electronics

MDPI

Article

Progressive Reconstruction on Region-Based Secret Image Sharing

Yanxiao Liu [1,2,3,*], Qindong Sun [2,4], Zhihai Yang [2,5], Yongluan Zhou [6], Weihua Zhao [1] and Dantong Shi [1]

[1] School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China; 2211221077@stu.xaut.edu.cn (W.Z.); 2211221071@stu.xaut.edu.cn (D.S.)
[2] Sichuan Digital Economy Industry Development Research Institute, Chengdu 610036, China; qdongsun@xjtu.edu.cn (Q.S.); zhihaiyang@chd.edu.cn (Z.Y.)
[3] Guangxi Key Laboratory of Trusted Software, Guilin 541004, China
[4] School of Cyber Science and Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[5] School of Data Science and Artificial Intelligence, Chang'an University, Xi'an 710061, China
[6] Department of Computer Science, University of Copenhagen, 2100 Copenhagen, Denmark; zhou@di.ku.dk
* Correspondence: liuyanxiao@xaut.edu.cn

Abstract: (k, n) threshold progressive secret image sharing (PSIS) has become an important issue in recent years. In (k, n) PSIS, a secret image is encrypted into n shadows such that k to n shadows can gradually reconstruct the secret image. Since an image can usually be divided into different regions in such a way that each region includes information with different importance levels, region-based PSIS has also been proposed where the reconstruction of different regions requires different thresholds on the shadow numbers. In this work, we propose new region-based (k, n) PSIS that achieves a novel reconstruction model, where all regions possess the property of (k, n) threshold progressive reconstruction, but the same number of shadows recovers a lower proportion of information in regions with a higher importance level. This new reconstruction model can further complete the application of region-based PSIS, where each region has an equal minimum threshold for reconstruction, and the difference in importance levels between regions can be reflected in the proportion of the recovered image using the same number of shadows. A theoretical analysis proves the correctness of the proposed scheme, and the experimental results from four secret images also show the practicality and effectiveness of the proposed scheme.

Keywords: secret image sharing; progressive reconstruction; region; proportion

Citation: Liu, Y.; Sun, Q.; Yang, Z.; Zhou, Y.; Zhao, W.; Shi, D. Progressive Reconstruction on Region-Based Secret Image Sharing. *Electronics* **2024**, *13*, 1529. https://doi.org/10.3390/electronics13081529

Academic Editor: Myung-Sup Kim

Received: 15 March 2024
Revised: 10 April 2024
Accepted: 12 April 2024
Published: 17 April 2024

1. Introduction

The (k, n) secret image sharing (SIS) scheme has become a popular issue in the field of image security in recent years. It provides a way of protecting secret images among multiple participants. In a (k, n) SIS scheme, a secret image is encrypted into n shadows in such a way that it satisfies the following two rules: (1) no information is reconstructed at all when there are less than k shadows and (2) the image can be reconstructed with k or more shadows. Different from traditional image encryption and image-based information hiding, which are another two issues in the field of image security, SIS is an image protection solution that is established between multiple participants. It can solve security problems such as the tampering and leakage of secret images during transmission and storage, and it is fault-tolerant. In addition, there is no need to consider the key distribution and computational complexity of encryption and decryption in traditional image encryption. There are mainly two approaches to achieving (k, n) SIS schemes. For instance, the works in [1–5] were visual cryptography-based SIS schemes, and the SIS schemes in [6–9] were based on Lagrange interpolation polynomials.

Recently, a new decoding model in (k, n) SIS schemes, which is called progressive decoding, was proposed. This new decoding model satisfies the following rules: (1) no information of the secret image is reconstructed when there are less than k shadows and (2) k to n shadows can progressively reconstruct the image. Since the idea of progressive

decoding was introduced, many (k, n) SIS schemes that satisfy progressive decoding models have been proposed. Some of these can satisfy the general (k, n) threshold, some can satisfy the property of smooth progressive reconstruction, some of these focus on reducing shadow size, and some of these are based on visual cryptography and other approaches. This novel decoding model in PSIS can not only solve the problem of the single-image reconstruction mode in the previous solution but also further expand the application scenarios of SIS schemes. For instance, the authors of [10] provided a PSIS scheme for traffic surveillance image management, the authors of [11] combined the Internet of Things with PSIS and proposed a secret image sharing scheme with a key information hiding function, and the authors of [12] applied PSIS to the industrial Internet.

In most previous (k, n) PSIS schemes, the feature of image reconstruction is that the entire image can be progressively reconstructed from k to n shadows, and more information can be reconstructed from more participating shadows. Although this feature of progressive reconstruction is improved from the traditional (k, n) threshold reconstruction, the strategy of image reconstruction can still be further improved. In this work, we constructed a (k, n) PSIS scheme with a new image reconstruction strategy such that one secret image can be segmented into different regions with different importance levels, and different reconstruction strategies are applied for different regions. The theoretical analysis proves the correctness of the proposed scheme, and the experimental results also show the practicality and effectiveness of the proposed scheme. With the new image reconstruction strategy in our scheme, PSIS schemes can be further carried out in more complicated applications.

The rest of this paper is organized as follows. Section 2 provides some related works, which include the formal definition of (k, n) PSIS and some results of PSIS schemes. In Section 3, we describe the proposed (k, n) PSIS with the new progressive decoding model, and a theoretical analysis is used to show the correctness of our scheme. Section 4 presents the experimental results of the proposed scheme, and a comparison between the proposed scheme and other PSIS schemes is also shown in this section. Section 5 provides the conclusions of our work at the end.

2. Related Works

In this part, we provide the definition of a (k, n) PSIS scheme and list some related results on existing PSIS schemes.

2.1. Definition of PSIS

Traditional (k, n) SIS schemes encode a secret image into n shadows and satisfy the following two conditions: (1) k or more shadows can decode the entire image and (2) no information about the image at all is reconstructed when there is less than k shadows. (k, n) PSIS schemes can also encode secret images into n shadows but satisfy a different decoding model, called the progressive decoding model, which is as follows:

1. At less than k shadows, no information about the image is reconstructed.
2. k to n shadows can gradually decode the image. Let the symbol R_t be the proportion of recovered information to the entire image using t shadows; we then have $0 < R_k < R_{k+1} < ... < R_{n-1} < R_n = 1$.

In PSIS schemes, more participating shadows are able to recover more information about the secret image, which is reasonable in many conditions. Thus, PSIS can improve the application value of SIS.

2.2. Previous Results on PSIS

In the first polynomial-based PSIS scheme [13], 2 to n shadows can gradually decode a secret image. However, the scheme in [13] does not meet the general (k, n) threshold. Later, Yang et al. [14] proposed a polynomial-based generalized (k, n) PSIS, and the shadow size was reduced to $\frac{1}{n}$ of the image. Later, Yang et al. introduced another two (k, n) PSIS schemes [15,16], where the progressive decoding model satisfies a smooth decoding property. The difference between the schemes [15,16] is that an equal number of shadows

decode the same regions using the scheme in [15] but decode different regions using that in [16] when the shadows change. The scheme in [17] proposed a way to further reduce shadow size in previous PSIS schemes. The PSIS schemes in [13,18] are based on visual cryptography. Besides interpolation polynomial and visual cryptography, there are also other approaches for PSIS: the scheme in [19] is based on error correction codes, and the scheme in [20] is based on a GEMD data-hiding algorithm.

The main idea of previous PSIS schemes can be concluded as follows: a secret image is first segmented into multiple regions; each region is encoded into n sub-shadows using different (t, n) thresholds where t can be chosen from the set $\{k, k+1, k+2, ..., n\}$. The shadow for each participant is combined with a sub-shadow from each region; thus, the entire image can be progressively decoded from an increasing number of shadows. In fact, these PSIS schemes have been combined with multiple-threshold SIS schemes for each region, and the decoding model for each region uses the (t, n) threshold, where the parameter t is unchangeable. In this work, we constructed a (k, n) PSIS scheme with a different progressive decoding model, where each region of the secret image satisfies a (k, n) progressive decoding model, and when t shadows are involved in image decoding, the proportion of decoded information from each region is different according to the region's importance level. The same number of shadows can recover lower proportions of information in regions with higher importance levels. This new progressive decoding model could further the applications of PSIS, such as in important applications where all regions have an equal minimum requirement for starting reconstruction, and the difference in the importance level of a region can also be reflected in the different proportions of recovered information.

3. Proposed Scheme

In this part, we construct a new (k, n) PSIS scheme that satisfies the progressive reconstruction model, but it is different from previous PSIS schemes. The motivation of our work is described in Section 3.1, and the proposed scheme is then introduced in Section 3.2.

3.1. Motivation

All previous (k, n) PSIS schemes can gradually decode secret images from k to n shadows. The approaches of these schemes can be summarized as follows:

1. The secret image O is segmented into multiple regions $o_1, o_2, ..., o_l$.
2. Each region is encoded into n sub-shadows using (m, n) threshold approaches, where m is chosen from the set $\{k, k+1, ..., n\}$ according to the importance level of the corresponding region.
3. The shadow is a combination of all l sub-shadows that come from different l regions.

Basically, these PSIS schemes are a combination of multiple (m, n) threshold SIS schemes where $m \in \{k, k+1, ..., n\}$. One characteristic in these schemes is that a group of shadows can reconstruct some regions losslessly but cannot obtain any information about other regions at all. However, some applications segment one secret image into multiple regions, and the minimum reconstruction thresholds for all regions are equal. In other words, each of these regions satisfies a (k, n) progressive reconstruction model, which is different from previous PSIS schemes. The difference in importance level between different regions can be reflected by the proportion of reconstructed information using the same number of shadows in different regions. For example, if region o_1 is more important than o_2, both o_1 and o_2 can be gradually reconstructed from k to n shadows, but any m shadows, $k \leq m < n$, can recover a larger proportion of information in o_2 than in o_1. This new progressive reconstruction model is suitable in many situations. For instance, a traffic image O consists of three regions o_1, o_2, and o_3 that include information on the road, vehicle, and person. Any k to n authorized participants can gradually reconstruct the image, while k participants can reconstruct rough information about the type of road, the category of vehicle, and the number of persons; $k+1$ participants can reconstruct the road's width, the brand of vehicle, the sex of the persons, and so on. Since the importance

levels satisfy $L_{o_3} > L_{o_2} > L_{o_1}$, the proportion $Pro_{(m)}^{(o)}$ of recovered information on region o using m shadows satisfies $Pro_{(m)}^{(o_1)} > Pro_{(m)}^{(o_2)} > Pro_{(m)}^{(o_3)}$ for any $m \in \{k, k+1, ..., n-1\}$.

We can summarize the differences in reconstruction strategies between previous PSIS schemes and our proposed PSIS scheme as follows:

1. Previous PSIS schemes applied the same (k, n) progressive reconstruction strategy on the entire secret image.
2. Our PSIS scheme first segments a secret image into different regions, where each region contains information with different importance levels, and then different (k, n) progressive reconstruction strategies are applied to different regions.

3.2. Proposed (k, n) PSIS Scheme

In this part, we describe a new (k, n) PSIS scheme that is consistent with the motivation and then present a theoretical analysis. Before describing our scheme, we propose a new algorithm for generating n shadow pixels of one pixel. A definition of a k-group distribution vector is also proposed together with this algorithm below.

For example, let $(k, n) = (3, 5)$ and pixel $p = v_1 \oplus v_2 \oplus v_3$. Then, $(s_1, s_2, s_3, s_4, s_5) = (v_2, v_3, v_1, v_3, v_1)$ is a group of five shadow pixels of p, since $V = (V_1, V_2, V_3) = (2, 1, 2)$. Here, we define the concept of Difference on the set V, denoted as $Def_{(V)}$. $Def_{(V)}$ can be computed as $Def_{(V)} = Max(V_i - V_j)$. For example, if $V = (2, 1, 2)$, $Def_{(V)} = 1$; if $V = (3, 1, 1)$, $Def_{(V)} = 2$.

Based on Algorithm 1, the proposed scheme is introduced in Scheme 1.

Algorithm 1 n shadow pixels for one pixel

Input: one pixel p; output: n shadow-pixels $s_1, s_2, ..., s_n$.

1 Randomly generate k pixels $v_1, v_2, ..., v_k$ such that $p = v_1 \oplus v_2 \oplus ... \oplus v_k$, where $\oplus$ denotes the XOR operation.
2 Randomly select n pixels $s_1, s_2, ..., s_n$ from the set $\{v_1, v_2, ..., v_k\}$. Let the vector $V = (V_1, V_2, ..., V_k)$, where V_i is the number of shadow v_i in the set $\{s_1, s_2, ..., s_n\}$.
3 $s_1, s_2, ..., s_n$ is a group of n shadow-pixels of p, when $V_i \geq 1, i = 1, 2, ..., k$.

Scheme 1: *Proposed (k, n) PSIS scheme.*
Shadow Generation phase: Input: image O; Output n shadows $S_1, S_2, ..., S_n$.

1 The image O is segmented into multiple regions $o_1, o_2, ..., o_l$ with different importance levels. We use the symbol L_i to denote the importance level of o_i; without loss of generality, let $L_1 < L_2 < ... < L_l$.
2 Generate k-dimensional vectors $V^{(1)}, V^{(2)}, ..., V^{(l)}$ that satisfy $Def_{(V^{(1)})} < Def_{(V^{(2)})} < ... < Def_{(V^{(l)})}$.
3 For each region $o_i, i = 1, 2, ..., l$, which consists of w_i pixels $o_i = p_{i,1}||p_{i,2}||...||p_{i,w_i}$,
   (1) Generate a group of n shadow pixels $s_1^{i,j}, s_2^{i,j}, ..., s_n^{i,j}$ for each pixel $p_{i,j}, j = 1, 2, ..., w_i$ using Algorithm 1. All these w_i groups of n shadow pixels use the same k-dimensional vector V^i.
   (2) The n sub-shadows for region $o_i, i = 1, 2, ..., l$ are $s_{i,j} = s_j^{i,1}||s_j^{i,2}||...||s_j^{i,w_i}, j = 1, 2, ..., n$.
4 The n shadows for image O are $S_j = s_{1,j}||s_{2,j}||...||s_{l,j}, j = 1, 2, ..., n$.

Image Reconstruction phase: Input: m shadows $(k \leq m \leq n)$; output: partial image O^{Par}.

1 Suppose that the m shadows are $S_1, S_2, ..., S_m$. Each shadow S_j is a combination of l sub-shadows on all l regions, $S_j = s_{1,j}||s_{2,j}||...||s_{l,j}$. Reconstruct the partial image o_i^{Par} using the equation $o_i^{Par} = s_{i,1} \oplus s_{i,2} \oplus ... \oplus s_{i,m}$.
2 The reconstructed partial image O^{Par} is $O^{Par} = o_1^{Par}||o_2^{Par}||...||o_l^{Par}$.

Next, we use theoretical analysis to explain the properties of the progressive (k, n) reconstruction in the proposed scheme. The following Theorem 1 is the basis for Theorems 2 and 3. Theorem 2 shows that the entire secret image O can be gradually reconstructed from k to n shadows, and Theorem 3 proves that when the same number of shadows are involved in the image decoding, a larger proportion of information can be reconstructed in the region with a lower importance level.

Theorem 1. *Suppose a region o is encoded into n sub-shadows under the k-dimensional vector* $V = (v_1, v_2, ..., v_k)$*, then the proportion of reconstructed information on o using m sub-shadows* $(k \le m \le n)$ *is* $Pro_{(V)}^{(m)} = \frac{\sum_{v_i \ge n_i \ge 1, i=1,2,...,k}^{(n_1+n_2+,...,+n_k=m)} (C_{v_1}^{n_1} C_{v_2}^{n_2}, ..., C_{v_k}^{n_k})}{C_n^m}$.

Proof. According to Algorithm 1 and Scheme 1, a region o is encoded into n sub-shadows under the k-dimensional vector $V = (v_1, v_2, ..., v_k)$, which means that each pixel p included in o is encoded into n shadow pixels $s_1, s_2, ..., s_n$ from the set of k shadow pixels $\{q_1, q_2, ..., q_k\}$ under the same k-dimensional vector $V = (v_1, v_2, ..., v_k)$. When randomly choosing m shadow pixels, the pixel can be decoded correctly only when at least one shadow pixel on each $q_1, q_2, ..., q_k$ is included in these m selected shadow pixels. The total number for this situations is $\sum_{v_i \ge n_i \ge 1, i=1,2,...,k}^{(n_1+n_2+,...,+n_k=m)} (C_{v_1}^{n_1} C_{v_2}^{n_2}, ..., C_{v_k}^{n_k})$, and the number of selected shadow pixels m out of n is C_n^m; therefore, the probability of correctly decoding pixel p from random m shadow pixels is $\frac{\sum_{v_i \ge n_i \ge 1, i=1,2,...,k}^{(n_1+n_2+,...,+n_k=m)} (C_{v_1}^{n_1} C_{v_2}^{n_2}, ..., C_{v_k}^{n_k})}{C_n^m}$. Since the region o consists of multiple pixels, the proportion of reconstructed information of o equals the probability of correctly decoding each pixel. Thus, the proportion of reconstructed information of region o from random m sub-shadows under a k-dimensional vector $V = (v_1, v_2, ..., v_k)$ is $Pro_{(V)}^{(m)} = \frac{\sum_{v_i \ge n_i \ge 1, i=1,2,...,k}^{(n_1+n_2+,...,+n_k=m)} (C_{v_1}^{n_1} C_{v_2}^{n_2}, ..., C_{v_k}^{n_k})}{C_n^m}$. □

Using the conclusion in Theorem 1, we describe Theorem 2 to analyze the progressive reconstruction property of the proposed scheme.

Theorem 2. *Our scheme satisfies the* (k, n) *progressive reconstruction model, where k to n shadows can gradually reconstruct the secret image.*

Proof. In our scheme, the secret image O is first segmented into l regions $o_1, o_1, ..., o_l$; each region o_i generates n sub-shadows $s_{i,1}, s_{i,2}, ..., s_{i,n}$, and the shadow S_j is a combination of l sub-shadows that comes from each region, $S_j = s_{1,j}||s_{2,j}||...||s_{l,j}$. In order to prove the (k, n) progress reconstruction model on secret image O, we only need to prove that each region o_i satisfies the (k, n) progress reconstruction model on these n sub-shadows $s_{i,1}, s_{i,2}, ..., s_{i,n}$.

According to the conclusion of Theorem 1, any m sub-shadows can reconstruct a proportion of $Pro_{(V)}^{(m)}$ on the corresponding region o_i. In order to prove the (k, n) progressive reconstruction property on the region o_i, we only need to prove $Pro_{(V)}^{(m+1)} > Pro_{(V)}^{(m)}$. In fact, $\frac{Pro_{(V)}^{(m+1)}}{Pro_{(V)}^{(m)}} = \frac{[\sum_{1 \le n_i' \le v_i, i \in [1,k]}^{(n_1'+n_2'+,...,+n_k'=m+1)} (C_{v_1}^{n_1'} C_{v_2}^{n_2'} ... C_{v_k}^{n_k'})](m+1)}{[\sum_{1 \le n_i \le v_i, i \in [1,k]}^{(n_1+n_2+,...,+n_k=m)} (C_{v_1}^{n_1} C_{v_2}^{n_2} ... C_{v_k}^{n_k})](n-m)}$. For each combination of $n_i, i = 1, 2, ..., k$ satisfying $n_1 + n_2 +, ..., +n_k = m$, there exist up to k different combinations $n_i', i = 1, 2, ..., k$ satisfying $n_1' + n_2' +, ..., +n_k' = m + 1$ $(n_i' = n_i + 1, i \in [1, k], n_j' = n_j, j \ne i)$. Then, we can obtain that $\frac{[\sum_{1 \le n_i' \le v_i, i \in [1,k]}^{(n_1'+n_2'+,...,+n_k'=m+1)} (C_{v_1}^{n_1'} C_{v_2}^{n_2'} ... C_{v_k}^{n_k'})]}{[\sum_{1 \le n_i \le v_i, i \in [1,k]}^{(n_1+n_2+,...,+n_k=m)} (C_{v_1}^{n_1} C_{v_2}^{n_2} ... C_{v_k}^{n_k})]} \approx k$. Generally, $m \ge k > \frac{n}{2}$; then, we have $\frac{m+1}{n-m} \ge 1$. Thus, we have proven that $Pr_{(V)}^{m+1} \ge Pr_{(V)}^{m}$. In addition, it is easy to prove that $Pro_{(V)}^{(n)} = 1$ and $Pro_{(V)}^{(m)} = 0$ when $m < k$. Thus, each region o_i in O satisfies the (k, n)

progressive reconstruction property, and the entire image $O = o_1||o_2||...||o_l$ satisfies the (k, n) progressive reconstruction property as a result. □

Theorem 2 explain that our proposed scheme satisfies the (k, n) progressive reconstruction property, which is the same as other progressive (k, n) SIS schemes, and it also shows the difference from other schemes in that each region in the entire image also satisfies the (k, n) progressive reconstruction property. The regions have different importance levels, and previous PSIS schemes adopted different thresholds for different regions. In contrast, in our scheme, for all regions subject to (k, n) progressive reconstruction, the different important levels of regions can be reflected from the proportions of reconstructed information using the same number of shadows on different regions. In the following, Theorem 3 provides the proof accordingly.

Theorem 3. *In our scheme, m shadows* $(k \leq m < n)$ *can reconstruct a larger proportion of information about a region with a lower importance level.*

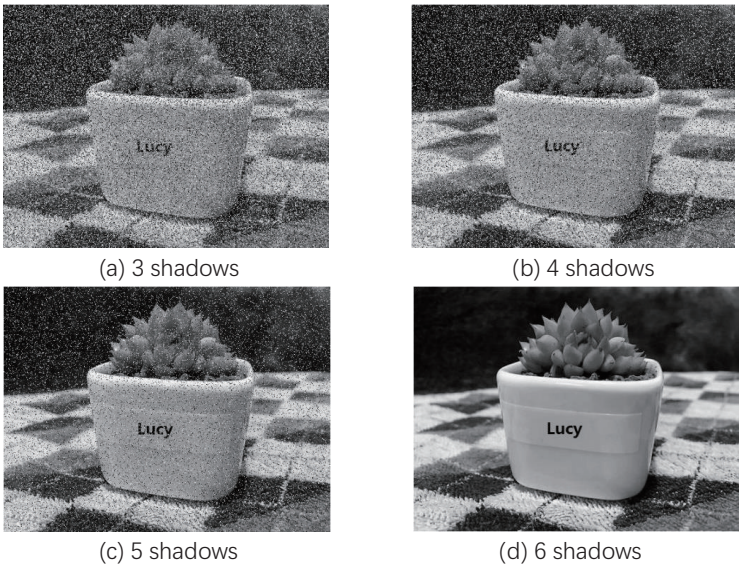
Proof. In our scheme, suppose two regions o_1 and o_2 are segmented from secret image O, where the importance levels satisfy $L_1 < L_2$. According to Scheme 1, sub-shadows on o_1 and o_2 are generated using two k-dimensional vectors $V^{(1)}$ and $V^{(2)}$ with $Def_{(V^{(1)})} < Def_{(V^{(2)})}$. The proportions of the reconstructed information on o_1 and o_2 using any m shadows are $Pro^{(m)}_{V^{(1)}}$ and $Pro^{(m)}_{V^{(2)}}$, respectively. Here, we are going to prove $Pro^{(m)}_{V^{(1)}} > Pro^{(m)}_{V^{(2)}}$.

According to Theorem 1, these two proportions are $Pro^{(m)}_{(V^e)} = \frac{\sum^{(n_1+n_2+,...,+n_k=m)}_{v^e_i \geq n_i \geq 1, i=1,2,...,k} (C^{n_1}_{v^e_1} C^{n_2}_{v^e_2}, ..., C^{n_k}_{v^e_k})}{C^m_n}$, $e = 1, 2$. Thus, we only need to compare the two numerators $H^e = \sum^{(n_1+n_2+,...,+n_k=m)}_{v^e_i \geq n_i \geq 1, i=1,2,...,k} (C^{n_1}_{v^e_1} C^{n_2}_{v^e_2}, ..., C^{n_k}_{v^e_k}), e = 1, 2$. Without loss of generality, we consider the case where $k = 2$ and $v^e_1 \geq v^e_2$; then, $H^e = \sum^{(n_1+n_2=m)}_{v^e_i \geq n_i \geq 1, i=1,2} (C^{n_1}_{v^e_1} C^{n_2}_{v^e_2}), e = 1, 2$. The following three situations are considered separately: (1) $m < v^e_2$, (2) $v^e_2 \leq m < v^e_1$, and (3) $m \geq v^e_1$. For case (1), $H^e = C^m_n - (C^m_{v^e_1} + C^m_{v^e_2})$. If we regard v^e_1 as a variable x, then H^e is the function $f(x) = C^m_n - (C^m_x + C^m_{n-x})$. In order to prove $H^1 > H^2$, we only need to explain that $f(x)$ is a decreasing function, since $Def_{(V^{(1)})} < Def_{(V^{(2)})}$, which means that the variable x is larger in H^2 than in H^1. For simplicity, we use the special case that $m = 2$, and thus, $f(x) = C^2_n - (x(x-1) + (n-x)(n-x-1))$. The first derivative of $f(x)$ is $f'(x) = 2(n-2x)$. Because $x = v^e_1, n - x = v^e_2$, $n - 2x < 0$ can be deduced from $v^e_1 > v^e_2$. Therefore, as $f'(x) < 0$, $f(x)$ is a decreasing function, and thus, $H^1 > H^2$. For case (2), $H^e = C^m_n - C^m_{v^e_1}$. Since $C^m_{v^1_1} < C^m_{v^2_1}$, we can obtain that $H^1 > H^2$. For case (3), $H^1 = H^2 = C^m_n$. From the analysis of the three cases, we can obtain the conclusion that in our proposed scheme, m shadows $(k \leq m < n)$ can reconstruct a larger proportion of information about a region with a lower importance level. □

4. Experimental Results and Comparisons

In this part, we present two experiments to show the performance of the proposed scheme. In experiment 1, two $(k, n) = (3, 6)$ PSIS schemes are used on an original image. One of them is a previous PSIS scheme, where the whole image is encrypted into $n = 6$ shadows; 3 to 6 shadows can gradually reconstruct the image. The other is our proposed PSIS scheme, where the original image is first segmented into three regions with different importance levels, and then $n = 6$ shadows are generated using our approach. During image reconstruction, each region can be gradually reconstructed from 3 to 6 shadows, but the same number of shadows can recover less information about a region with a higher importance level. Figures 1 and 2 show the results of the image reconstruction using the previous PSIS and proposed PSIS schemes, respectively, and the percentages of the recovered image and each recovered region are listed in Table 1. From this experiment, we could see that, compared to the previous PSIS scheme, our proposed scheme can employ

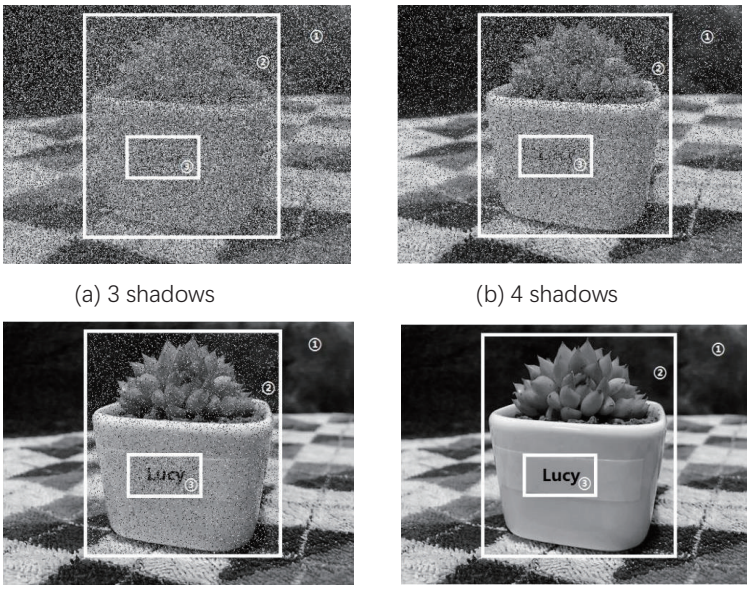
different (k, n) progressive reconstruction models on different regions from one secret image, where each region contains information with different important levels. Therefore, our scheme can provide a more complicated (k, n) progressive reconstruction model than previous PSIS schemes. This feature allows our solution to be applied to more scenarios.



(a) 3 shadows (b) 4 shadows

(c) 5 shadows (d) 6 shadows

Figure 1. Image reconstruction using previous $(3, 6)$ PSIS scheme.



(a) 3 shadows (b) 4 shadows

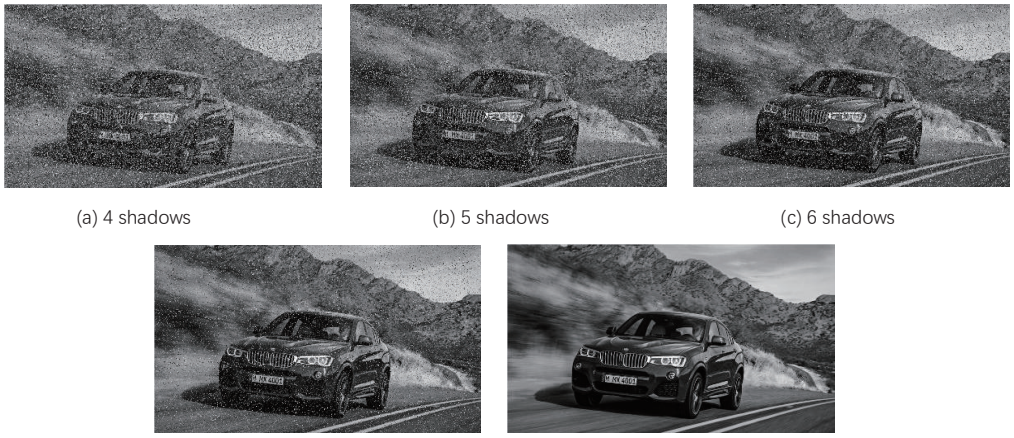
(c) 5 shadows (d) 6 shadows

Figure 2. Image reconstruction using proposed $(3, 6)$ PSIS scheme.

Table 1. Percentages of recovered image from two $(3, 6)$ PSIS schemes.

Number of Shadows	Previous PSIS	Proposed PSIS		
		Region 1	Region 2	Region 3
3	50%	41%	27%	21%
4	67%	78%	62%	39%
5	83%	100%	83%	66%
6	100%	100%	100%	100%

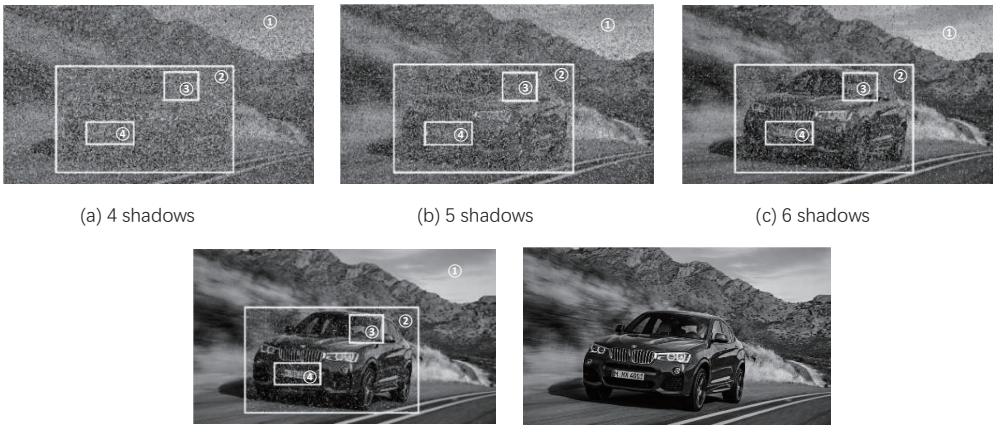
In experiment 2, two $(k, n) = (4, 8)$ PSIS schemes were used, a previous PSIS scheme and our proposed PSIS scheme. In both schemes, the original image was encrypted into $n = 6$ shadows; 3 to 6 shadows can gradually reconstruct the image using the previous PSIS scheme. In our proposed PSIS scheme, the original image is first segmented into four regions with different importance levels, and then $n = 8$ shadows are generated using our approach. During image reconstruction, each region can be gradually reconstructed from 4 to 8 shadows, but the same number of shadows can recover less information about a region with a higher importance level. Figures 3 and 4 show the results of the image reconstruction using the previous PSIS and proposed PSIS schemes, respectively, and the percentages of the recovered image and each recovered region are listed in Table 2. Normally, the selection of parameters k and n depends on the specific application scenarios of secret image sharing. The parameter n is determined based on the number of users, and the parameter k is half or a little more than half of n, which matches the majority principle. In the experiments of this work, the images are simple, and we assume that there are few participants. However, in some large-scale application scenarios, the parameters of k and n can be in the hundreds or even larger than that.



(a) 4 shadows (b) 5 shadows (c) 6 shadows

(d) 7 shadows (e) 8 shadows

Figure 3. Image reconstruction using previous $(4, 8)$ PSIS scheme.



(a) 4 shadows (b) 5 shadows (c) 6 shadows

(d) 7 shadows (e) 8 shadows

Figure 4. Image reconstruction using proposed $(4, 8)$ PSIS scheme.

Table 2. Percentages of recovered image using two $(4, 8)$ PSIS schemes.

Number of Shadows	Previous PSIS	Proposed PSIS			
		Region 1	Region 2	Region 3	Region 4
4	50%	23%	17%	13%	11%
5	63%	57%	43%	32%	28%
6	75%	86%	68%	53%	48%
7	88%	100%	88%	75%	72%
8	100%	100%	100%	100%	100%

5. Conclusions

In (k, n) PSIS schemes, an image can be gradually reconstructed from k to n shadows. Some PSIS schemes segment secret images into multiple regions with different importance levels, where more shadows can recover regions with higher importance levels. Such reconstruction models have a property ensuring that the regions can be either fully recovered or not recovered at all. In this work, we introduced a new reconstruction model for region-based (k, n) PSIS, where each region can be gradually reconstructed from k to n shadows, and the same number of shadows can reconstruct a lower proportion of information about a region with a higher importance level. The theoretical analysis and experimental results prove the effectiveness of the proposed scheme. This novel reconstruction model can expand the utilization of PSIS to more applications.

Author Contributions: Conceptualization, Q.S. and Y.L.; formal analysis, Z.Y.; methodology, Y.Z.; writing—original draft, W.Z. and D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by the Natural Science Foundation of China under Grant 62172331; the Youth Innovation Team of Shaanxi Universities (No.: 2019-38); the Natural Science Foundation of Sichuan Province (Nos.: 2022NSFSC0554, 2022NSFSC0549, and 2023NSFSC0502); the Youth Innovation Team Construction of the Shaanxi Provincial Department of Education under Grants 21JP081 and 22JP059; the Natural Science Foundation of Shaanxi under Grant 2023-YBGY-271; the Guangxi Key Laboratory of Trusted Software (No.: KX202036); and the Xi'an Science and Technology Plan under Grant 22GXFW0083, 22GXFW0079.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

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

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

Abbreviations

The following abbreviations are used in this manuscript:

PSIS	Progressive secret image sharing;
SIS	Secret image sharing;
GEMD	Generalized exploiting modification directions.

References

1. Yang, C.N.; Chung, T.H. A general multi-secret visual cryptography schemes. *Opt. Commun.* **2010**, *283*, 4949–4962. [CrossRef]
2. Shyu, S.J.; Jiang, H.W. General constructions for threshold multiple-secret visual cryptography schemes. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 733–743. [CrossRef]
3. Hou, Y.C.; Quan, Z.Y.; Tsai, C.F.; Tseng, A.Y. Block-based progressive visual secret sharing. *Inf. Sci.* **2013**, *233*, 290–304. [CrossRef]

4. Jia, X.X.; Wang, D.S.; Nie, D.X.; Zhang, C.Y. Collaborative visual cryptography schemes. *IEEE Trans. Circuits Syst. Video* **2018**, *28*, 1056–1070. [CrossRef]
5. Wu, X.T.; Feng, X.J. Size invariant visual cryptography schemes with evolving threshold access structures. *IEEE Trans. Multimed.* **2024**, *26*, 1488–1503. [CrossRef]
6. Thien, C.C.; Lin, J.C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [CrossRef]
7. Lin, C.C.; Tsai, W.H. Secret image sharing with steganography and authentication. *J. Syst. Softw.* **2004**, *73*, 405–414. [CrossRef]
8. Yang, C.N.; Ouyang, J.F.; Harn, L. Steganography and authentication in image sharing without party bits. *Opt. Commun.* **2012**, *285*, 1725–1735. [CrossRef]
9. Wang, R.Z.; Su, C.H. Secret image sharing with smaller shadow images. *Pattern Recognit. Lett.* **2006**, *27*, 551–555. [CrossRef]
10. Liu, Y.X.; Yang, C.N.; Sun, Q.D. Thresholds based image extraction schemes in big data environment in intelligent traffic management. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3952–3960. [CrossRef]
11. Wu, W.; Peng, H.P.; Tong, F.H.; Li, L.X. A chaotic compressed sensing-based multigroup secret image sharing method for IoT with critical information concealment function. *IEEE Internet Things J.* **2023**, *10*, 1192–1270. [CrossRef]
12. Xiong, L.Z.; Han, X.; Zhong, X.W.; Yang, C.N.; Xiong, N. RSIS: A secure and reliable secret image sharing system based on extended hamming codes in industrial internet of things. *IEEE Internet Things J.* **2023**, *10*, 1933–1945. [CrossRef]
13. Wang, R.Z. Region incrementing visual cryptography. *IEEE Signal Process. Lett.* **2009**, *16*, 659–662. [CrossRef]
14. Yang, C.N.; Shih, H.W.; Harn, L. k out of n region incrementing scheme in visual cryptography. *IEEE Trans. Circuits Syst. Video Technol.* **2012**, *22*, 799–810. [CrossRef]
15. Yang, C.N.; Huang, S.M. Constructions and properties of k out of n scalable secret image sharing. *Opt. Commun.* **2010**, *283*, 1750–1762. [CrossRef]
16. Yang, C.N.; Chu, Y.Y. A general (k, n) scalable secret image sharing scheme with the smooth scalability. *J. Syst. Softw.* **2011**, *84*, 1726–1733. [CrossRef]
17. Liu, Y.X.; Yang, C.N. Reducing shadow size in smooth scalable secret image sharing. *Secur. Commun. Netw.* **2014**, *7*, 2237–2244. [CrossRef]
18. Hou, Y.C.; Quan, Z.Y. Progressive visual cryptography with unexpanded shares. *IEEE Trans. Circuits Syst. Video Technol.* **2011**, *21*, 1760–1764. [CrossRef]
19. Liu, Y.X.; Yang, C.N.; Wu, S.Y.; Chou, Y.S. Progressive (k, n) secret image sharing schemes based on Boolean operations and covering codes. *Signal Process. Image Commun.* **2018**, *66*, 77–86. [CrossRef]
20. Liu, Y.X.; Yang, C.N.; Wu, S.Y.; Chou, Y.S.; Sun, Q.D. Progressive (k, n) secret image sharing scheme with meaningful shadow images by GEMD and RGEMD. *J. Vis. Commun. Image Represent.* **2018**, *55*, 766–777. [CrossRef]