International Journal of Digital Crime and Forensics
Volume 13 • Issue 4 • July-August 2021

Applying Secret Image Sharing to Economics

Xuemei Zhao, Anhui Business and Technology College, Hefei, China
Tongtong Zhang, 31433 Institute, China
Jun Liu, National University of Defense Technology, Changsha, China
Canju Lu, National University of Defense Technology, Changsha, China
Huan Lu, National University of Defense Technology, Changsha, China
Xuehu Yan, National University of Defense Technology, Changsha, China
https://orcid.org/0000-0001-6388-1720

ABSTRACT

Economics has some limitations, such as insecure multiple parties economical investment decision and leakage of business quotation. Secret image sharing (SIS) for (k, n)-threshold is such a technique that protects an image through splitting it into n shadows, a.k.a. shadow images or shares, assigned to n corresponding participants. The secret image can be disclosed by obtaining k or more shadows. Polynomial-based SIS and visual secret sharing (VSS) are the chief research branches. This paper first analyzes the insecure issues in economics and then introduces two methods to apply typical SIS schemes to improve economical security. Finally, experiments are realized to illustrate the efficiency of the methods.

KEYWORDS

Economics Security, Information Hiding, Secret Image Sharing, Visual Secret Sharing

1. INTRODUCTION

Secret image sharing (SIS) for (*k, n*)-threshold splits a secret image into *n* noise-like shadows, *a.k.a*, shares or shadow images, and then assigns the shadows among *n* participants. The secret can be disclosed by obtaining *k* or more authorized shadows. However, less than *k* shadows overall dis- close no information on the secret. Polynomial-based SIS (Shamir, 1979) and visual secret sharing (VSS) (Naor & Shamir, 1995; Wang, Liu & Yan, 2016) are the chief research branches.

In Shamir's original polynomial-based secret sharing (Shamir, 1979) for (*k, n*)-threshold, the secret is split into the constant coefficient of a random (*k* 1)-degree polynomial to obtain *n* shadows, which are then also assigned to *n* corresponding participants. The secret can be disclosed by Lagrange interpolation when obtaining any *k* or more shadows. Following Shamir's original scheme and using all the coefficients of the polynomial to embed secret pixels, Thien and Lin (Thien & Lin, 2002) reduced the size of each shadow 1/*k* times to that of the original secret image. Based on Thien and Lin's work, some other polynomial-based schemes (Yang & Ciou, 2010; Zhou, Lu, Yan, Wang & Liu, 2018; Li, Yang & Kong, 2018) were further proposed to obtain more features. The strength of polynomial-based SIS lies in the secret image can be disclosed with high quality. Although polynomial-

DOI: 10.4018/IJDCF.20210701.oa2

based SIS only uses any k shadows to disclose a distortion-less secret image, in the disclosing phase it needs more complicated computations, *a.k.a*, Lagrange interpolation, and known order of shares.

In a VSS (Cimato, De Prisco & De Santis, 2006; Wang, Zhang, Ma & Li, 2007; Wang, Arce & Di Crescenzo, 2009; Weir & Yan, 2010) for (k, n)-threshold, first the split n shadows are printed onto transparencies and then assigned to n corresponding participants. The merit of VSS is that, the secret image can be disclosed by just superposing any k or more shadows (transparencies) and human eyes with no cryptographic computation. Less than k shadows generally give no clue about the secret even if high computation power is available. Following Naor and Shamir's original method, the physical properties and corresponding VSS limitations are widely researched, such as threshold (Yan, Wang & Niu, 2014), contrast (Wu & Sun, 2013; Yan, Liu & Yang, 2018), pixel expansion (Cimato, De Prisco & De Santis, 2006; Guo, Liu & Wu, 2013; Fu & Yu, 2014), multiple secrets (Li, Ma, Su & Yang, 2012), meaningful shadows (Yan, Wang, Niu & Yang, 2015a; Wang, Arce & Di Crescenzo, 2009; Liu & Wu, 2011; Yan, Wang, Niu & Yang, 2015b), and so on (Yan & Lu, 2018; Liu, Wang, Yan & Zhang, 2017).

Although SIS can be applied to not only information hiding and watermarking, but also authentication, transmitting passwords, access control, distributed storage and computing, etc (Yan, Lu, Liu, Wan, Ding & Liu, 2017a; Belazi & El-Latif, 2017; Yan, Lu, Liu, Wan, Ding & Liu, 2017b), its practical application is an important issue.

Nowadays, economics has some limitations, such as, insecure multiple parties economical investment decision and leakage of business quotation. As Figs. 1 and 2. During traditional multiple directors economical investment decision, since the bank account is authorized by fewer directors, economical investment decision may be not democratic. A staff in general sends a business quotation to the boss via Email, where a business quotation is the top secret for a company. A watcher may steal the Email to obtain the quotation leading to losing money for the company.

To deal with the issues, the motivations of the paper is to apply typical SIS schemes to improve the security in the above economical scenarios (Figures 1-2).

This paper first analyzes the insecure issues in economics, and then introduces two methods to apply typical SIS schemes to improve economical security. Polynomial-based SIS for (k, n)-threshold is applied to enhance the security of multiple parties economical investment decision. Random grid (RG)-based VSS for (2, 2)-threshold is applied to enhance the security of business quotation. Finally, analyses and experiments are realized to illustrate the efficiency of our methods.

We organize the rest of the paper as follows. Section 2 represents some requirements and related works . Section 3 gives the designed schemes. Section 4 is devoted to partial experimental results. Finally, Section 5 concludes our paper.

2. PRELIMINARIES

In this section, to clearly show our work we present some preliminaries. In a (k, n)-threshold SIS, the secret image is denoted by S, n shadows by SC_1, SC_2, SC_n, and the disclosed secret image S' is disclosed from any t shadows.

s indicates the value of one secret pixel $S(i, j)$ or a secret region. Symbols $\oplus$ and $\otimes$ mean the Boolean XOR and OR operations.

2.1. Polynomial-Based SIS

Moreover, polynomial-based SIS will be presented as an example.

In order to split secret data s into n shadows, as Equation(1)original polynomial-based secret sharing generates a k 1 degree polynomial, in which a_i is random in [0,P], for $i = 1, 2,\ldots k\_1$, and P is a prime greater than s.

Figure 1. The first scenario of multiple parties economical investment decision

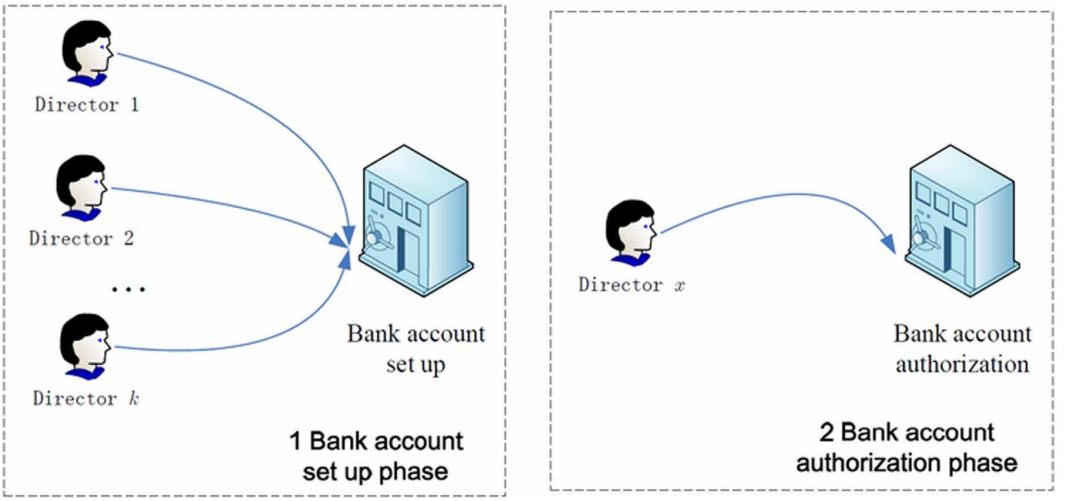
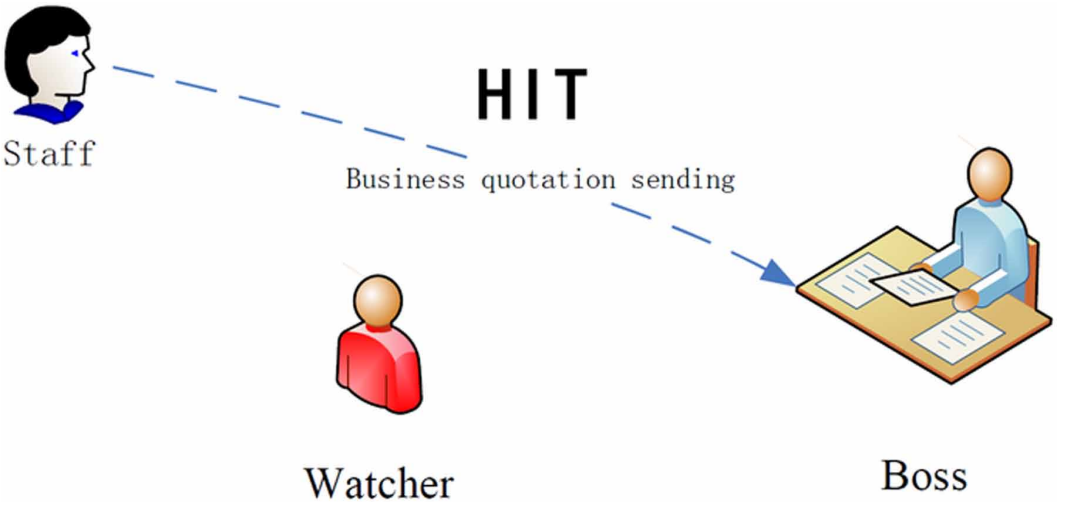


Figure 2. The second scenario of business quotation



$$f(x) = (s + a_1 x + \cdots + a_{k-1} x^{k-1}) \bmod P \tag{1}$$

For any given x = i, f (x) is obtained with Equation(1) and these n pairs $\{(i, sci)\}_{i=1}^{n}$ are assigned to the n participants. In the disclosing phase, given any k pairs of these n pairs $\{(i, sci)\}_{i=1}^{n}$, through solving Equation(1) we losslessly disclose a unique s.

When applying original polynomial-based secret sharing to a grayscale image, since 251 is the closet number less than 256, in general $P = 251$ in follow-up polynomial-based SIS.

The inverse phases of above polynomial-based SIS for (k, n)-threshold will be applied in the introduced method to enhance the security of multiple parties economical investment decision.

2.2. VSS

In a RG-based VSS (Kafri & Keren, 1987), 0 indicates a white pixel and 1 indicates a black pixel. The splitting and disclosing phases of one classic RG-based VSS for (2, 2)-threshold are demonstrated as follows.

Splitting step 1: Pseudo-randomly split 1 RG SC_1 by using coin flipping function. Splitting step 2: As Equation (2) calculate SC_2 .

Disclosing phase: $S' = SC_1 \otimes SC_2$ as Equation (3). If s is 1, the disclosing bit $sc_1 \otimes sc_2 = 1$ is always black; otherwise if s is 0, the disclosing bit $sc_1 \otimes sc_2 = SC_1(i, j) \otimes SC_1(i, j)$ has 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 inverse phases of above classic RG-based VSS for (2, 2)-threshold will be applied in the introduced method to enhance the security of business quotation.

3. THE INTRODUCED METHODS

Here, in this section, two methods will be introduced to apply typical SIS schemes to improve economical security. Their difference lies in different application scenarios.

3.1. The Method for the First Scenario of Multiple Parties Economical Investment Decision

The design idea for the first scenario of multiple parties economical investment decision is shown in Figure 3.

In the first scenario of multiple parties economical investment decision, in the bank account set up phase, each director of the total k directors initializes his personal shadow (key) and sends to the bank center. The bank center utilizes their personal shadows and SIS to generate a secret image stored in the center, and destroys their personal shadows simultaneously. In the bank account authorization phase, when all the k directors agree with the economical investment, they can send their shadows to authorize the account.

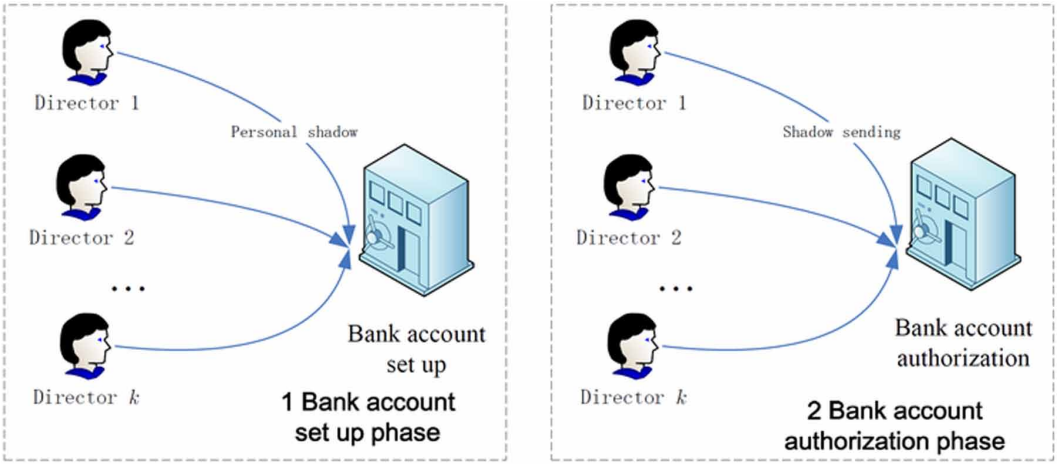
The splitting and disclosing phases of the introduced method for the first scenario of multiple parties economical investment decision are demonstrated as follows.

The bank account set up phase is as follows.

Step 1: A prime number $P = 251$ is selected. Director i selects his personal shadow with a size of $H \times W$, whose pixel value is in the range of $[0, P - 1]$, denoted by SC_i, $i = 1, 2, \cdots, k$.
Step 2: For each position $(h, w) \in \{(h, w) | 1 \le h \le H, 1 \le w \le W\}$, repeat Steps 3-4.
Step 3: Solve Equation (4) to obtain $a_0, a_1, \cdots, a_{k-1}$ by Lagrange interpolation.

$$SC_1(h,w) = \left(a_0 + a_1 1 + \ldots + a_{k-1} 1^{k-1}\right) mod\, P$$

Figure 3. The design idea for the first scenario of multiple parties economical investment decision



$$SC_2\left(h,w\right)=\left(a_0+a_1 2+\ldots+a_{k-1}2^{k-1}\right)mod\,P$$

$$SC_{k-1}\left(h,w\right)=\left(a_0+a_1\left(k-1\right)+\ldots+a_{k-1}\left(k-1\right)^{k-1}\right)mod\,P \tag{4}$$

$$SC_k\left(h,w\right)=\left(a_0+a_1 k+\ldots+a_{k-1}k^{k-1}\right)mod\,P$$

Step 4: Compute $S(h, k(w-1)+1) = a_0$, $S(h, k(w-1)+2) = a_1$, $\cdots$, $S(h, k(w-1)+k-1) = a_{k-1}$.
Step 5: The bank stores grayscale secret image S with a size of $H \times kW$ and destroys SC_i for

$i = 1, 2, \cdots, k$.

The bank account authorization phase is as follows.

Step 1: For each position $(h, w) \in \{(h, w) | 1 \le h \le H, 1 \le w \le W\}$, repeat Steps 2-3.
Step 2: Construct a $k-1$ degree polynomial as follows.

$f(x) = (a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}) \bmod P(5)$ where $a_0 = S(h, k(w-1)+1)$, $a_1 = S(h, k(w-1)+2)$, $\cdots$, $a_{k-1} = S(h, k(w-1)+k-1)$.

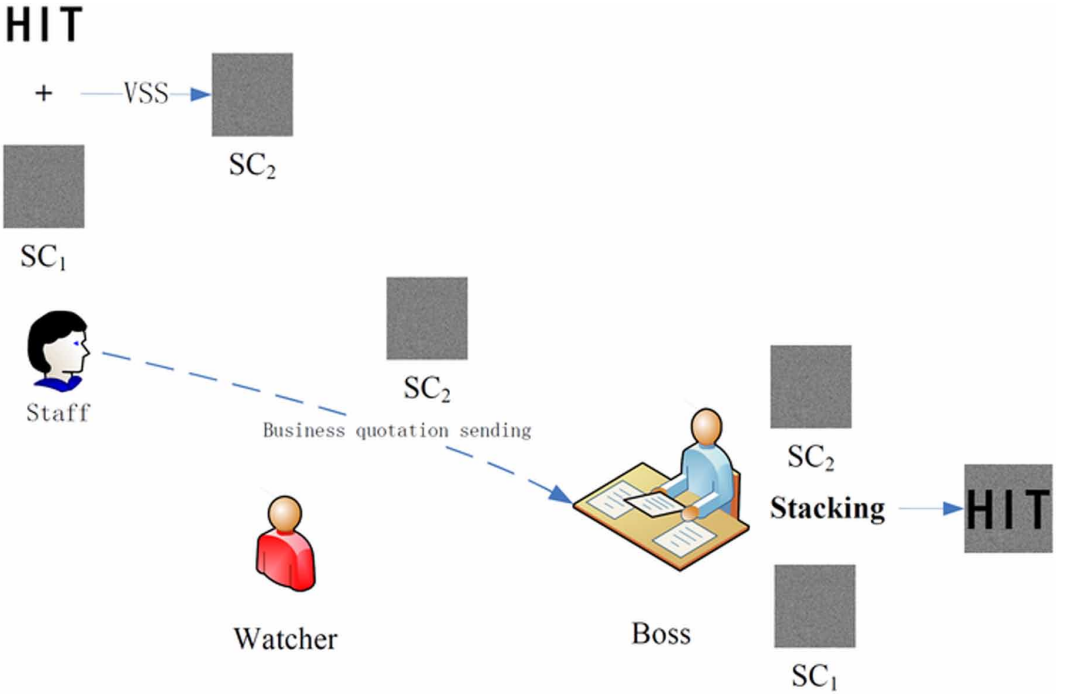
Step 3: If $SC_i(h, w) = f(i)$, for $i = 1, 2, k$, go to next position; otherwise, failed authentication.
Step 4: Bank account authorization.

3.2. The Method for the Second Scenario of Business Quotation

In the second scenario of business quotation, the business quotation is protected by SIS and the watcher obtains nothing of the business quotation even if the watcher steals the transmit content.

The design idea for the second scenario of business quotation is illustrated in Figure 4.

Figure 4. The design idea for the second scenario of business quotation



The splitting and disclosing phases of the introduced method for the second scenario of business quotation are demonstrated as follows.

Step 1: The boss generates his personal shadow with a size of $H \times W$, whose pixel value is 0 or 1, denoted by SC_1. SC_1 is preserved by himself and the staff.
Step 2: When the staff wants to transmit a business quotation, he converts it into a binary secret image, denoted by S.
Step 3: With S and SC_1, the staff obtains SC_2 using RG-based VSS for (2, 2)-threshold. The staff sends SC_2 to the boss via Email and so on.
Step 4: When the boss receives SC_2, he stack SC_2 and SC_1 to reveal the business quotation.

4. EXPERIMENTAL RESULTS AND ANALYSES

In this section, experiments and analyses are taken into account to evaluate the effectiveness of the proposed scheme.

4.1. Image Illustration

Figure 5 is one experimental result of the introduced method for the first scenario of multiple parties economical investment decision, where $k = 3$ and grayscale secret images selected by the directors are in Figures 5 (a-c). Figure 5 (d) is the generated one secret image S, which is noise-like and stored in the center. Figures 5 (e-g) display the constructed grayscale shadows with ith order, for $i = 1, 2, 3$. Since Figures 5 (e-g) are the same as Figures 5 (a-c), the bank account is authorized. A fake shadow randomly generated is presented in Figure 5 (h), which is not the same as any one of Figures 5 (a-c) and thus the authentication is failed.

Figure 6 is the experimental result of the introduced method for the second scenario of business quotation, where $k = 2$ and its stored binary random shadow is in Figure 6 (a). Figure 6 (b) is the business quotation image, which covers the business quotation. Figure 6 (c) illustrates the generated SC_2 using RG-based VSS for (2, 2)-threshold with S and SC_1. Figure 6 (d) displays the revealed business quotation image by stacking SC_1 and SC_2, where the business quotation is clearly revealed.

Based on the above results we conclude that:

1. In the first scenario of multiple parties economical investment decision, our method achieves that only when all the directors send their true personal shadows the account is authorized.
2. In the second scenario of business quotation, even a watcher steals the Email he cannot reveal the business quotation content.

4.2. Comparisons with Related Works

We will compare the proposed SIS with the related possible schemes by means of qualitative analyses rather than quantitative illustration and comparison, due to the features are significantly different.

For the first scenario of multiple parties economical investment decision, we may easily consider to joint the directors' private keys to generate S to authorize the bank account, called jointed key. However this method is not order-free and leaks part information on S with insufficient directors. Furthermore, the jointed key is only a simple combination of the directors' private keys, which may be attacked one by one. It cannot authenticate each director after he sends his personal shadow. By contrast, the introduced first method has all the features. In addition, each personal shadow can be used many times rather than once.

For the second scenario of business quotation, we may consider to encrypt the business quotation using typical encryption schemes, such as, DES and AES, and then transmit the encrypted business quotation. In general, an encryption scheme is complex with high cryptographic computation especially for the decryption phase. By contrast, the introduced second method can disclose the secret business quotation by just stacking the shadows (transparencies) and human eyes with no cryptographic computation.

5. CONCLUSION

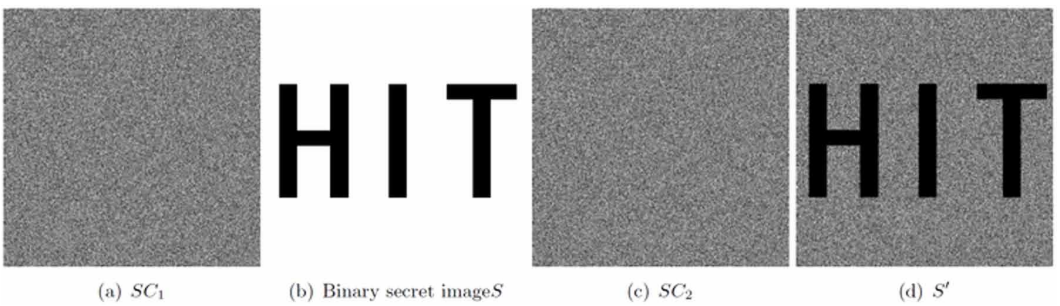
In this paper, based on the study of the limitations of economics and typical secret image sharing (SIS) schemes, two methods are introduced to apply typical SIS schemes to improve economical security. The first method is for the scenario of multiple parties economical investment decision, where inverse polynomial-based SIS is applied. The second method for the scenario of business quotation, where inverse visual secret sharing (VSS) is applied. Analyses and experimental results are provided to show the effectiveness of our methods. Improving our methods to be more practical will be our future work.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China (Grant Number: 61602491), the Key Program of the National University of Defense Technology (Grant Number: ZK-17-02-07), and the 2020 Anhui quality engineering project: Accounting and Statistics teaching team (2020jxtd031).

Figure 5. Simulation results of the introduced method for the first scenario of multiple parties eco- nomical investment decision, where k = 3. (a) (c) three shadows SC_1, SC_2 and SC_3 with size of 128 128; (d) the generated grayscale secret image with size of 128 384; (e) (g) the constructed grayscale shadows with ith order; (h) a fake shadow; (i) failed authentication.

Figure 6. Simulation results of the introduced method for the second scenario of business otation, where k = 2. (a) a random shadow SC_1; (b) the business quotation image; (c) the constructed binary shadow SC_2; (d) the disclosed business quotation image.



REFERENCES

Belazi, A., & El-Latif, A. A. A. (2017). A simple yet efficient s-box method based on chaotic sine map. *Optik (Stuttgart)*, *130*, 1438–1444. doi:10.1016/j.ijleo.2016.11.152

Cimato, S., De Prisco, R., & De Santis, A. (2006). Probabilistic visual cryptography schemes. *The Computer Journal*, *49*(1), 97–107. doi:10.1093/comjnl/bxh152

Fu, Z.-x., & Yu, B. (2014). Visual cryptography and random grids schemes. In *Digital-Forensics and Watermarking* (pp. 109–122). Springer.

Guo, T., Liu, F., & Wu, C. (2013). Threshold visual secret sharing by random grids with improved contrast. *Journal of Systems and Software*, *86*(8), 2094–2109. doi:10.1016/j.jss.2013.03.062

Kafri, O., & Keren, E. (1987). Encryption of pictures and shapes by random grids. *Optics Letters*, *12*(6), 377–379. doi:10.1364/OL.12.000377 PMID:19741737

Li, P., Ma, P.-J., Su, X.-H., & Yang, C.-N. (2012). Improvements of a two-in-one image secret sharing scheme based on gray mixing model. *Journal of Visual Communication and Image Representation*, *23*(3), 441–453. doi:10.1016/j.jvcir.2012.01.003

Li, P., Yang, C. N., & Kong, Q. (2018). A novel two-in-one image secret sharing scheme based on perfect black visual cryptography. *Journal of Real-Time Image Processing*, *14*(1), 41–50. doi:10.1007/s11554-016-0621-z

Liu, F., & Wu, C. (2011). Embedded extended visual cryptography schemes. *Information Forensics and Security, IEEE Transactions on, 6*, 307–322.

Liu, X., Wang, S., Yan, X., & Zhang, W. (2017). Homomorphic visual cryptography. *Journal of Information Hiding and Multimedia Signal Processing*, *8*, 744–756.

Naor, M., & Shamir, A. (1995). Visual cryptography. In *Advances in Cryptology-EUROCRYPT'94 Lecture Notes in Computer Science, Workshop on the Theory and Application of Cryptographic Techniques* (pp. 1–12). Perugia, Italy: Springer.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, *22*(11), 612–613. doi:10.1145/359168.359176

Thien, C.-C., & Lin, J.-C. (2002). Secret image sharing. *Computers & Graphics*, *26*(5), 765–770. doi:10.1016/S0097-8493(02)00131-0

Wang, D., Zhang, L., Ma, N., & Li, X. (2007). Two secret sharing schemes based on boolean operations. *Pattern Recognition*, *40*(10), 2776–2785. doi:10.1016/j.patcog.2006.11.018

Wang, G., Liu, F., & Yan, W. Q. (2016). Basic visual cryptography using braille. *International Journal of Digital Crime and Forensics*, *8*(3), 85–93. doi:10.4018/IJDCF.2016070106

Wang, Z., Arce, G. R., & Di Crescenzo, G. (2009). Halftone visual cryptography via error diffusion. *IEEE Transactions on Information Forensics and Security*, *4*(3), 383–396. doi:10.1109/TIFS.2009.2024721

Weir, J., & Yan, W. (2010). A comprehensive study of visual cryptography. In *Transactions on DHMS V, LNCS 6010* (pp. 70–105). Springer.

Wu, X., & Sun, W. (2013). Improving the visual quality of random grid-based visual secret sharing. *Signal Processing*, *93*(5), 977–995. doi:10.1016/j.sigpro.2012.11.014

Yan, X., Liu, X., & Yang, C.-N. (2018). An enhanced threshold visual secret sharing based on random grids. *Journal of Real-Time Image Processing*, *14*(1), 61–73. doi:10.1007/s11554-015-0540-4

Yan, X., & Lu, Y. (2018). Progressive visual secret sharing for general access structure with multiple decryptions. *Multimedia Tools and Applications*, *77*(2), 2653–2672. doi:10.1007/s11042-017-4421-7

Yan, X., Lu, Y., Liu, L., Wan, S., Ding, W., & Liu, H. (2017a). Exploiting the homomorphic property of visual cryptography. *International Journal of Digital Crime and Forensics*, *9*(2), 45–56. doi:10.4018/IJDCF.2017040105

Yan, X., Lu, Y., Liu, L., Wan, S., Ding, W., & Liu, H. (2017b). Security analysis of secret image sharing. *Data Science: Third International Conference of Pioneering Computer Sci- entists, Engineers and Educators, ICPCSEE 2017, Changsha, China, September 22–24, 2017*, *Proceedings, Part I*, (pp. 305–316). doi:10.1007/978-981-10-6385-5_26

Yan, X., Wang, S., & Niu, X. (2014). Threshold construction from specific cases in visual cryptog- raphy without the pixel expansion. *Signal Processing*, *105*, 389–398. doi:10.1016/j.sigpro.2014.06.011

Yan, X., Wang, S., Niu, X., & Yang, C.-N. (2015a). Generalized random grids-based threshold visual cryptography with meaningful shares. *Signal Processing*, *109*, 317–333. doi:10.1016/j.sigpro.2014.12.002

Yan, X., Wang, S., Niu, X., & Yang, C.-N. (2015b). Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality. *Digital Signal Processing*, *38*, 53–65. doi:10.1016/j.dsp.2014.12.002

Yang, C.-N., & Ciou, C.-B. (2010). Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. *Image and Vision Computing*, *28*(12), 1600–1610. doi:10.1016/j.imavis.2010.04.003

Zhou, X., Lu, Y., Yan, X., Wang, Y., & Liu, L. (2018). Lossless and efficient polynomial-based secret image sharing with reduced shadow size. *Symmetry*, *10*(7), 249. Advance online publication. doi:10.3390/sym10070249

Xuemei Zhao, born in Jan 1982, received her bachelor's degree in economics from Anhui University of Finance and Economics in 2004 and her master's degree in economics in 2007. She is now an associate professor of Anhui Business and Technology College. Her area of interest is econometrics.

Tongtong Zhang was born in China in May 1983. She obtained a master's degree in communications from Hefei Institute of Electronic Engineering in 2010. She is now an engineer at the 31433 Institute. Her areas of interest are computer applications and network security.

Jun Liu was born in China, in Dec 1981, received the B.Sc. degree with honor rank in Computer Science and technology, China in 2005, M.Sc. degree in Computer Application Technology in 2009 from Central China Normal University. He now is a professor at National University of Defense Technology, Hefei, P. R. China. His areas of interests are computer application and multiple image processing.

Canju Lu was born in China, in Sep 1978, received the degree in Computer Science and Technology, China in 2003, from University of Science and Technology of China, M.Sc. degree in Computer Software and Theory in 2007, from Lanzhou Jiaotong University . He now is a professor at National University of Defense Technology, Hefei, P. R. China. His areas of interests are computer application.

Huan Lu was born in China, in Jan 1989, received the B.Sc. degree with honor rank in Network Engineering, China in 2012. He now is a lecturer at National University of Defense Technology, Hefei, P. R. China. His areas of interests are computer application and network engineering.

Xuehu Yan was born in China, in Feb 1984, received the B.Sc. degree with honor rank in Science in Information & Calculate Science, China in 2006, M.Sc. degree in Computational Mathematics in 2008, and doctoral degree in Computer Science and Technology in 2015 from Harbin Institute of Technology. He now is an Associate Professor at National University of Defense Technology, Hefei, P. R. China. His areas of interests are visual cryptography, secret image sharing, information hiding, cryptography and multimedia security. He has published more than 100 papers in these areas. He is co-recipient of an International Workshop of Digital Crime and Forensics (IWDCF) 2016 best paper award for the paper " Exploiting the Homomorphic Property of Visual Cryptography". He is an Associate Editor of the International Journal of Digital Crime and Forensics (IJDCF) (Jan. 2017 - present).