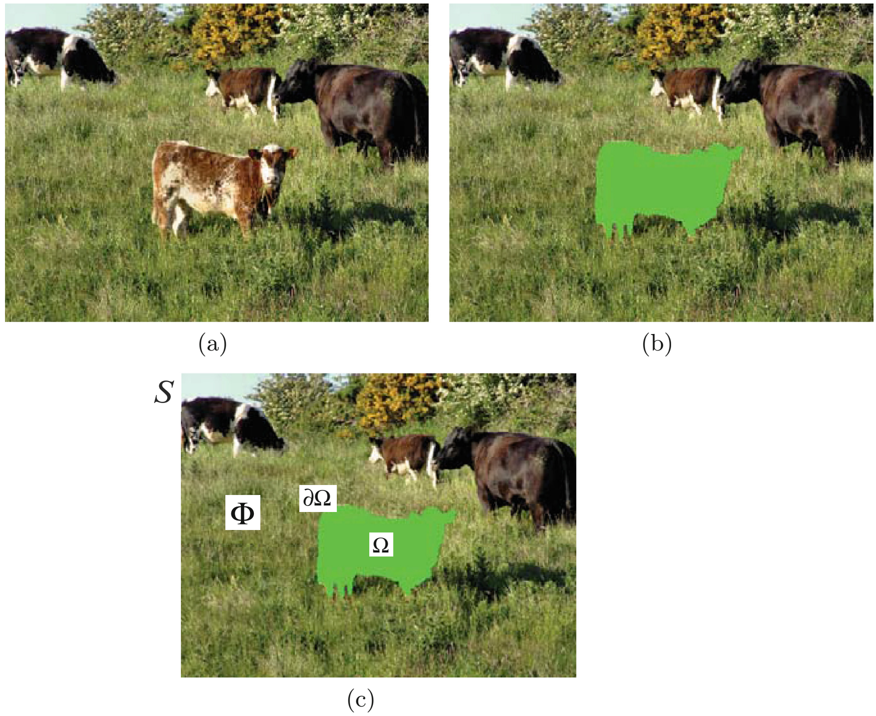


Fig. 1. An example of PSIS problem description. (a) The secret image S; (b) the same input cover image C by manually selecting and removing the target part with color green from the original secret image S; (c) notations in the problem definition. (Color figure online)

2.2 Linear Congruence

Equations (1) and (2) are the basic equations for LC secret sharing, by which (n, n) threshold secret sharing can be achieved, where P denotes a number larger than the biggest pixels value, x_i and y represent the i-th shared pixel and secret pixel, respectively. In Eq. (1), a one-to-many mapping between y and sum of all the x is established, so the secret value can be recovered losslessly with all the shared values. But there is no direct map relationship between secret value and less than k shared value, thus the method is secure. So Eq. (1) guarantees the feasibility of precise recovery and security for the proposed scheme. At the meanwhile, the condition in Eq. (2) ensures that no duplicate values exist in first n shared pixels.

$$(x_1 + x_2 + \cdots + x_n) \ mod \ P = y \tag{1}$$

$$x_i \neq x_j, when \ i \neq j. \tag{2}$$

Equation (3) is the basic equation for LC secret recovery. After removing the duplicate shared values, the rest of shared values $x_{i_1}, x_{i_2}, \cdots, x_{i_t}$ take part in the computation for the recovered secret value y' using Eq. (3).

$$y' = (x_{i_1} + x_{i_2} + \cdots + x_{i_t}) \ mod \ P \tag{3}$$

Figure 2 indicates an example by directly applying LC method for $(2, 2)$ threshold, where the input secret image is the same as Fig. 1. We can see that the secret target part can be reconstructed losslessly, while the corresponding the secret target parts of the shadow images are noise-like. In the revealing process of the secret image, it only needs to iterate t pixels and execute $t-1$ times addition operation and one time module operation to decode a secret pixel. Obviously, the time complexity is smaller. Hence, LC sharing idea is selected in our scheme as an SIS method.

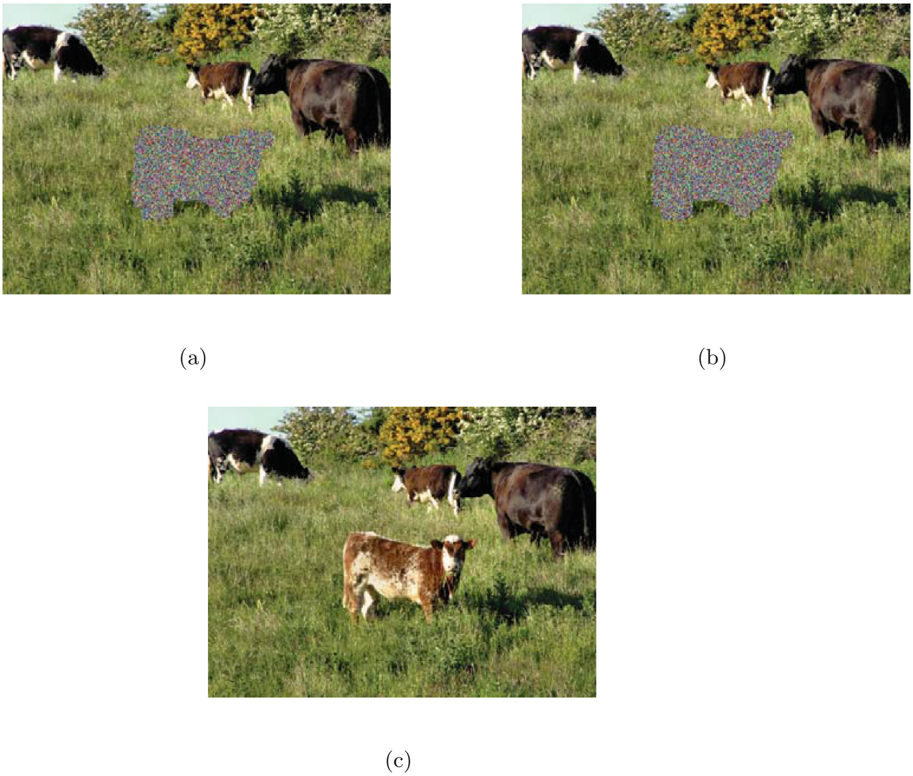


Fig. 2. Simulation results of directly applying LC method for threshold $(2, 2)$. (a)–(b) two shadow images SC_1, SC_2; (c) recovered result by SC_1 and SC_2.

2.3 Image Inpainting

Many image inpainting schemes were proposed in the literature, here Criminisi et al. approach [25,26] will be applied in our scheme, which is researched widely. We will introduce Criminisi et al. image inpainting approach in detail. The keynote of it is the selection of patch priorities order in region-filling. The patch with the highest priority will be filled preferentially. The priorities will be renewed after every filling until the image is inpainted totally in the same manner. The main inpainting process includes:

1. Select the part Ω to be inpainted, and $\Omega = S - \Phi$.
2. Determine the size of template window, denoted as Ψ_p, using image texture feature, where any $p \in \partial\Omega$ exhibits center of template window and the size of the window should be larger than the biggest texture element.
3. Compute patch priorities by Eq. (4) which is defined as the product of the confidence term and data term.

$$W(p) = C(p)D(p) \tag{4}$$

where $C(p)$ and $D(p)$ denote the confidence term and data term, respectively, defined as follows:

$$C(p) = \frac{\sum\limits_{q \in \psi_p \cap \bar{\Omega}} C(q)}{|\psi_p|} \tag{5}$$

$$D(p) = \frac{\left|\nabla S_p^{\perp} \cdot n_p\right|}{a} \tag{6}$$

where $|\psi_p|$ indicates the area of ψ_p and a is a normalization factor. $\nabla S_p^{\perp}$ and n_p denote the isophote direction and the normal vector direction at point p, respectively.
The confidence term expresses the amount of reliable information contained in template window. The data term measures the difference between the isophote direction and the normal vector direction. In a word, we conclude that the template window includes more information and the difference between the isophote direction and the normal vector direction is less, the priority of the patch is higher.
4. Find $\hat{p}$ using Eq. (7) and the most matching block $\psi_{\hat{q}} \in \Phi$ in the source image using template window according to Eq. (8), where the evaluation standard is the Sum of Squared Differences (SSD). Finally, the most matching block replaces the patch of current window.

$$\hat{p} = \arg\max_{p \in \partial\Omega} W(p) \tag{7}$$

$$\hat{q} = \arg\min_{q \in \Phi} d(\psi_{\hat{p}}, \psi_q) \tag{8}$$

5. Renew the confidence terms after each filling process $C(q) = C(\hat{p})$ for any $q \in \psi_{\hat{p}} \cap \Omega$.
6. Repeat steps 3–5 until the image is inpainted completely.

Taking as an example, the inpainted image by Criminisi et al. approach is presented in Fig. 3. We can see that another visually plausible image is obtained, thus image inpainting will be applied in the proposed scheme to achieve meaningful shadow images.

Fig. 3. An example of the inpainted image from Fig. 1(b) by Criminisi et al.'s approach

3 The Proposed PSIS Scheme

Here, in order to deal with the PSIS issue, in this paper, we propose a novel PSIS scheme for (n, n) threshold based on image inpainting and LC. We present the proposed PSIS scheme based on the original secret image S and the selected secret target part Ω, resulting in n output meaningful shadow images $SC_1, SC_2, \cdots SC_n$. Our generation steps are described in Algorithm 1.

In step 2 of our Algorithm, each shadow image has its own order (highest priority) in which the filling proceeds, i.e., $\hat{p_i}$. Aiming to inpaint synchronously, among the n candidate orders, the highest priority is selected again in Step 3 as the applied order for all the n shadow images inpainting.

After the most matching block replaces the patch of the current window in Step 4, the secret block of the current window corresponding to the secret target part will be generated into the n shadow images corresponding blocks based on LC sharing in Steps 5–6. Thus, the modified patches of the current window will be the basis for next inpainting processing so that the target secret pixel is encoded into the pixels corresponding to shadow images in the processing of shadow images inpainting. As a result, meaningful shadow images may be achieved in a visually plausible way.

The secret recovery of the proposed scheme is the same as LC method according to Eq. (3) by all the n shadow images.

Algorithm 1. The proposed PSIS scheme for (n, n) threshold
Input: The threshold parameters (n, n), the original secret image S and The selected secret target part Ω. **Output**: n shadow images $SC_1, SC_2, \cdots SC_n$
Step 1: Remove the target part Ω from the original secret image S to obtain the same n cover images, denoted as $C_1, C_2, \cdots C_n$. Let $SC_i = C_i$ be the input inpainting image. Determine the size of template window, denoted as Ψ_{p^*}. **Step 2:** For each shadow image, find $\hat{p_i}$ using Eq. (7). **Step 3:** Find $i^* = \arg \max_{i \in [1,n]} W_i(\hat{p_i})$, set $\hat{p_i} = \hat{p_{i^*}}$, $i = 1, 2, \cdots n$. **Step 4:** Based on $\hat{p_i}$ and Eq. (8), search for the most matching block to gain $\psi_{\hat{q_i}}$, where $i = 1, 2, \cdots n$. For each cover image, the most matching block replaces the patch of current window. **Step 5:** For each position $(i, j) \in \{(i, j) \mid M_1 \leq i \leq M_2, N_1 \leq j \leq N_2\}$, where (M_1, N_1) and (M_2, N_2) denote the coordinates of the processing template window in S, repeat Step 6. **Step 6:** Least modify $SC_1(i, j), SC_2(i, j), \cdots SC_n(i, j)$ to satisfy Eq. (1). **Step 7:** Renew the confidence terms after each filling process $SC(q_i) = SC(\hat{p_i})$ for any $q_i \in \psi_{\hat{p_i}} \cap \Omega$, $i = 1, 2, \cdots n$. **Step 8:** Repeat steps 2–7 until each cover image is inpainted completely. **Step 9:** Output n shadow images $SC_1, SC_2, \cdots SC_n$.

4 Experimental Results and Analyses

In this section, experiments and analyses are conducted to evaluate the effectiveness of the proposed method. In the experiments, the same example as shown in Fig. 1 will be employed as the input color secret image, with size of 512 × 384.

Simulation result by the proposed PSIS scheme is presented in Fig. 4 for $(4, 4)$ threshold, where Fig. 4(a) − (d) show the generated four shadow images SC_1, SC_2, SC_3, SC_4 and the recovered results by two or more shadow images are presented in Fig. 4(e) − (o). Here "+" indicates addition and module operation as in LC. The shadow images corresponding to the secret target part are meaningful in a way that looks reasonable to the human eye, although little artifact appears in the shadow images due to the modification of the shadow images blocks for secret block generation based on LC sharing in Steps 5–6 of our Algorithm. We can see that the secret target part can be reconstructed losslessly when all the four shares are collected. The recovering results by less than four shadow images cannot recovery the secret while secret leakage appears especially for the edge of the selected secret target part, which also may be caused by the modification of the shadow images blocks in Steps 5–6 of our Algorithm. In the revealing process of the secret image, it only needs to execute one time addition operation and one time module operation to decode a secret pixel so that the recovery computation complexity is simple. Decreasing the artifacts and threshold extension will be our future work.

Additional $(3, 3)$ threshold simulation result is illustrated in Fig. 5, we can conclude similar results as the previous simulation except for a little more artifact in the shadow image, which is caused by LC sharing feature.

(a) SC_1 (b) SC_2 (c) SC_3 (d) SC_4

(e) $SC_{\{+,1,2\}}$ (f) $SC_{\{+,1,3\}}$ (g) $SC_{\{+,1,4\}}$

(h) $SC_{\{+,2,3\}}$ (i) $SC_{\{+,2,4\}}$ (j) $SC_{\{+,3,4\}}$

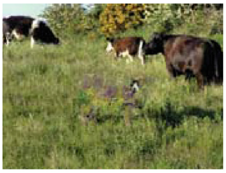
(k) $SC_{\{+,1,2,3\}}$ (l) $SC_{\{+,1,2,4\}}$ (m) $SC_{\{+,1,3,4\}}$ (n) $SC_{\{+,2,3,4\}}$

(o) $SC_{\{+,1,2,3,4\}}$

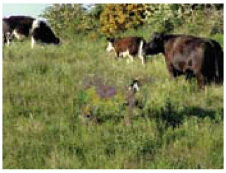
Fig. 4. Experimental example of the proposed scheme for threshold $(4, 4)$

Based on the above results we can conclude that:

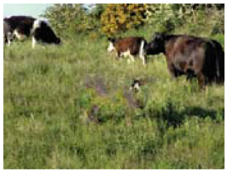
1. The target part is successfully inpainted into visually plausible shadow image.
2. Each shadow image is meaningful in a way that looks reasonable to the human eye, while Every single shadow image can not disclose the secret image.
3. When $t < n$ shadow images are collected, we cannot recovery the secret although secret leakage appears.
4. When $t = n$ shadow images are recovered by only addition and module operation, the secret image including the secret target part could be recovered losslessly.
5. An acceptable the partial secret image sharing (PSIS) for (n, n) threshold is achieved in our scheme.



(a) SC_1



(b) SC_2

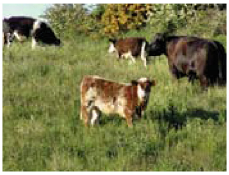


(c) SC_3

(d) $SC_{\{+,1,2\}}$

(e) $SC_{\{+,1,3\}}$

(f) $SC_{\{+,2,3\}}$



(g) $SC_{\{+,1,2,3\}}$

Fig. 5. Experimental example of the proposed scheme for threshold $(3, 3)$

5 Conclusion

This paper considered the new partial secret image sharing (PSIS) issue as well as proposed a novel PSIS scheme for (n, n) threshold based on image inpainting and linear congruence (LC) secret sharing method. Experiments showed that the output inpainted shadow images are meaningful, and the full secret image including the target secret part and other parts can be recovered losslessly by addition. Decreasing the artifacts and threshold extension will be our future work.

Acknowledgement. This work is supported by the National Natural Science Foundation of China (Grant Number: 61602491).

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
2. 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

3. Thien, C.C., Lin, J.C.: Secret image sharing. Comput. Graph. **26**(5), 765–770 (2002)
4. Lin, S.J., Lin, J.C.: VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (vc) and polynomial-style sharing (pss) approaches. Pattern Recogn. **40**(12), 3652–3666 (2007)
5. Yang, C.N., Ciou, C.B.: Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. Image Vis. Comput. **28**(12), 1600–1610 (2010)
6. Li, P., Ma, P.J., Su, X.H., Yang, C.N.: Improvements of a two-in-one image secret sharing scheme based on gray mixing model. J. Vis. Commun. Image Represent. **23**(3), 441–453 (2012)
7. Yan, X., Wang, S., El-Latif, A.A.A., Niu, X.: Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery. Multimedia Tools Appl., 1–22 (2013)
8. Yang, C.N.: New visual secret sharing schemes using probabilistic method. Pattern Recognit. Lett. **25**(4), 481–494 (2004)
9. Cimato, S., De Prisco, R., De Santis, A.: Probabilistic visual cryptography schemes. Comput. J. **49**(1), 97–107 (2006)
10. Wang, D., Zhang, L., Ma, N., Li, X.: Two secret sharing schemes based on boolean operations. Pattern Recognit. **40**(10), 2776–2785 (2007)
11. Wang, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography via error diffusion. IEEE Trans. Inf. Forensics Security. **4**(3), 383–396 (2009)
12. 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
13. Yang, C.N., Sun, L.Z., Yan, X., Kim, C.: Design a new visual cryptography for human-verifiable authentication in accessing a database. J. Real-Time Image Proc. **12**(2), 483–494 (2016)
14. Wu, X., Sun, W.: Improving the visual quality of random grid-based visual secret sharing. Sig. Process. **93**(5), 977–995 (2013)
15. Yan, X., Wang, S., Niu, X.: Threshold construction from specific cases in visual cryptography without the pixel expansion. Sig. Process. **105**, 389–398 (2014)
16. Luo, H., Yu, F., Pan, J.S., Lu, Z.M.: Robust and progressive color image visual secret sharing cooperated with data hiding. In: Eighth International Conference on Intelligent Systems Design and Applications, ISDA 2008, vol. 3, Kaohsiung, Taiwan, IEEE, pp. 431–436. IEEE (2008)
17. Yan, X., Wang, S., Niu, X., Yang, C.N.: Generalized random grids-based threshold visual cryptography with meaningful shares. Sig. Process. **109**, 317–333 (2015)
18. Zhou, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography. IEEE Trans. Image Process. **15**(8), 2441–2453 (2006)
19. Liu, F., Wu, C.: Embedded extended visual cryptography schemes. IEEE Trans. Inf. Forensics Secur. **6**(2), 307–322 (2011)
20. Yan, X., Wang, S., Niu, X., Yang, C.N.: Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. Digit. Signal Proc. **38**, 53–65 (2015)
21. Guo, T., Liu, F., Wu, C.: Threshold visual secret sharing by random grids with improved contrast. J. Syst. Softw. **86**(8), 2094–2109 (2013)
22. Fu, Z., Yu, B.: Visual cryptography and random grids schemes. In: Shi, Y.Q., Kim, H.-J., Pérez-González, F. (eds.) IWDW 2013. LNCS, vol. 8389, pp. 109–122. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43886-2_8

23. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Visual cryptography for general access structures. Inf. Comput. **129**(2), 86–106 (1996)
24. Li, P., Yang, C.N., Wu, C.C., Kong, Q., Ma, Y.: Essential secret image sharing scheme with different importance of shadows. J. Vis. Commun. Image Represent. **24**(7), 1106–1114 (2013)
25. Criminisi, A., Perez, P., Toyama, K.: Region filling and object removal by exemplar-based image inpainting. IEEE Trans. Image Process. **13**(9), 1200–12 (2004). A Publication of the IEEE Signal Processing Society
26. Shen, W., Song, X., Niu, X.: Hiding traces of image inpainting. Res. J. Appl. Sci. Eng. Technol. **4**(23), 4962–4968 (2012)
27. Liu, L., Lu, Y., Yan, X., Wan, S.: A progressive threshold secret image sharing with meaningful shares for gray-scale image. In: 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), pp. 380–385. IEEE (2016)