Hindawi
Security and Communication Networks
Volume 2020, Article ID 6627178, 13 pages
https://doi.org/10.1155/2020/6627178

Research Article

On the Value of Order Number and Power in Secret Image Sharing

Yongqiang Yu, Longlong Li, Yuliang Lu, and Xuehu Yan

National University of Defense Technology, Hefei 230037, China

Correspondence should be addressed to Xuehu Yan; publictiger@126.com

Received 7 October 2020; Revised 10 November 2020; Accepted 13 November 2020; Published 23 November 2020

Academic Editor: Jialiang Peng

Shadow images generated from Shamir's polynomial-based secret image sharing (SSIS) may leak the original secret image information, which causes a significant risk. The occurrence of this risk is closely related to the basis of secret image sharing, Shamir's polynomial. Shamir's polynomial plays an essential role in secret sharing, but there are relatively few studies on the power and order number of Shamir's polynomial. In order to improve the security and effectiveness of SSIS, this paper mainly studies the utility of two parameters in Shamir's polynomial, order number and power. Through the research of this kind of utility, the choice of order number and power can be given under different security requirements. In this process, an effective shadow image evaluation algorithm is proposed, which can measure the security of shadow images generated by SSIS. The user can understand the influence rule of the order number and power in SSIS, so that the user can choose the appropriate order number and power according to different security needs.

1. Introduction

With the development and application of computer network and multimedia technology, the production, transmission, and storage of digital images have increased exponentially. The increasing problem of information leakage and the improvement of people's awareness of network information security have led to more and more individuals and organizations beginning to pay attention to and study the security issues in image transmission and storage. To protect the secret images of the national government and military departments, it is particularly urgent to solve such security problems.

For information security, digital images need to be protected during transmission and storage [1]. Traditional image protection technologies include image encryption [2–4] and image hiding [5–7]. Encryption is the use of a specific algorithm to present the secret in another way. Using a secure encryption algorithm to encrypt the image can effectively protect the security of the image content. Image hiding is to hide the secret existence in other carriers or modules through hiding algorithms. Both of these secret image protection technologies have a common feature: transmission through a single channel. When the channel fails or is destroyed, the recipient cannot normally recover the secret image. The same problem also occurs in storage. If the encrypted secret image and the carrier hiding the secret image are tampered with or destroyed, the secret image cannot be completely restored. In addition to image encryption and image hiding, there are also image sharing [8–12]. Secret image sharing (SIS) not only has the function of protecting secret images, but also has the advantages of loss tolerance that other conventional methods do not have [13].

Secret sharing (SS) is to share the original secret into multiple subsecrets and distribute the generated shares to different participants. When the shares contributed by participants meet the required conditions, the secret can be recovered. SS solves the problem that secrets may be destroyed or tampered with in transmission and storage by using multiple channels for transmission and storage. Secret sharing based on Shamir's polynomial principle is an important branch of SS [14, 15]. Thien et al. introduced the principle of secret sharing into the field of images and proposed SSIS [16]. The proposal of SSIS is of great significance to the protection of secret images. However, some shadows generated by SSIS may leak the original secret image information, which has a significant impact and

challenge on the security of SSIS. It is found that information leakage of shadows occurs at different order numbers, and the degree of leakage varies from order number to order number. Similarly, the change of power also has some influence on the leakage of shadow images. It has been proved that the occurrence of SSIS's information leakage is related to the order number, power, and image itself.

This paper mainly uses theoretical analysis and experimental validation to study the impact of order number and power on the security of SSIS. This paper finds out the influence rule of order number and power and gives different selection schemes of order number and power so that users can select order number and power more effectively and conveniently according to different security needs. In order to evaluate the security of shadows more objectively, this paper also proposes a new shadow security evaluation algorithm. The degree to which the shadows leak the secret of the original image can be objectively measured by the parameters obtained by the evaluation algorithm, thus avoiding the subjective error of the human visual system (HVS).

2. Preliminary

In 1979, Shamir [17] and Blakley [18] proposed classical threshold SS schemes using algebra and geometry, respectively. Shamir's polynomial-based secret sharing (SSS) is to split secret S into n shares, which are assigned to n participants. Any k or more shares can be used to reconstruct S, while less than k shares cannot get any information on S. SSS is a threshold sharing scheme, which shares the secret S into n shadows by $f(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \bmod p$, in which $a_0 = S, a_1, a_2, \ldots, a_{k-1}$ are selected randomly in $[0, p]$. SIS can only embed one bit at a time, which is sufficient for sharing ordinary text data, but it is far from enough for sharing secret images. Every pixel in a secret image needs to be shared. If a secret pixel is shared every time, the space occupied by the sharing and the efficiency of sharing will be greatly reduced. In order to improve the efficiency of sharing and the space occupied by sharing, Thien and Lin sequentially embed the pixels of the secret image into all the coefficients of the Shamir's polynomial [16], and the specific measures are as follows:

(1) a_i is the ith pixel value of each group in the secret image sharing process.

(2) p is selected as 251, and the pixels above 250 are treated as 250.

The increase in sharing efficiency also brings about a problem: the shadow images generated by some images will leak the original secret image information [19, 20]. When the pixel correlation of the original secret image is strong, leakage is more likely to occur. It is worth noting that although the images are different, the leakage always occurs on some specific order numbers. In the application of the Thien–Lin's scheme, the choice of order number is of great significance to the security of the secret image, which has been extensively studied [21–23]. Tompa and Woll [21] proposed random generation of order numbers in theory but did not propose specific and effective generation schemes. In reference [22], when using the Thien–Lin's method, change p to 257, and the order number is defined as an integer from 1 to n. Literature [23] uses Thien–Lin's method on GF(2^8), taking order number as image ID number, so it cannot be randomly generated. These studies have noticed the importance of order numbers in SSIS, but they have not given a feasible order number selection scheme. Like the order number, the power is also a coefficient in the polynomial, and its role in sharing the polynomial cannot be ignored. Unfortunately, there is relatively little research on the power of Shamir's polynomial.

The rest of the paper is organized as follows. Section 3 introduces the research motivation of this paper and our contribution. The proposed scheme is introduced in Section 4, including parameter analysis, shadow image security evaluation algorithm, and order number and power selection scheme. Section 5 gives the experimental process and data. Finally, Section 6 concludes this paper.

3. Motivation

SIS has gradually developed into a popular research direction, so many SIS schemes have been proposed. Although there are many SIS schemes, SSIS is a simple and efficient SIS scheme. This simplicity is reflected in the easy-to-understand sharing principle and easy-to-use sharing steps, without other operations such as image preprocessing. The efficiency is reflected in the low time complexity of sharing, and the shadow image generated by sharing takes up less space, which is only $1/k$ of the original secret image. The advantages of time and space make the study of SSIS valuable.

Most of the shadow images generated by SSIS are noise images, which ensures the security of SIS. However, part of the shadow image of some images will leak part of the information of the original secret image. The leaked shadow image of this part destroys the confidentiality of SS and affects the security of sharing to a certain extent. In this paper, the purpose of our research on order number and power is to avoid such information leakage and improve the security of SIS. Order number and power are important parameters for SSIS. The occurrence of shadow image leakage must be related to the order number and power, but there is no research to prove this relationship. The influence of order number and power on SSIS can be found through research, and suggestions for selecting safer order number and power are given. When the user performs SSIS, by selecting a safe order number and power, the appearance of insecure shadow images is reduced, the generated shadow images are prevented from leaking the original secret image information, and the security of SSIS is provided to a great extent.

3.1. Our Contributions

(1) The function of each parameter in Shamir's polynomial is analyzed, and the selection suggestions of

the order number and power under different security conditions are given.

(2) A security evaluation algorithm for shadow images generated by SSIS is proposed, which can measure the degree to which the shadow image leaks the original secret image, that is, the security of the shadow image.

4. The Proposed Scheme

In this section, we describe the function of each parameter in Shamir's polynomial in detail and give some suggestions on the selection of order number and power, which solves the utility problem and selection problem of order number and power in Shamir's polynomial.

4.1. Parameters Analyses. In this section, the function of each parameter in Shamir's polynomial is described in detail, the security evaluation algorithm of the shadow image is proposed, and some suggestions are given for the choice of order number and power, which solves the utility problem of the order number and power in Shamir's polynomial and choice issues.

The position and number of secret pixels are inserted. When using SSS to share a secret image, that is, when only the first coefficient a_0 is inserted into the secret pixel s, and the remaining coefficients a_i are randomly selected from the finite field p, the shadow image will not leak the original secret image information, because the existence of random numbers ensures the security of shadow images. If a single pixel is inserted into the other coefficients a_i of Shamir's polynomial, and the coefficients other than a_i are random numbers, then the shadow image will not leak the original secret image information. This shows that the secret insertion position is not directly related to the leakage of the shadow image.

As the number of inserted secret pixels increases, the location of the secret pixels will have different options. Research has found that no matter how the position and number of the inserted secret pixels change, as long as the number of inserted secret pixels is less than k, the shadow image will not leak information visually. It is not difficult to find that the visual security of the shadow image can be protected as long as there are random coefficients in the polynomial, no matter the position or number of the inserted secret pixels is studied. The existence of random numbers causes shadow images to resemble noisy images. It can be seen that the existence of random numbers ensures the security of SIS, which has nothing to do with the selection of order number and power. However, there is no randomness of coefficient in Thien–Lin's scheme, so the security of its sharing should be maintained by other parameters.

4.1.1. The Type of Secret Image. In Thien–Lin's scheme, different secret images have different degrees of leakage, so we broadly divide the secret images into three categories: monochrome images, strong correlation images, and weak correlation images.

4.1.2. For Monochrome Images. A monochrome image is an image with all the same pixels. Sharing a secret image requires multiple participations of polynomials. But for monochromatic image, there is only one situation: the shared pixels are the same for each group, which leads to the fact that the shared values must be the same. This means that the shadow image is just a color change, which cannot guarantee the security of the secret image content.

4.1.3. For Strongly Correlated Images. In a strong correlation image, the pixel correlation degree is relatively close, and the adjacent pixel values are similar or the same, but they are not exactly the same as monochrome images, so there will be a problem of partial shadow images leaking part of original secret image content. We can deduce the formula as follows: when $k = 2$, $f(x) = (a_0 + a_1 x) \mod p = (a_1 (x + 1) + (a_0 - a_1)) \mod p = (a_1 X + \Delta a) \mod p$. Adjacent pixels are the same or similar, so Δa is visually unchanged, that is, $\Delta a = 0$. The randomness of pixels in the shadow image mainly comes from the influence of $a_1 X$. Using λX to represent a_1, we get $a_1 X = \lambda X^2$. This means that when $k = 2$, randomness is related to x^2. Similarly, the following formula can be obtained.

$$\begin{aligned} k = 2 &\sim x^2 \bmod p, \\ k = 3 &\sim x^3 \bmod p, \\ k = 4 &\sim x^4 \bmod p, \\ &\cdots \qquad . \end{aligned} \tag{1}$$

In order to better observe the influence of order numbers on the randomness of shadow pixels, corresponding scatterplots are drawn, as shown in Figure 1.

The randomness of the shadow image is closely related to the order number. By analyzing formula (1) and observing Figure 1, we get the following conclusion:

The larger the k, the greater the randomness of shadow pixels, and the greater the range of safe selection of order numbers .

This conclusion can be explained in many ways:

(1) The more regular the distribution of shadow pixels, the smaller the randomness, and the greater the risk of shadow image leakage. For example, in Figure 2, the distribution of green, blue, and red dots is regular, which means that the randomness is small.

(2) The larger the k, the smaller the probability of continuous k pixels being the same.

(3) The larger the k, the larger the pixel grouping, and the smaller the shadow image.

4.1.4. For Weakly Correlated Image. The correlation degree of pixels in weakly correlated images is small, and each group of pixels can be regarded as a group of random numbers.

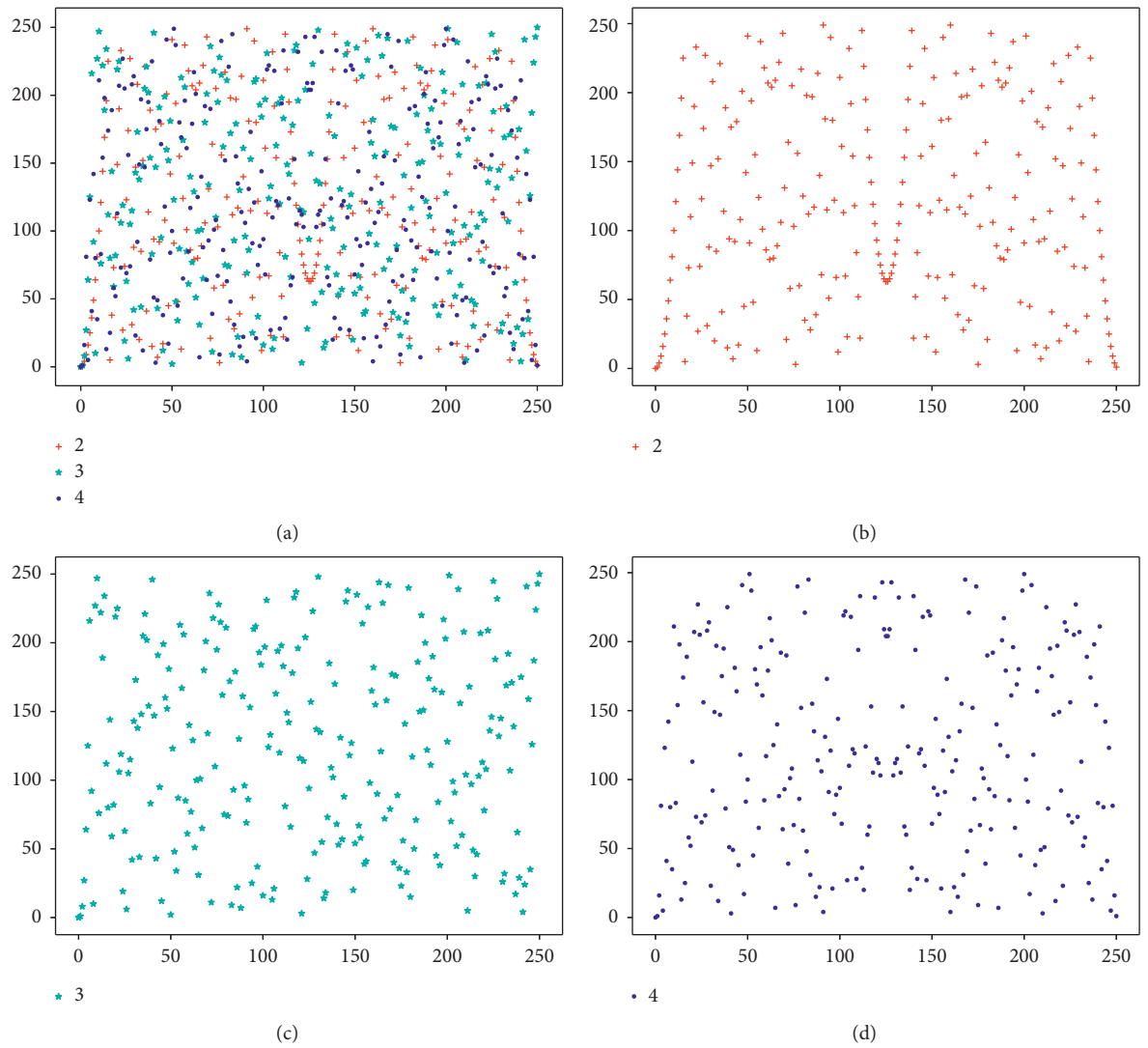


Figure 1: Random distribution. (a) $k = 2, 3, 4$. (b) $k = 2$. (c) $k = 3$. (d) $k = 4$.

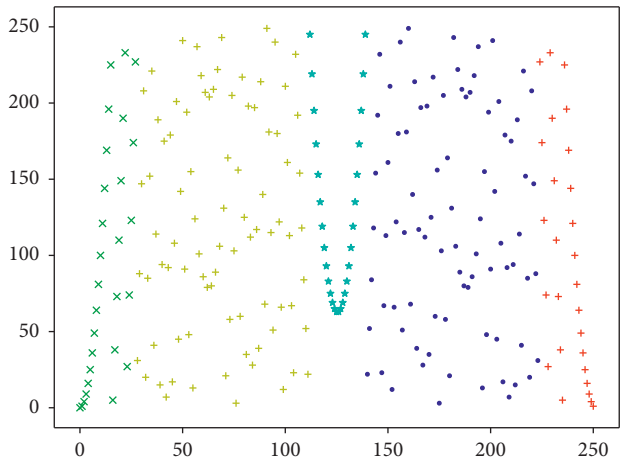


Figure 2: Distribution of $k = 2$.

This guarantees the security of SIS. But it is affirmative that applying the conclusion of strongly correlated images to weakly correlated images can greatly improve the security of sharing.

In this section, we have come to the conclusion that monochrome images are not suitable for sharing with SSIS and that the sharing of strong or weak correlation images requires a reasonable choice of order number and power.

4.2. Shadow Image Security Evaluation Algorithm. If the human visual system (HVS) is used to determine whether a shadow is unsafe, it is not only subjective and arbitrary, but also may have more or less errors. In order to remove human visual errors and subjective factors, we propose an algorithm for evaluating the quality of shadow images. After trying many evaluation methods such as information entropy and mutual information entropy, a new method is proposed. The algorithm is as follows Algorithm 1:

The algorithm is based on randomness, which guarantees the security of shadow images. Parameter ε represents the weighted variance of the distribution of shadow pixels after the corresponding pixels are shared.

Combining the above knowledge and the distribution histogram of shadow image pixels, we will introduce the design ideas of the algorithm. Here, we mainly introduce the algorithm with the classic threshold $k = 2$ as an example. Figure 3(a) is a comparison image, and Figure 3(b) is its pixel distribution histogram. Figures 4 and 5 are the shadow images with order numbers 1 and 59 and their corresponding shadow pixel histograms, respectively. We can clearly see that when the order number is equal to 1, the content of the secret image is leaked, and when the order number is equal to 59, the shadow image is safe. Corresponding to the distribution histogram of the pixels, we can see that when the order number is 1, the general rule of most pixels has not changed, there is only an offset, and the random degree of the pixels has not changed substantially. However, when the order number is 59, the distribution of secret pixels has undergone major changes, and the degree of randomness of pixels has been increased. The more the pixel distribution in the shadow image changes relative to the pixel distribution of the original secret image, the greater the randomness is, and the greater the visual change it brings.

In order to achieve the purpose of evaluating the randomness in the shadow image, we will judge each pixel and calculate the sum according to the weight of each pixel. To evaluate the randomness in a shadow image, we will determine each pixel and weigh it according to its weight. Here, as an example of a pixel with a pixel value of 52, Figure 6(a) shows the corresponding pixel distribution when the order number is 1, and Figure 6(b) shows the corresponding pixel distribution when the order number is 59.

We can see that when the order number is 59, the randomness of the corresponding pixels is greater. The distribution of other pixels is similar to that. After calculating them by weight, the randomness of the shadow image relative to the original secret image can be better evaluated.

The algorithm outputs a parameter ε, and the larger the parameter ε is, the safer it will be. According to the distribution rule of ε, we have established a security system in Table 1. Level A has an obvious leak and is not suitable for application. According to different safety needs, Levels B, C, and D can be chosen.

Based on the algorithm, it can be confirmed that the discrimination of shadow images requires images of equal size. So, we get the required contrast images by embedding the sharing algorithm, as shown in Figure 7.

The actual effect proves that leakage can be completely represented by parameter ε, as shown in Figure 8. When $k = 2$, Figures 8(a) and 8(b) have obvious leakage and cannot be applied in practice. The leakage of Figures 8(c) and 8(d) is not obvious; it can be used optionally. Figures 8(e) and 8(f) are noisy images, which can be used more safely.

The shadow image evaluation algorithm is feasible in practical applications, and the algorithm complexity will be analyzed. Steps 1 and 2 of the algorithm require statistics on the distribution of each pixel in secret and shadow images. In this process, all the pixels in the image need to be traversed, and the time complexity is $O(n^2)$. Steps 3 and 4 perform simple operations with less time complexity. Therefore, the overall time complexity of the algorithm is $O(n^2)$. After analysis, the feasibility and computability of the algorithm have apparent advantages.

4.3. Research and Suggestions on the Selection of Order Number and Power

4.3.1. Research and Analysis on Order Number. With the default power of $0 \sim (k-1)$, we find the following rules:

Rule 1: Information disclosure will be roughly symmetrical.

Rule 2: Information leakage is easy to happen at both ends.

Rule 3: The leakage of different thresholds is different, and the leakage degree is $k = 2 > k = 3 > k = 4$.

Rule 4: There is no simple relationship between information leakage and whether the order number is prime or sum.

Some selection suggestions are given, and users can choose according to their own security requirements.

Refer to Table 2 when $k = 2, 3, 4$:

When users use $f(x) = (a_0 + a_1 x + \cdots + a_{k-} \ 1x^{k-1}) \bmod p$ for secret image sharing, we give the top five order numbers, as shown in Table 3:

4.3.2. Research and Analysis on Power. It is impossible to exhaust all combinations of powers, because the space for power combinations is too large. Some representative power combinations have been selected; see Table 4 for details.

After extensive testing, the following rules are found:

Rule 1: There is no uniform distribution law, which is related to the combination of power.

Rule 2: Shadow image information leaks much less when the first power is not zero than when the first power is zero.

Rule 3: When the power combination is even, the order number is symmetrical.

Rule 4: Shared security increases with the highest power.

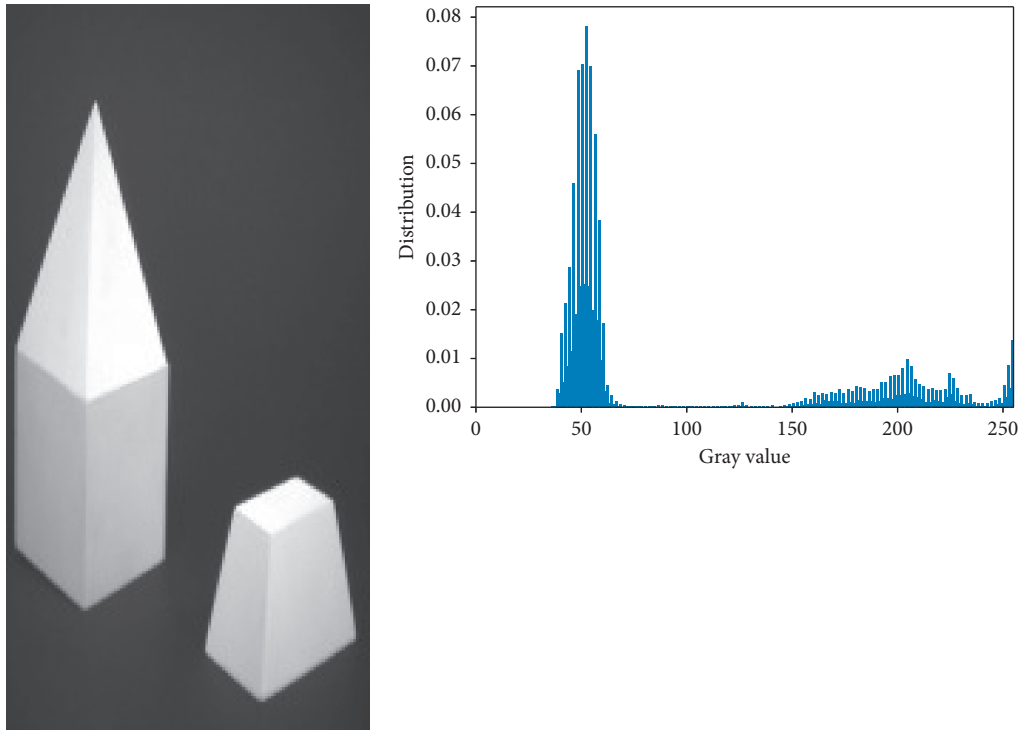
Rule 5, 6: Rules 3 and 4 in order number also apply here.

After comparative analysis, it is recommended that the first power is not zero, and all powers are not even at the same time.

For example,

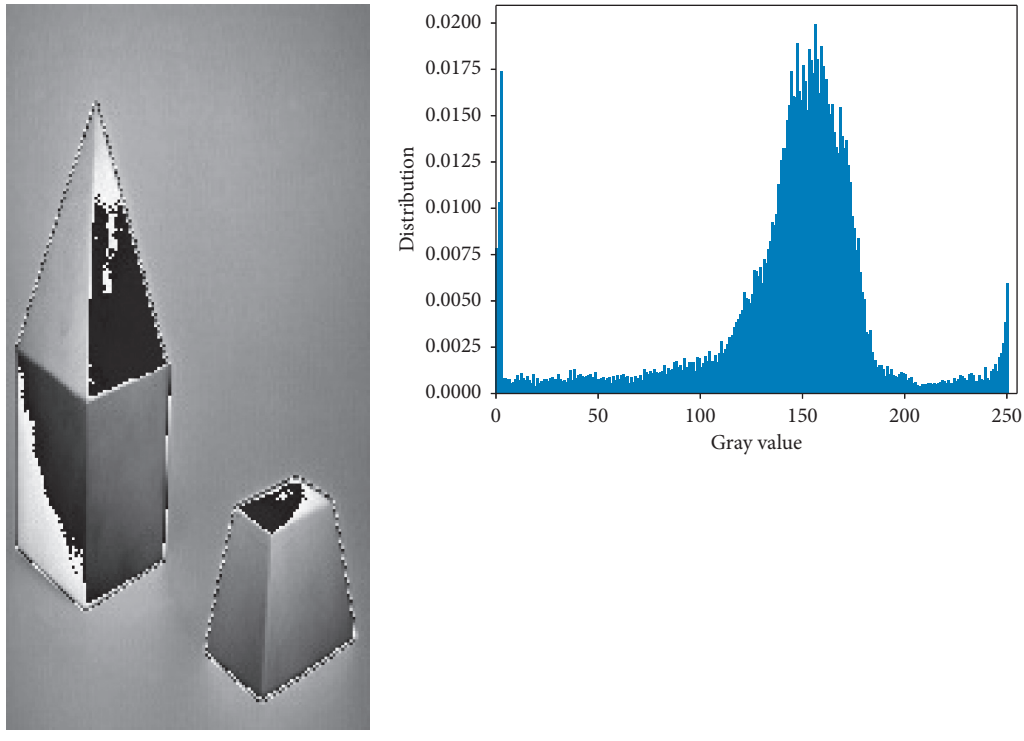
(1) when $k = 2$, the power combination that can be selected is $(1, 2)$.

(2) when $k = 3$, the power combination that can be selected is $(1, 2, 3)$.



(a) (b)

Figure 3: Indor.



(a) (b)

Figure 4: $X = 1$.

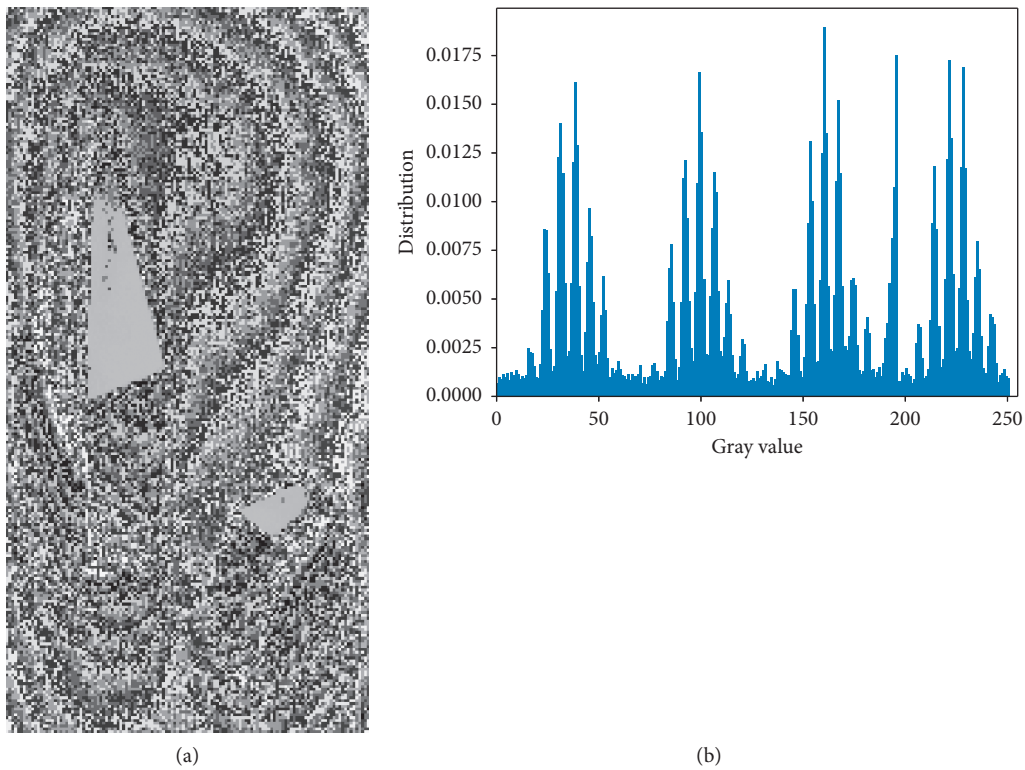


Figure 5: $X = 59$.

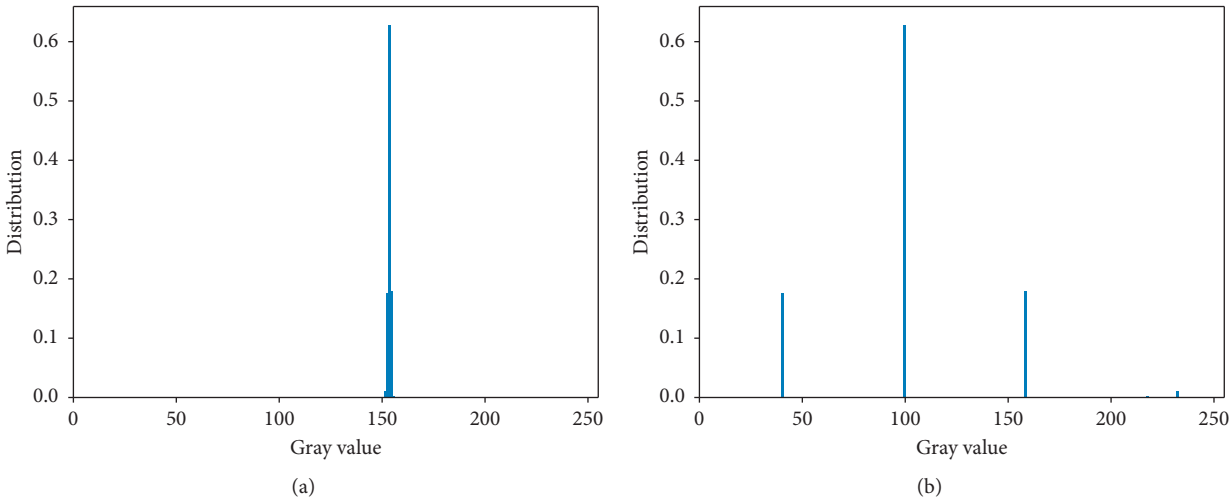
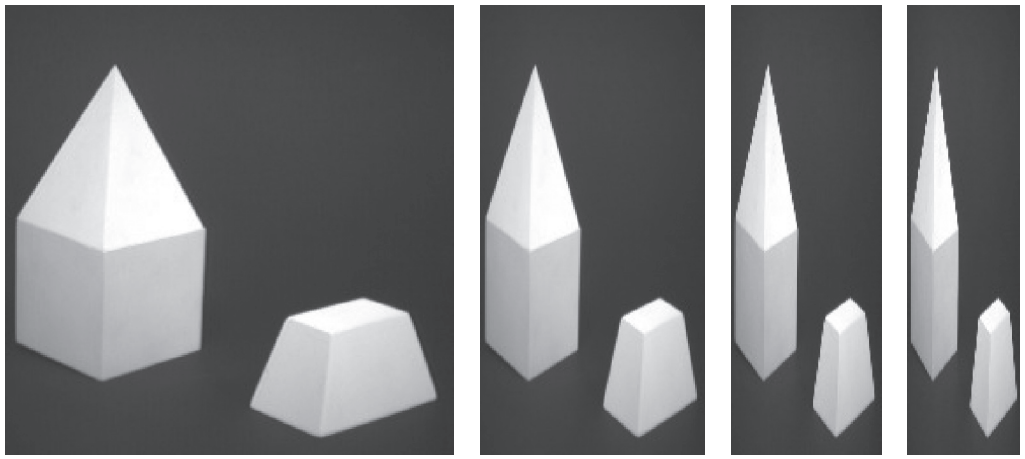


Figure 6: When $k = 2$, pixel = 52.

Input: original image, Shadow images
Output: evaluating indicator ε
Step 1: statistics of the distribution $D(o)$ and probability $P(o)$ of the pixels in the original secret images.
Step 2: $D(s)$ is obtained by counting the pixels of the corresponding location of $D(o)$ in shadow image.
Step 3: calculate the variance of $D(s)$ to get $V(s)$.
Step 4: get the weighted variance wv of a single pixel through $V(s)P(o)$.
Step 5: add up all wv and output Evaluating indicator ε.

Algorithm 1: Shadow image security evaluation algorithm.

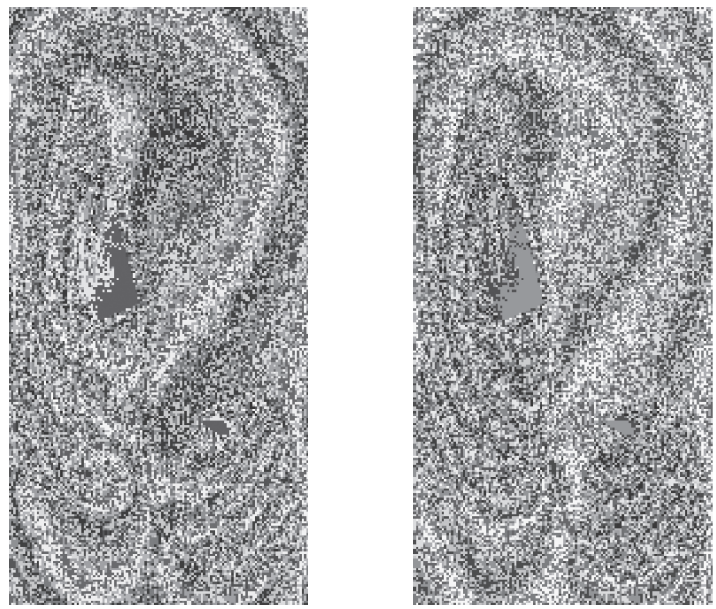


(a) (b) (c) (d)

Figure 7: Contrast image. (a) Indor; (b) 1/2Indor; (c) 1/3Indor; (d) 1/4Indor.

(a) (b) (c) (d)

Figure 8: Continued.



(e) (f)

Figure 8: The number below the image is the parameter ε corresponding to the shadow image. (a, b) belong to Level A. (c, d) belong to Level B. (e, f) belong to Level C. (a) 1145 (b) 2471 (c) 3310 (d) 3980 (e) 4202 (f) 4351.

Table 1: Safety level table.

Security level	A	B	C	D
ε	<3000	>3000	>4000	>5000

Table 2: Selection suggestions of order number.

	Security level	B	C	D
$k = 2$	Range of order numbers	[35,217]	[61,119; 130,186]	—
	Example shadow	Figure 9(a)	Figures 9(b) and 9(c)	—
$k = 3$	Range of order numbers	[5,244]	[7,242]	[18,227]
	Example shadow	Figure 10(a)	Figure 10(b)	Figure 10(c)
$k = 4$	Range of order numbers	[2,249]	[3,247]	[6,243]
	Example shadow	Figure 11(a)	Figure 11(b)	Figure 11(c)

(3) when $k = 4$, the power combination that can be selected is $(1, 2, 3, 4)$.

The security level of the shadow image obtained by sharing is mostly distributed in B, C, and D levels, which meets the requirements of safe sharing. User can choose safe order number between 10 and 240.

5. Experiments

In this section, we will introduce the process and design of the experiment. The experiment follows the following principles:

(1) Choose a strongly correlated image, Indor image for experimentation, and validate it with a weakly correlated image, Lena image.

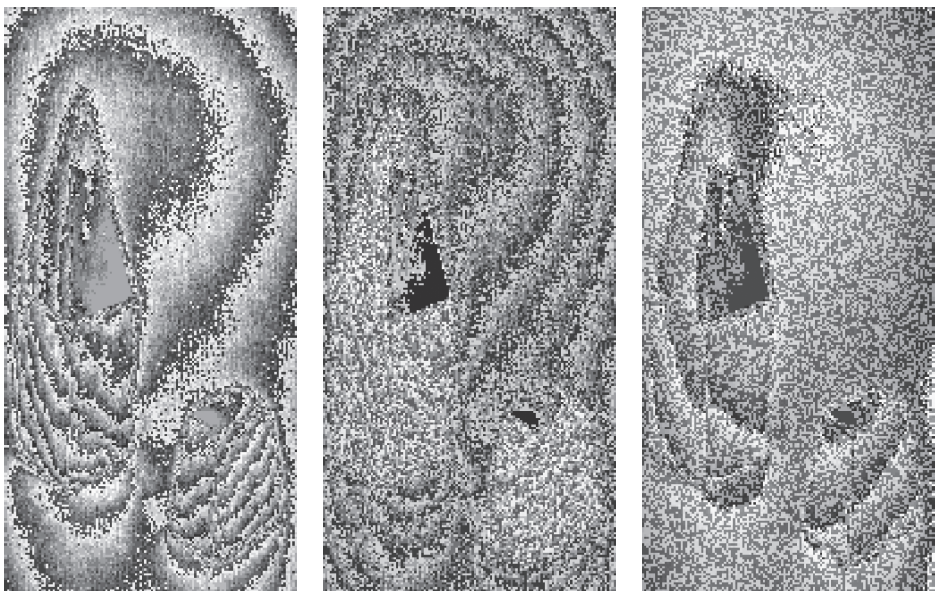
(2) In order to facilitate changing the insertion position, number, and power, the operation of polynomials is changed to the operation of matrix.

(3) List all order numbers, and select $n = 250$.

(4) Select some power combinations for experiments.

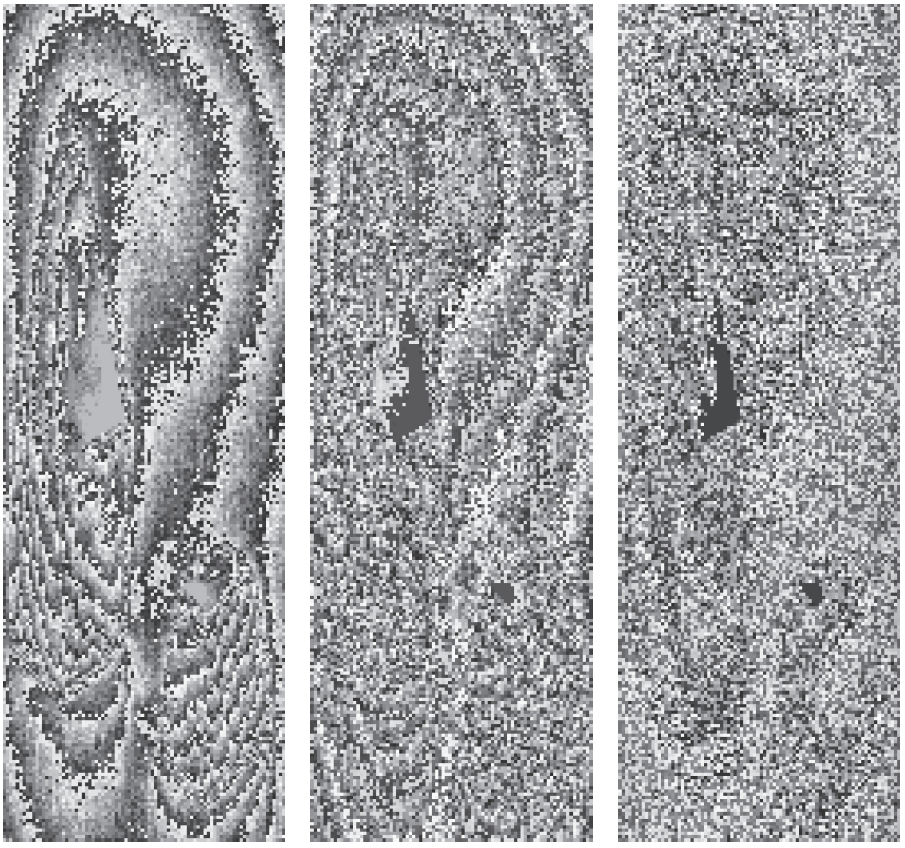
An experiment on SSIS verifies that there is a partial order number leak problem. Here, $k = 2$ is used as an example to show a set of pictures with varying degrees of leaks, such as Figure 12. It can be clearly seen that almost all of them have the problem of leaking the original secret image information, but the degree of leakage is different.

In the experiment, we not only used Indor images, but also other images for auxiliary verification. We find that the shadow image shared by Lena image is leaked, and the



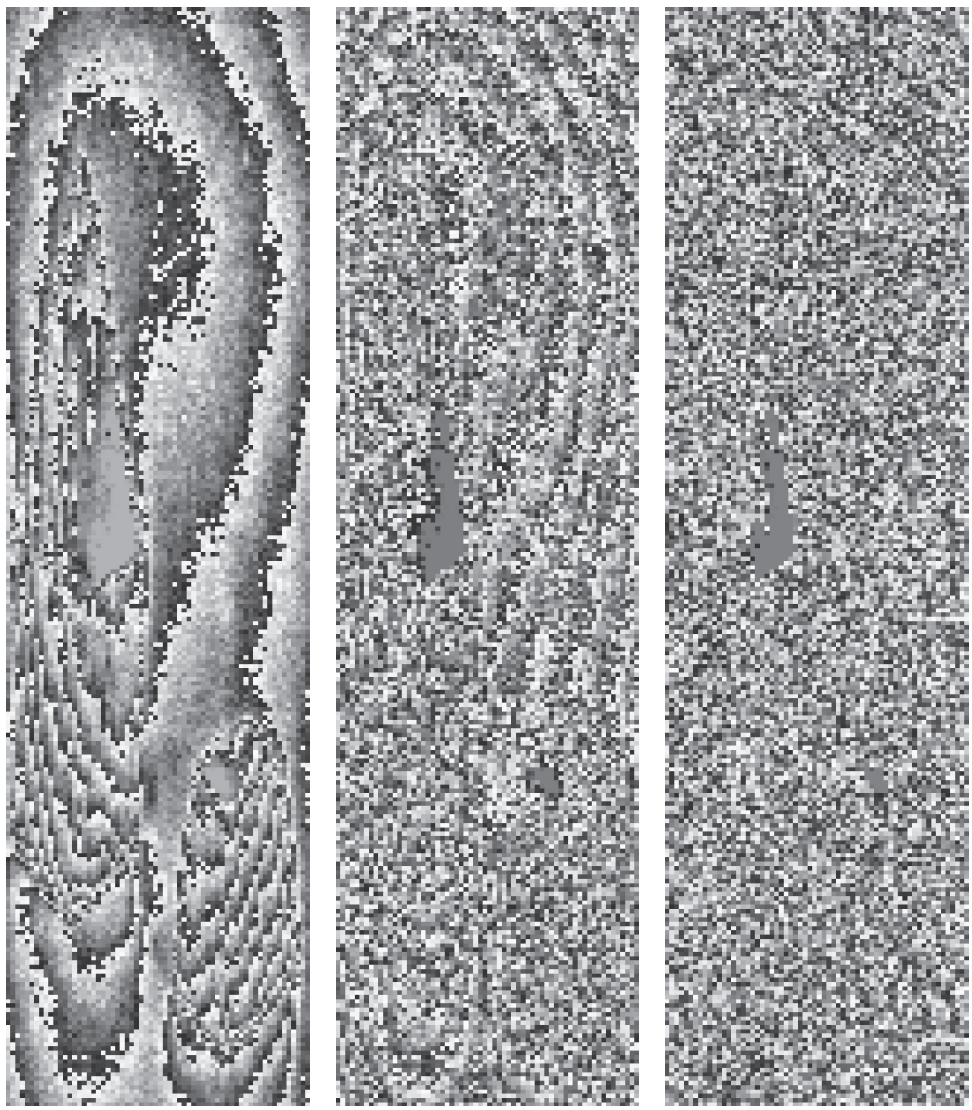
(a) (b) (c)

Figure 9: Shadow images in Table 2. The number below the image is the order number of the shadow image. (a) 35 (b) 61 (c) 130.



(a) (b) (c)

Figure 10: Shadow images in Table 2. The number below the image is the order number of the shadow image. (a) 5 (b) 7 (c) 18.



(a) (b) (c)

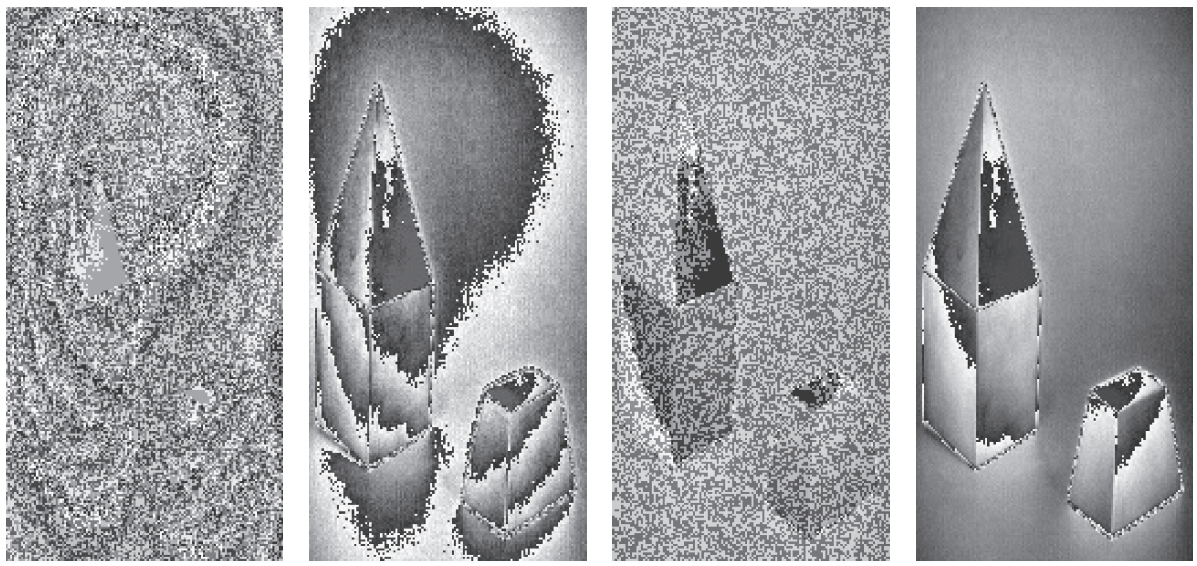
Figure 11: Shadow images in Table 2. The number below the image is the order number of the shadow image. (a) 2 (b) 3 (c) 6.

Table 3: The top five order numbers.

k	Order numbers
$k = 2$	109, 77, 152, 88, 185
$k = 3$	21, 145, 103, 197, 51
$k = 4$	56, 219, 178, 11, 161

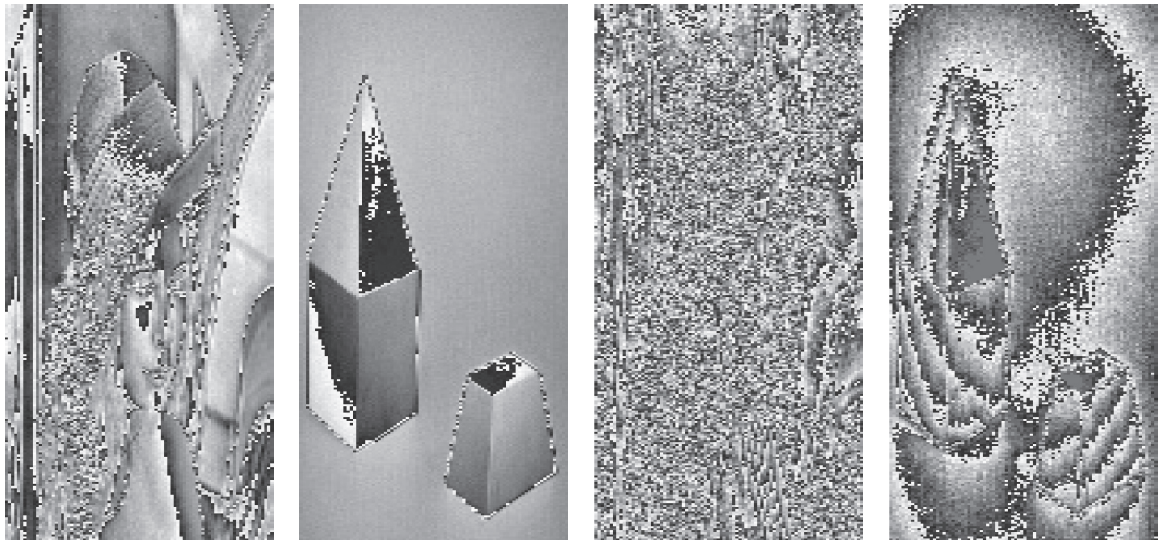
Table 4: Power combination.

The value of k	The value of power
2	(0,1); (0,2); (0,3); (1,2); (3,5); (3,8)
3	(0,1,2); (0,3,8); (0,5,7); (1,2,3); (1,3,5); (2,4,6); (3,5,7)
4	(0,1,2,3); (0,2,5,8); (0,5,7,11); (3,5,7,11)



(a) (b) (c) (d)

Figure 12: When $k = 2$. (a) No leaks; (b–d) is leakage, but the degree of leakage is different. The number below the image is the order number of the shadow image. (a) 159 (b) 13 (c) 125 (d) 5.



(a) (b) (c) (d)

Figure 13: When $k = 3, X = 245, 248$. (a, b) Both Lena's shadow and Indor's shadow leakage. (c, d) Lena's shadow has no leakage, but Indor's shadow has leakage. (a) L248 (b) I248 (c) L245 (d) I245.

corresponding shadow image shared by Indor image must be leaked; the shadow image shared by Indor image is leaked, but the corresponding shadow image shared by Lena image does not have to be leaked. Therefore, strongly correlated image's conclusions apply to the weakly correlated image. See, for example, Figure 13.

Other experimental results are given in other parts of this paper and are not discussed here. In this section, the result of the experiment fully proves that the security evaluation algorithm of the shadow image and the selection scheme of order number and power proposed by us are correct.

6. Conclusion

The shadow image shared by SSIS has the problem of leaking the secret information of the original image. This paper studies the utility of SSIS sharing order numbers and power. We analyzed the utility of each parameter in SSIS and gave suggestions for selecting the order number and power. Users can choose order power and number before sharing according to different security needs. The convenient selection of safe order number and power greatly improves the efficiency and security of SSIS. In this process, a security

algorithm to evaluate the security of shadow image is proposed, which greatly facilitates the detection of shadow images. Further theoretical analyses and application of the evaluation algorithm will be our future work.s

Data Availability

This article contains data to support the results of this study. If other data are needed, the data used to support the results of this study can be obtained from the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was funded by the Program of the National University of Defense Technology and the National Natural Science Foundation of China (Number: 61602491).

References

[1] J. A. Calvert, M. J. Schuster, and S. P. Radziszowski, "Security in computing," *Computers & Security*, vol. 16, no. 3, pp. 2645–2666, 1997.

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC, Boca Raton, FL, USA, 2007.

[3] J. Peng, B. Abd-El-Atty, H. S. Khalifa, and A. A. A. El-Latif, "Image watermarking algorithm based on quaternion and chaotic lorenz system," in *Proceedings of the Eleventh International Conference on Digital Image Processing (ICDIP 2019)*, Guangzhou, China, May 2019.

[4] L. Li, B. Abd-El-Atty, A. A. El-Latif, and A. Ghoneim, "Quantum color image encryption based on multiple discrete chaotic systems," in *Proceedings of the 2017 Federated Conference on Computer Science & Information Systems*, Prague, Czech Republic, September 2017.

[5] Y.-X. Sun, B. Yan, J.-S. Pan, H.-M. Yang, and N. Chen, "Reversible data hiding in encrypted color halftone images with high capacity," *Applied Sciences*, vol. 9, no. 24, p. 5311, 2019.

[6] R. L. Rivest, A. Shamir, and L. M. Adleman, "Cryptographic communications system and method (September 20 1983)," US Patent 4,405,829, 1983.

[7] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, "Exploiting the homomorphic property of visual cryptography," *International Journal of Digital Crime and Forensics*, vol. 9, no. 2, pp. 45–56, 2017.

[8] C.-N. Yang, Y.-C. Lin, and P. Li, "Cheating immune k-out-of-n block-based progressive visual cryptography," *Journal of Information Security and Applications*, vol. 55, Article ID 102660, 2020.

[9] X. Yan, X. Liu, and C. N. Yang, "An enhanced threshold visual secret sharing based on random grids," *Journal of Real-Time Image Processing*, vol. 14, pp. 61–73, 2015.

[10] X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible image secret sharing," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3848–3858, 2020.

[11] L. Li, M. S. Hossain, A. A. A. El-Latif, and M. F. Alhamid, "Distortion less secret image sharing scheme for internet of things system," *Cluster Computing*, vol. 22, pp. 2293–2307, 2017.

[12] P. Li, J. Ma, and Q. Ma, "(t, k, n) xor-based visual cryptography scheme with essential shadows," *Journal of Visual Communication and Image Representation*, vol. 72, Article ID 102911, 2020.

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

[14] N. A. Ebri, J. Baek, and C. Y. Yeun, "Study on secret sharing schemes (SSS) and their applications," in *Proceedings of the International Conference for Internet Technology & Secured Transactions*, Abu Dhabi, United Arab Emirates, December 2012.

[15] X. Yan, Y. Lu, C.-n. Yang, X. Zhang, and S. Wang, "A common method of share authentication in image secret," *IEEE Transactions on Circuits and Systems for Video Technology*, 2020.

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

[17] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[18] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, pp. 313–317, IEEE Computer Society, New York, NY, USA, June 1979.

[19] Z. Zhou, C. N. Yang, and Y. Cao, "Secret image sharing based on encrypted pixels," *IEEE Access*, vol. 6, pp. 15021–15025, 2018.

[20] X. Yan, Y. Lu, L. Liu, S. Wan, W. Ding, and H. Liu, *Security Analysis of Secret Image Sharing*, Springer, Singapore, Singapore, 2017.

[21] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 3, pp. 133–138, 1989.

[22] S.-J. Lin and J.-C. Lin, "VCPSS: a two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches," *Pattern Recognition*, vol. 40, no. 12, pp. 3652–3666, 2007.

[23] C.-N. Yang and C.-B. Ciou, "Image secret sharing method with two-decoding-options: lossless recovery and previewing capability," *Image and Vision Computing*, vol. 28, no. 12, pp. 1600–1610, 2010.