entropy

MDPI

Article

Meaningful Secret Image Sharing with Saliency Detection

Jingwen Cheng [1,2], Xuehu Yan [1,2,*], Lintao Liu [1,2], Yue Jiang [1,2] and Xuan Wang [1,2]

[1] College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China; chengjingwen87@nudt.edu.cn (J.C.); liuta1989@163.com (L.L.); jiangyue17@nudt.edu.cn (Y.J.); wangxuan21d@nudt.edu.cn (X.W.)

[2] Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China

* Correspondence: yanxh17@nudt.edu.cn

Abstract: Secret image sharing (SIS), as one of the applications of information theory in information security protection, has been widely used in many areas, such as blockchain, identity authentication and distributed cloud storage. In traditional secret image sharing schemes, noise-like shadows introduce difficulties into shadow management and increase the risk of attacks. Meaningful secret image sharing is thus proposed to solve these problems. Previous meaningful SIS schemes have employed steganography to hide shares into cover images, and their covers are always binary images. These schemes usually include pixel expansion and low visual quality shadows. To improve the shadow quality, we design a meaningful secret image sharing scheme with saliency detection. Saliency detection is used to determine the salient regions of cover images. In our proposed scheme, we improve the quality of salient regions that are sensitive to the human vision system. In this way, we obtain meaningful shadows with better visual quality. Experiment results and comparisons demonstrate the effectiveness of our proposed scheme.

Keywords: secret image sharing; random elements utilization model; statistical correlation; saliency detection; meaningful shadows; polynomial-based SIS

check for updates

Citation: Cheng, J.; Yan, X.; Liu, L.; Jiang, Y.; Wang, X. Meaningful Secret Image Sharing with Saliency Detection. *Entropy* **2022**, *24*, 340. https://doi.org/10.3390/e24030340

Academic Editor: Ercan Kuruoglu

Received: 23 January 2022
Accepted: 22 February 2022
Published: 26 February 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the development of artificial intelligence and internet technology, many studies have focused on the information security. Large amounts of images are transmitted in the cloud networks every day. It is worth paying attention to the transmission safety of sensitive images such as remote-sensing images and military images. Image encryption [1] and information hiding [2,3] are traditional image protection technologies, but they are not applicable in some scenarios. Secret image sharin g (SIS), as one of the applications of information theory in information security protection, has been widely used in many areas, such as blockchain [4], identity authentication [5,6] and distributed cloud storage [7,8].

In a secret image sharing scheme with a (k, n) threshold [9], a secret image is divided into n shadows and sent to n participants. If k or more shadows are collected, the original secret can be reconstructed. In contrast, less than k shadows reveal nothing of the secret image.

Generally, there are three main branches in SIS: visual cryptography (VC) [10,11], Chinese Remainder Theorem (CRT)-based SIS [12–14] and polynomial-based SIS (PSIS) [15–18]. PSIS is always adopted because of the lossless recovery, no pixel expansion and good visual quality shadows. The primitive polynomial can be used to realize PSIS, and Lagrange interpolation is exploited to reconstruct the original secret image. The polynomial multiplication is required as the main operation in Lagrange interpolation with a higher computational cost than VC and CRT-SIS. The Number Theoretic Transform (NTT) can be used to improve the performance of polynomial multiplication [19–21]. Thus, the recovery efficiency is improved, especially with large polynomial degrees. According to the characteristics of

images, the existing PSIS is more commonly implemented over the integer field with a prime P, which is illustrated in Section 2.1.

In traditional SIS, the shadows are usually noise-like. These noise-like shadows easily attract the attention of attackers. On the other hand, it is difficult to distinguish noise-like shadows, which presents difficulties in shadow management. To facilitate shadow management and ensure transmission security, some researchers have committed to generating meaningful shadows. Meaningful SIS was first proposed by Ateniese et al. [22]. They applied visual cryptography to generate meaningful binary shadows. According to different design concepts, meaningful SIS can be classified into two categories.

The first design concept combines SIS with information hiding schemes. First, traditional SIS schemes are employed to share the secret image and obtain noise-like shadows. Then, an information hiding scheme is applied to embed noise-like shadows into cover images to make shadows meaningful. In the recovery phase, the noise-like shadows are first extracted from the covers, and the original secret image can be reconstructed by the recovery algorithm.

Yuan et al. [23] applied multi-cover adaptive steganography to share natural images. The secret image is adaptively embedded into the textured regions of cover images, but pixel expansion occurs in their scheme. Cheng et al. [24] employed a Gray code to obtain meaningful shadows. In their method, AMBTC compression is used to reduce the transmission bit rate. Chiu et al. [25] presented a $(2, n)$ threshold progressive visual cryptography scheme to generate meaningful shadows. He et al. [16] used LOCO-I compression to reduce the statistical correlations between neighboring pixels and obtain meaningful shadows based on steganography. Derya et al. [26] introduced a method to generate meaningful shares with Arabic letters. They embedded shares into the R, G and B channels of their RGB cover images with steganography.

All the abovementioned schemes are based on an information hiding scheme to generate meaningful shadow images. Shadows in these schemes possess some information hiding properties, such as steganography resistance. However, limited by the embedding rate of information hiding schemes, these sharing schemes must minimize the size of the secret image. To obtain better visual quality, they usually have pixel expansion.

The second design concept does not require steganography. With the constraints of secret pixel values and cover pixel values, researchers have improved the sharing algorithm to generate a shadow pixel, which is close to its corresponding cover pixel. As a result, the shadows are meaningful and similar to the cover images.

Wu et al. [27] constructed meaningful shadows based on random grid visual cryptography. Their covers consisted of binary images. Yang et al. [28] applied digital halftoning technology to improve the visual quality of meaningful binary shadow images. Liu et al. [29] utilized a sharing map and a sharing pool to obtain meaningful shadows. They made the most significant bit of each shadow equal to the higher bit of the corresponding cover image. Yan et al. [30] presented a CRT-based SIS that can generate meaningful shadows. A modular operation is applied to share the secret image. They also used binary images as covers.

These methods mostly use binary cover images, which have lower visual quality than grayscale images. Some of them only use one cover image; thus, their shadows are all similar to the cover with the same content. Generally, neither of these two kinds of schemes has high visual quality, and the secret images are shared as pure data. However, as natural images, adjacent pixels in a cover image have a strong correlation in color, texture and luminance, which are not considered in the above two kinds of schemes.

The motivation of this article is to propose a meaningful SIS scheme with saliency detection to improve the visual quality of shadows. Since the salient regions are quite different from adjacent regions in color, texture, or luminance, human attention always focuses on an image's salient regions. In the proposed scheme, we try to improve the visual quality of salient regions in shadows; then, the overall visual quality can be improved apparently. LC algorithm is utilized to identify the salient regions, and a random elements

utilization model is exploited to screen shared values and distribute more identical bits to salient regions. In this way, salient regions in shadows are more similar to the same salient regions in covers. The experiment results show that our shadows have better visual quality than the relative schemes.

We organize this article as follows: Section 2 introduces the principle of polynomial-based SIS and a saliency detection method named LC. The proposed scheme is presented in Section 3. Experiments and comparisons with relative schemes are presented in Section 4. Section 5 concludes this paper.

2. Preliminaries

2.1. Polynomial-Based Sis

In (k, n) threshold polynomial-based SIS, as seen in Equation (1), a $(k-1)$ degree polynomial is constructed in a finite field $GF(P)$, where P is a prime number. In the sharing phase, we set the secret pixel value $s = a_0$ and randomly select the coefficients a_1, a_2, $\cdots$, and a_{k-1} within the interval $[0, P)$. $f(i)$ is calculated as the share value according to Equation (1). After all secret pixel values have been shared, n shadows can be obtained.

$$f(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) \bmod P \tag{1}$$

As described in Equation (2), Lagrange interpolation is used to reconstruct the original polynomial if k or more shares are gathered. In this way, k coefficients are calculated, and a_0 is the recovered secret pixel value s'. The polynomial cannot be reconstructed with fewer than k shares; consequently, no secret information can be revealed.

$$f(x) = \sum_{i=1}^{k} f(x_i) \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{(x - x_j)}{(x_i - x_j)} \tag{2}$$

2.2. Saliency Detection

The human vision system can quickly determine the interesting regions in a complex image [31]. The salient regions are more likely to attract the attention of the human eyes because they are quite different from other regions in terms of texture, color and luminance. Saliency detection is used to simulate the human vision system to obtain the salient regions in an image.

Here, we introduce a pixel-level saliency detection algorithm based on a pixel's contrast to all other pixels (the so-called LC algorithm). The LC algorithm is proposed by Zhai and Shah [32], and it is one of the state-of-the-art traditional methods for saliency detection.

The LC algorithm builds a saliency map with a color contrast between pixel values. The saliency value of pixel P_t is defined as Equation (4), which equals the sum of Euclidean distances between the pixel value of P_t and all the other pixels of image I.

$$Sal(P_t) = \sum_{\forall P_i \in I} \|P_t - P_i\| \tag{3}$$

The LC algorithm is suitable for grayscale images because the saliency value of pixel P_t is the sum of Euclidean distance between pixel P_t and all the other pixels in the image. The saliency value computation for a pixel P_t can be optimized with the use of image color histograms as:

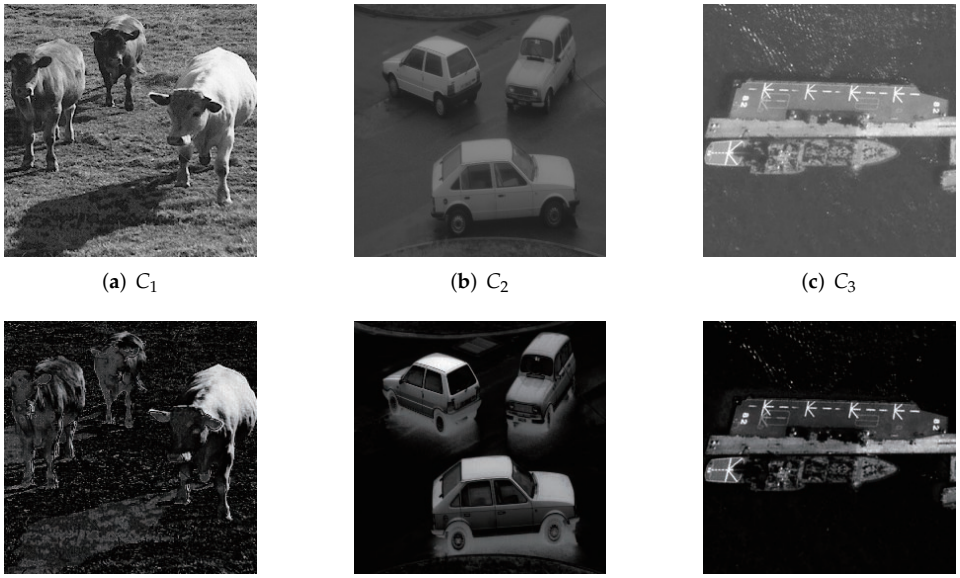
$$Sal(P_t) = \sum_{n=0}^{255} f_n D(t, n) \tag{4}$$

where t is the color value of pixel P_t; $D(t, n)$ is the color difierence between P_t and P_n; f_n is the probability of pixel value n in image I.

Figure 1 illustrates our experiment images their saliency maps with LC algorithm. Compared with other saliency detection methods [33–35], such as AC [36], FT [37], CA [38],

RC [33], LC takes a little running time because LC is purely computational with low computational complexity. According to Figure 1 and the comparing results illustrated in [33], the precision of LC is satisfied, and the saliency maps with LC algorithm are accordant with human eye perception. However, other traditional saliency detection like FT [37], AC [36] and RC [33] can also be used in our scheme after some adjustments since they are designed for color images.

Recent saliency detection researches are focused on Convolutional Neural Networks (CNN). The CNN-based saliency detection methods may obtain more precise saliency maps. However, the CNN models are complex, which leads to high computation complexity and long running time. Moreover, the LC algorithm is good enough for our scheme as demonstrated in our experiment results.



(**a**) C_1 (**b**) C_2 (**c**) C_3

(**d**) LC_1 (**e**) LC_2 (**f**) LC_3

Figure 1. LC algorithm results. (**a**–**c**) original grayscale images; (**d**–**f**) saliency maps for original images.

3. The Proposed Scheme

Here, we introduce our proposed scheme. First, the concept of our method is presented. Then, the details of our sharing method are described in Algorithm 1.

Algorithm 1. The Sharing Phase of Our Proposed Scheme.

Input: a grayscale secret image S with a size of $W \times H$; n grayscale cover images C_i with a size of $W \times H$;
Output: n meaningful shadows SC_1, SC_2, ...,SC_n.
Step 1: Use the LC algorithm to calculate the saliency values for every pixel in cover C_i. Note the saliency values as Sal_i^1, Sal_i^2, ..., $Sal_i^{W\times H}$.
Step 2: Compare Sal_1^t and Sal_2^t,...,Sal_n^t, which are the saliency values of the same pixel position P_t of n covers.
Step 3: Utilize the random elements utilization model and the result of Step 2 to screen the shadow pixel values.
Step 4: Repeat Step 2 and Step 3 until all secret image pixels have been shared.
Step 5: Output n meaningful grayscale shadow images $SC_1, SC_2, \cdots SC_n$.

3.1. Design Concept

The design concept of our scheme is illustrated in Figure 2. In our method, the LC algorithm is utilized to calculate the saliency values (noted as Sal_i^1, Sal_i^2, ..., $Sal_i^{W\times H}$) for every pixel of each cover image. The saliency value indicates the pixel's significance in

the image. A larger saliency value means a more significant role that the pixel plays in the image. The saliency maps of covers can be obtained through the LC algorithm.

To generate meaningful shadows, we set some specific conditions during the sharing phase. In terms of visual quality, the higher bits of a pixel value are more important than the lower bits. If we keep more higher bits identical for corresponding pixels, the two images are more similar. However, there is a limit to the sum of identical bits, and for n different cover images, the salient regions are different. If we distribute more identical bits to salient regions, the shadow quality will be better.

The design concept of our scheme distributes more identical bits to salient regions according to the saliency values. A random elements utilization model is used to screen the shadow pixels that satisfy these specific conditions. In this way, the salient regions in shadows are more similar to the same regions of the corresponding cover image. Therefore, the shadows will obtain better visual quality.

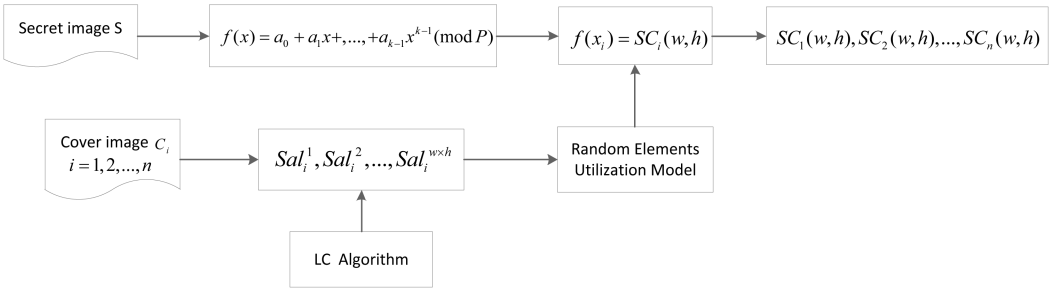


Figure 2. Design concept of the proposed scheme.

3.2. Random Elements Utilization Model

According to the principle of PSIS, coefficients a_i $(1 \leq i \leq k-1)$ are selected randomly to gain shared values. Different a_i lead to different shared values, and the coefficients a_i are regarded as the random elements in the sharing phase.

The random elements utilization model is exploited to screen shared values to obtain meaningful shadows with better quality. The sum of identical bits is expected as more as possible to obtain better visual quality, t. Since w_i is noted as the identical higher bits that distribute to SC_i, we correlate the random elements utilization model with a maximize problem as follows.

$$Maximize \sum_{i=1}^{n} w_i \tag{5}$$

$$s.t. \begin{cases} \sum_{i=1}^{n} w_i \leq 8(k-1) \\ f(x_t) = s + \sum_{m=1}^{k-1} a_m x_t^m \bmod P \\ a_m \in \mathrm{Z}, a_m \in (0, P] \\ s \in [0, 255] \\ f(x_t) \in [0, 255] \\ t = 1, 2, ..., n \end{cases} \tag{6}$$

The maximization problem can be solved by the integer linear programming technique. According to the random elements utilization model, identical higher bits w_i are distributed to SC_i, respectively. The shared values in SC_i can be screened while keeping w_i identical bits with the corresponding cover pixels; thus, the shadows are meaningful and similar to the corresponding covers.

3.3. Our Scheme

The detailed sharing steps are described in Algorithm 1, and we make the following points:

1. The salient regions have a greater influence on human visual perception than other regions. We improve the visual quality of the shadows by improving the visual quality of the salient region.

2. We apply the LC algorithm to calculate the saliency values for every pixel in each cover. Saliency values are used to measure the importance of corresponding pixels. A larger saliency value indicates that the cover pixel is in a salient region, while a cover pixel with a smaller saliency value is in a non-salient (less important) region.
3. In our scheme, the sum of identical higher bits for all shadows is limited. With the random elements utilization model and the comparison results in Step 2, we distribute more identical higher bits to salient regions and less to non-salient regions. Thus, the salient regions obtain better visual quality and are more similar to corresponding regions in cover images. Moreover the distribution process is adaptive to different shadow images.
4. There is a limitation on the sum of identical higher bits for all shadows. Since we choose 257 as the prime number, the total number of sharing values is $257^{k-1} \approx 2^{8(k-1)}$. In our scheme, the total number of satisfied sharing values is $2^{\sum_{i=1}^{n} w_i}$. To ensure the successful sharing process, the sum of identical higher bits should be subject to $\sum_{i=1}^{n} w_i \leq 8(k-1)$.
5. Polynomial-based SIS is used to share the secret pixels, and a prime number P of 257 is chosen to ensure lossless recovery. In the recovery phase, the secret image can be losslessly reconstructed by Lagrange interpolation. The recovery operation complexity is $O(klog^2k)$ [39].

4. Experiments and Discussion

In this section, we first exhibit our experimental results. Then, comparisons with relative schemes are performed to show the effectiveness of our proposed scheme with the same threshold and secret image. In addition, a discussion is provided.

4.1. Image Illustration

The experimental results of our proposed scheme with the $(2, 2)$ threshold are exhibited in Figure 3; Figure 3a shows the grayscale secret image. Two grayscale cover images are shown in Figure 3b,c; the recovered secret image is illustrated in Figure 3d; Figure 3e,f demonstrates two shares. The shares are not noise-like but meaningful. They are similar to the corresponding cover images. The details of the shadows can also be accurately recognized. For example, as Figure 3e illustrates, the lines on the deck of the warship can be recognized easily and accurately. All the shares and reconstructed secret images have the same size as the original secret image, and no pixel expansion occurs.

4.2. Quality Evaluation Metrics

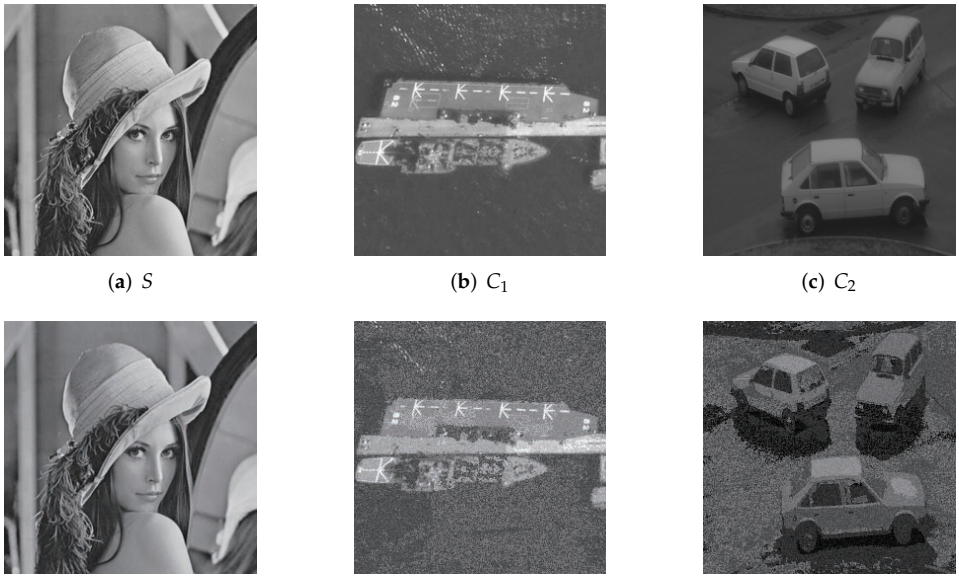
Our experiment evaluates the image quality with the statistical correlation between shadows and corresponding covers. Here, three statistic-based metrics are introduced to obtain the statistical correlation between two images. In SIS, peak signal-to-noise-ratio (PSNR), structural similarity (SSIM) [40], and universal quality index (UQI) [41] are widely used statistic-based metrics.

PSNR between image S and S′ is calculated as Equation (7).

$$PSNR = 10\log_{10}\frac{255^2}{MSE}(dB) \tag{7}$$

$$MSE = \frac{1}{W \times H}\sum_{i=1}^{W}\sum_{j=1}^{H}\left[S'(i,j) - S(i,j)\right]^2 \tag{8}$$

where MSE represents the mean square error of image S′ and image S. The value range of PSNR is $[0, +\infty]$. The larger the value of PSNR is, the more similar the two images are.



(**a**) S (**b**) C_1 (**c**) C_2

(**d**) S'_{12} (**e**) SC_1 (**f**) SC_2

Figure 3. (2,2) threshold experimental results of our proposed method; (**a**) grayscale secret image; (**b**,**c**) two grayscale cover images; (**d**) recovered secret image with two shares; (**e**,**f**) two meaningful shadow images.

Different from PSNR, SSIM evaluates image similarity from brightness, contrast, and structure. SSIM is defined as Equation (9).

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \tag{9}$$

where

$$\begin{aligned} l(x,y) &= \frac{2\mu_x\mu_y+C_1}{{\mu_x}^2{\mu_y}^2+C_1} \\ c(x,y) &= \frac{2\sigma_x\sigma_y+C_2}{{\sigma_x}^2{\sigma_y}^2+C_2} \\ s(x,y) &= \frac{2\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3} \end{aligned} \tag{10}$$

UQI can also be used to evaluate image distortion, and its value range is $[-1,1]$. The larger value of UQI indicates less distortion and better quality. UQI is calculated as follows.

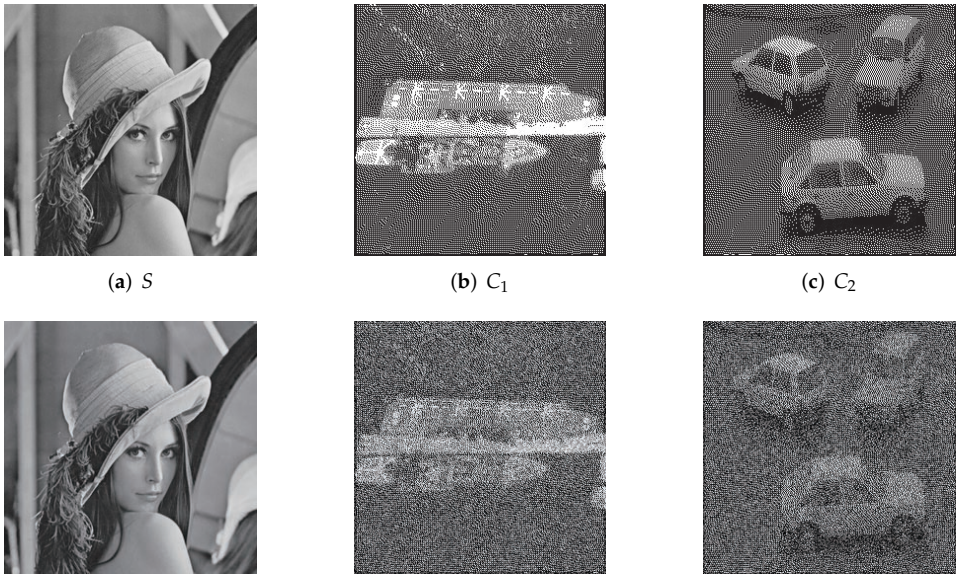
$$UQI = \frac{4\mu_x\mu_y\sigma_{xy}}{(\mu_x^2+\mu_y^2)(\sigma_x^2+\sigma_y^2)} \tag{11}$$

The three statistic-based metrics can be directly used for grayscale images. In the comparison experiment, the input binary images are first grayed, and the pixel value is multiplied by $P-1$. Then, the three metrics can be used to evaluate the image quality.

4.3. Comparisons with Relative Methods

In this section, we compare the proposed scheme with two relevant meaningful SIS methods: Liu et al. [29] and Yan et al. [30]. These methods both obtain meaningful shadows. To better show the advantages of our proposed scheme, we use the same secret image and thresholds in the comparative experiments.

Liu et al. [29] obtained meaningful shadows by employing a sharing map and sharing pool. The sharing pool is determined by the secret pixel values and cover pixel values. Different binary images are used in their method as covers. They choose appropriate shared pixel values from the sharing pool to obtain meaningful shadows. We use two binary covers that have the same content as our covers to realize their $(2,2)$ threshold experiment. The results are illustrated in Figure 4.



(**a**) S (**b**) C_1 (**c**) C_2

(**d**) S'_{12} (**e**) SC_1 (**f**) SC_2

Figure 4. (2,2) threshold experimental results of Liu et al.; (**a**) grayscale secret image; (**b**,**c**) binary cover images; (**d**) recovered secret image; (**e**,**f**) meaningful shadow images.

Yan et al. [30] presented a meaningful SIS scheme based on the Chinese Remainder Theorem. They also utilized binary images as covers, and the secret image was shared by a modular operation. We also realize their scheme with a (2,3) threshold. The results are exhibited in Figure 5e–h.

To show the effectiveness of saliency detection in our scheme, we designed a comparison experiment without saliency detection. In the comparison experiment, the threshold and the sum of the identical bits are equal our proposed scheme. We removed the saliency detection, and identical bits were distributed randomly among each shadow. The comparison experiment we refer to as IBDR. Figure 5i–l shows the $(2, 3)$ threshold results of the IBDR scheme.

The results of our proposed scheme with the $(2, 3)$ threshold are illustrated in Figure 5m–p. Compared with our experimental results with relative schemes in Figures 4 and 5, we can see that the visual quality of the shadows in our scheme is obviously better than Liu et al. [29] and Yan et al. [30]. In their shadows, only the outlines of the objects can be distinguished. In the IBDR scheme, the visual quality is higher than Liu et al. and Yan et al., but it failed to display some of the details of the shadows. For example, in Figure 5l, we can identify that it is a warship, but we cannot determine the lines on the deck, and the details of the ship cannot be recognized clearly. In contrast, in the results of our proposed scheme, the lines on the deck of the warship are accurately illustrated in Figure 5p. Moreover, as shown in Figure 5k,o, the outline of the cars in our scheme is clearer than that of the IDBR scheme.

The visual quality of images can be measured by PSNR, SSIM and UQI. Tables 1 and 2 exhibit the statistical results of our proposed scheme and the comparison schemes. Compared with Liu et al. [29] and Yan et al. [30], the visual quality is improved significantly. This is also demonstrated by the PSNR values in Table 1, but the PSNR values of IBDR are close to our scheme. For further analysis, we calculated SSIM and UQI for these two schemes, as shown in Table 2. The statistical data show that our method performs better in SSIM and UQI.

(**a**) S (**b**) C_1 (**c**) C_2 (**d**) C_3

(**e**) S'_{123} (**f**) SC_1 (**g**) SC_2 (**h**) SC_3

(**i**) S'_{123} (**j**) SC_1 (**k**) SC_2 (**l**) SC_3

(**m**) S'_{123} (**n**) SC_1 (**o**) SC_2 (**p**) SC_3

Figure 5. $(2,3)$ threshold experimental results of IBDR, Yan et al. and our proposed method; (**a**) grayscale secret image; (**b**–**d**) three grayscale cover images; (**e**–**h**) results of Yan et al.'s scheme; (**i**–**l**) results of IBDR scheme; (**m**–**p**) results of our proposed scheme.

Table 1. PSNR comparison between the proposed scheme and relative schemes.

Threshold	Schemes	Shadows1	Shadow2	Shadow3	Average
(2,2)	Liu	10.6781	10.6942		10.6861
	Ours	22.4381	20.4256		21.4318
(2,3)	Yan	7.9441	8.2266	8.1357	8.1021
	IBDR	16.4911	17.2531	17.5863	17.1101
	Ours	16.7203	18.2884	18.2662	17.7583

Table 2. SSIM and UQI comparison between our proposed scheme and BIDR scheme.

Schemes	Metrics	Shadows1	Shadow2	Shadow3	Average
IBDR	SSIM	0.4362	0.1089	0.1677	0.2376
	UQI	0.4659	0.0751	0.1461	0.2291
Ours	SSIM	0.4647	0.1599	0.2213	0.2817
	UQI	0.4892	0.1182	0.1853	0.2642

4.4. Analysis and Discussion

According to Figures 4 and 5 and Tables 1 and 2, some analyses are given as follows.

1. Our scheme significantly improved visual quality compared with Liu et al. [29] and Yan et al. [30].
2. The PSNR of the IBDR method is close to ours. However, PSNR is calculated based on the discrepancy between the corresponding two pixel values, while the visual characteristics of human eyes are not taken into account. For example, human eyes are sensitive to luminance and texture and are usually influenced by the neighboring regions around the target object. The PSNR values are often inconsistent with the subjective judgment of human eye perception.
3. To further compare our scheme with IBDR, we calculated the indicators SSIM and UQI, which can better reflect the overall structure of images. As exhibited in Table 2, the higher values of SSIM and UQI show that our scheme is more effective than IBDR.
4. In our scheme, saliency detection is applied, which can effectively improve the visual quality of salient regions in shadows. For instance, the lines on the deck of the warship in Figure 3e can be clearly distinguished, but they are blurred in the corresponding shadows of other relative schemes. Our scheme exhibits the details of shadow images more accurately. The structural characteristics are used in saliency detection, so the outline of the cars in Figure 5o are clearer than in Figure 5k. These are also demonstrated with SSIM and UQI in Table 2.
5. The relative meaningful SIS schemes process each pixel individually. However, the color, texture and luminance among neighboring pixels have a strong correlation. They are sensitive to human eye perception. Our proposed scheme takes the correlation among neighboring pixels and structural characteristics into account by utilizing saliency detection. According to the random elements utilization model, the identical higher bit distribution process is adaptive to different shadow images. Then, the visual quality of saliency regions of shadows can be improved adaptively.
6. Our scheme performs well with small thresholds such as $(2, 2)$ and $(2, 3)$. For larger thresholds such as $(4, 4)$ or $(4, 5)$, the total number of identical bits is $8(k - 1) = 24$. Because there are enough identical higher bits for each pixel and the lower bits have a smaller influence on visual quality, both the salient and less salient regions can obtain satisfied visual quality. In this condition, saliency detection is not very effective with large thresholds.
7. The LC algorithm can identify the salient regions accurately in our scheme. However, there are also some limitations. The sum of Euclidean distances between pixel values is calculated to obtain the saliency map in the LC algorithm. Mistakes will be involved when pixels with rare pixel values mistakenly gain high saliency values. Other saliency detection methods, such as FT [37], AC [36] and RC [33], can also be used in our scheme to obtain accurate saliency maps.

5. Conclusions

In this article, we design an SIS scheme with saliency detection to obtain meaningful shadows. Saliency detection methods such as the LC algorithm are used to determine the salient regions, which are sensitive to the human vision system. In this way, the shadows in our scheme have better visual quality than the relative method. The experimental results indicate the effectiveness of our scheme. In addition, our future work will focus on meaningful SIS for color images with other saliency detection methods.

Author Contributions: Conceptualization, J.C. and X.Y.; methodology, J.C. and X.Y.; software, J.C. and L.L.; validation, J.C.; formal analysis, J.C.; investigation, J.C. and L.L; writing—original draft preparation, J.C.; writing—review and editing, J.C., Y.J. and X.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by the National Natural Science Foundation of China (Grant Number: 61602491).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the editor and the anonymous reviewers for their valuable comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Muhammad, K.; Hamza, R.; Ahmad, J.; Lloret, J.; Wang, H.; Baik, S.W. Secure surveillance framework for IoT systems using probabilistic image encryption. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3679–3689. [CrossRef]
2. Zhou, H.; Chen, K.; Zhang, W.; Yao, Y.; Yu, N. Distortion design for secure adaptive 3-d mesh steganography. *IEEE Trans. Multimed.* **2018**, *21*, 1384–1398. [CrossRef]
3. Wang, J.; Zhang, L.Y.; Chen, J.; Hua, G.; Zhang, Y.; Xiang, Y. Compressed sensing based selective encryption with data hiding capability. *IEEE Trans. Ind. Inform.* **2019**, *15*, 6560–6571. [CrossRef]
4. Fukumitsu, M.; Hasegawa, S.; Iwazaki, J.Y.; Sakai, M.; Takahashi, D. A proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain. In Proceedings of the 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), Taipei, Taiwan, 27–29 March 2017; pp. 803–810.
5. Li, Y.; Guo, L. Robust image fingerprinting via distortion-resistant sparse coding. *IEEE Signal Process. Lett.* **2017**, *25*, 140–144. [CrossRef]
6. Chavan, P.V.; Atique, M.; Malik, L. Signature based authentication using contrast enhanced hierarchical visual cryptography. In Proceedings of the 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India, 1–2 March 2014; pp. 1–5.
7. Attasena, V.; Darmont, J.; Harbi, N. Secret sharing for cloud data security: A survey. *VLDB J.* **2017**, *26*, 657–681. [CrossRef]
8. Komargodski, I.; Naor, M.; Yogev, E. Secret-sharing for NP. *J. Cryptol.* **2017**, *30*, 444–469. [CrossRef]
9. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
10. Naor, M.; Shamir, A. Visual cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1994; pp. 1–12.
11. Wang, G.; Liu, F.; Yan, W.Q. Basic visual cryptography using braille. *Int. J. Digit. Crime Forensics (IJDCF)* **2016**, *8*, 85–93. [CrossRef]
12. Yan, W.; Ding, W.; Dongxu, Q. Image sharing based on chinese remainder theorem. *J. North China Univ. Tech* **2000**, *12*, 6–9.
13. Chuang, T.W.; Chen, C.C.; Chien, B. Image sharing and recovering based on Chinese remainder theorem. In Proceedings of the 2016 International Symposium on Computer, Consumer and Control (IS3C), Xi'an, China, 4–6 July 2016; pp. 817–820.
14. Yan, X.; Lu, Y.; Liu, L.; Wan, S.; Ding, W.; Liu, H. Chinese remainder theorem-based secret image sharing for (k, n) threshold. In Proceedings of the International Conference on Cloud Computing and Security, Nanjing, China, 16–18 June 2017; Springer: Cham, Switzerland, 2017; pp. 433–440.
15. 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.* **2012**, *23*, 441–453. [CrossRef]
16. He, J.; Lan, W.; Tang, S. A secure image sharing scheme with high quality stego-images based on steganography. *Multimed. Tools Appl.* **2017**, *76*, 7677–7698. [CrossRef]
17. Yang, C.N.; Ciou, C.B. Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. *Image Vis. Comput.* **2010**, *28*, 1600–1610. [CrossRef]
18. Li, P.; Yang, C.N.; Kong, Q.; Ma, Y.; Liu, Z. Sharing more information in gray visual cryptography scheme. *J. Vis. Commun. Image Represent.* **2013**, *24*, 1380–1393. [CrossRef]
19. Mert, A.C.; Öztürk, E.; Savaş, E. Design and implementation of a fast and scalable NTT-based polynomial multiplier architecture. In Proceedings of the 2019 22nd Euromicro Conference on Digital System Design (DSD), Kallithea, Greece, 28–30 August 2019; pp. 253–260.
20. Feng, X.; Li, S.; Xu, S. RLWE-oriented high-speed polynomial multiplier utilizing multi-lane stockham NTT algorithm. *IEEE Trans. Circuits Syst. II Express Briefs* **2019**, *67*, 556–559. [CrossRef]
21. Bisheh-Niasar, M.; Azarderakhsh, R.; Mozaffari-Kermani, M. High-speed NTT-based polynomial multiplication accelerator for CRYSTALS-Kyber post-quantum cryptography. In Proceedings of the 2021 IEEE 28th Symposium on Computer Arithmetic (ARITH), Lyngby, Denmark, 14–16 June 2021; pp. 94–101.
22. Ateniese, G.; Blundo, C.; De Santis, A.; Stinson, D.R. Extended capabilities for visual cryptography. *Theor. Comput. Sci.* **2001**, *250*, 143–161. [CrossRef]
23. Yuan, H.D. Secret sharing with multi-cover adaptive steganography. *Inf. Sci.* **2014**, *254*, 197–212. [CrossRef]
24. Cheng, T.F.; Chang, C.C.; Liu, L. Secret sharing: Using meaningful image shadows based on gray code. *Multimed. Tools Appl.* **2017**, *76*, 9337–9362. [CrossRef]
25. Chiu, P.L.; Lee, K.H. Efficient constructions for progressive visual cryptography with meaningful shares. *Signal Process.* **2019**, *165*, 233–249. [CrossRef]

26. Avci, D. A novel meaningful secret image sharing method based on Arabic letters. *Kuwait J. Sci.* **2016**, *43* , 114–124.
27. Wu, X.; Sun, W. Generalized random grid and its applications in visual cryptography. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1541–1553. [CrossRef]
28. Yang, C.N.; Yang, Y.Y. New extended visual cryptography schemes with clearer shadow images. *Inf. Sci.* **2014**, *271*, 246–263. [CrossRef]
29. Liu, L.; Lu, Y.; Yan, X. Polynomial-based extended secret image sharing scheme with reversible and unexpanded covers. *Multimed. Tools Appl.* **2019**, *78*, 1265–1287. [CrossRef]
30. Yan, X.; Lu, Y.; Liu, L.; Song, X. Reversible image secret sharing. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3848–3858. [CrossRef]
31. Duncan, J.; Humphreys, G.W. Visual search and stimulus similarity. *Psychol. Rev.* **1989**, *96*, 433. [CrossRef] [PubMed]
32. Zhai, Y.; Shah, M. Visual attention detection in video sequences using spatiotemporal cues. In Proceedings of the 14th ACM International Conference on Multimedia, Santa Barbara, CA, USA, 23–27 October 2006; pp. 815–824.
33. Cheng, M.M.; Mitra, N.J.; Huang, X.; Torr, P.H.; Hu, S.M. Salient object detection and segmentation. *IEEE Trans. Pattern Anal. Mach. Intell.* **2013**, *37*, 1.
34. Huang, Y.; Qiu, C.; Yuan, K. Surface defect saliency of magnetic tile. *Vis. Comput.* **2020**, *36*, 85–96. [CrossRef]
35. Wang, X.; Ma, H.; Chen, X.; You, S. Edge preserving and multi-scale contextual neural network for salient object detection. *IEEE Trans. Image Process.* **2017**, *27*, 121–134. [CrossRef]
36. Achanta, R.; Estrada, F.; Wils, P.; Süsstrunk, S. Salient region detection and segmentation. In Proceedings of the International Conference on Computer Vision Systems, Santorini, Greece, 12–15 May 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 66–75.
37. Achanta, R.; Hemami, S.; Estrada, F.; Susstrunk, S. Frequency-tuned salient region detection. In Proceedings of the 2009 IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA, 20–25 June 2009; pp. 1597–1604.
38. Goferman, S.; Zelnik-Manor, L.; Tal, A. Context-aware saliency detection. *IEEE Trans. Pattern Anal. Mach. Intell.* **2011**, *34*, 1915–1926. [CrossRef]
39. Asmuth, C.; Bloom, J. A modular approach to key safeguarding. *IEEE Trans. Inf. Theory* **1983**, *29*, 208–210. [CrossRef]
40. Wang, Z.; Bovik, A.C.; Sheikh, H.R.; Simoncelli, E.P. Image quality assessment: From error visibility to structural similarity. *IEEE Trans. Image Process.* **2004**, *13*, 600–612. [CrossRef]
41. Wang, Z.; Bovik, A.C. A universal image quality index. *IEEE Signal Process. Lett.* **2002**, *9*, 81–84. [CrossRef]