mathematics

Article

Thumbnail Secret Image Sharing in Cloud Storage

Yongqiang Yu [1,2], Xuehu Yan [1,2,*], Shudong Wang [1,2], Xianhui Wang [1,2] and Huan Lu [1,2]

[1] College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China
[2] Anhui Key Laboratory of Cyberspace Security Situation Awareness and Evaluation, Hefei 230037, China
[*] Correspondence: publictiger@126.com

Abstract: In recent years, the amount of data has increased explosively, which has spawned the large-scale development of cloud storage. Increasingly, individuals and enterprises store images in cloud space. The storage security of the cloud is generally guaranteed by encryption, but this can no longer meet the needs of image management and protection. In order to realize the management and loss tolerance of images, this paper proposes a thumbnail secret image sharing method. The proposed scheme combines the advantages of thumbnail-preserving encryption (TPE) and secret image sharing (SIS) with different meaningful shadows. Thumbnails can realize the visual management of stored images, and secret image sharing can realize the perfect security of stored images. The proposed scheme realizes the confidentiality, integrity, and availability of images, which are three elements of information security. Compared with TPE, our scheme not only realizes the visual management of images but also achieves loss tolerance and perfect security. Compared with SIS with different meaningful shadows, our scheme will greatly improve the sharing efficiency and reduce the consumption of computing resources. In this paper, the theoretical analysis and security proof of the proposed scheme are presented. In addition, we also conduct sufficient experiments and comparative explanations.

Keywords: cloud storage; extended secret image sharing; thumbnails; loss tolerance; shadow management

MSC: 94A62

check for updates

Citation: Yu, Y.; Yan, X.; Wang, S.; Wang, X.; Lu, H. Thumbnail Secret Image Sharing in Cloud Storage. *Mathematics* **2022**, *10*, 3076. https://doi.org/10.3390/math10173076

Academic Editors: Ximeng Liu and Antanas Cenys

Received: 19 July 2022
Accepted: 23 August 2022
Published: 26 August 2022

1. Introduction

Currently, with the rapid development of the internet and the wide application of intelligent devices, people are increasingly fond of sharing their lives on social media and networks [1]. There is no doubt that images are the main way to show the state of a person's life and their understanding of the real world [2]. According to statistics, 136,000 photos are uploaded to Facebook every minute, which is equivalent to 195 million images per day, while this number was only 2.7 million in 2010 [3,4]. Photos uploaded to social platforms are only part of the volume of images taken. In June 2021, Rise Above Research, a consulting firm that provides market research for the digital imaging industry, estimated the number of global images was 1.12 trillion in 2020 and predicts that the number of global images will grow to 1.4 trillion images in 2021 [5]. Faced with such a large and growing amount of images, local storage in the traditional sense will become difficult to deal with. If these images are all stored in a local storage device, it will take up a great deal of resources and space from the user and cause inconvenience in management.

Uploading images to the cloud space for storage and management has overturned the traditional image storage and management methods and has become the current development trend [6,7]. Many internet companies and major mobile phone manufacturers now provide general cloud storage services, such as Dropbox, OneDrive, Google Drive, and iCloud. The development and popularity of cloud storage services make cloud storage space larger and cheaper. Therefore, more users will be attracted to use cloud storage services, and increasing numbers of images will be uploaded to the cloud space. Among the massive images, there are some high-value images containing personal privacy and trade secret information that need to be protected, which are called secret images. The large increase of secret images has forced them to be uploaded to the cloud space to alleviate the lack of local resources [8,9]. However, in the 2020 Cloud Security Report from Check Point [10], nine main cloud security issues and threats were listed in 2021: misconfiguration, unauthorized access, insecure interfaces/APIs, hijacking of accounts, lack of visibility, external sharing of data, malicious insiders, cyberattacks, and denial of service attacks. Although many users have no choice but to decide to upload sensitive data and secret images to the cloud space, these threats have caused great concerns among users [11,12]. These concerns mainly include data loss/leakage and data privacy/confidentiality. The status of cloud storage is shown in Figure 1.

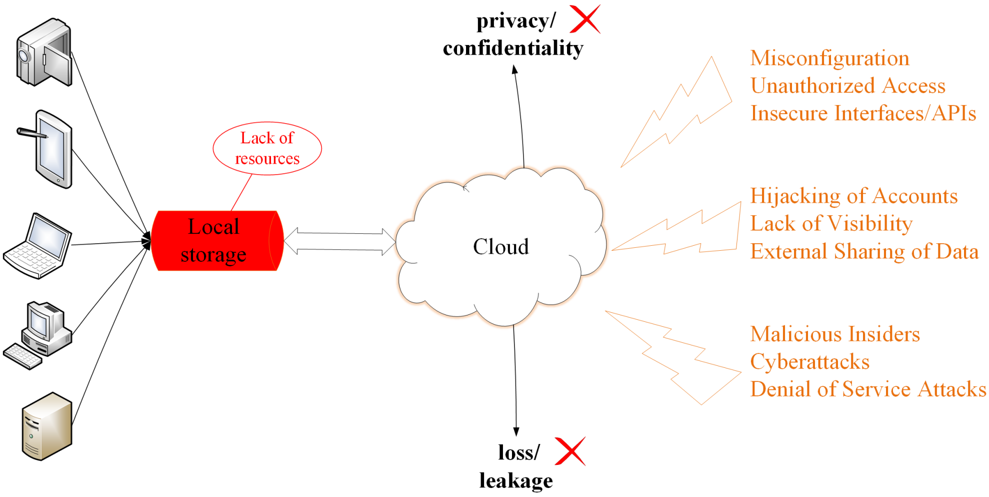


Figure 1. Cloud storage status.

1.1. Related Work

To protect secret images stored in cloud space, a series of works have been proposed. Information security is often assessed by CIA (confidentiality, integrity, availability) [13,14], which are three elements of information security. For the security of secret images, secret images cannot be uploaded directly to the cloud space but must be processed. Currently, the most common way is to encrypt [15–17] the secret image and upload cipher images to the cloud space. Traditional image encryption algorithms with a confusion and diffusion structure are commonly used to encrypt secret images. Although these schemes can protect the confidentiality of secret images, there are still many problems after uploading encrypted images to the cloud. For example, users cannot directly browse cipher images through the cloud, so they are prohibited from organizing and managing images through visual content [18–20]. Users can only understand the content of the image after downloading and decrypting the cipher image, which violates the principle of availability in cloud space. Regarding the problem of cipher images management, some scholars have combined the research results of visual memory in visual psychology to propose a concept of image encryption based on prior knowledge, that is, thumbnail-preserving encryption (TPE) [21–23]. The basic idea of TPE is that the cipher image retains the thumbnail of the original image. Legal users with prior knowledge can combine the visual information of the cipher image with prior knowledge to infer the specific content of the image, while illegal users without prior knowledge cannot infer from the rough visual information of the cipher image, as shown in Figure 2.

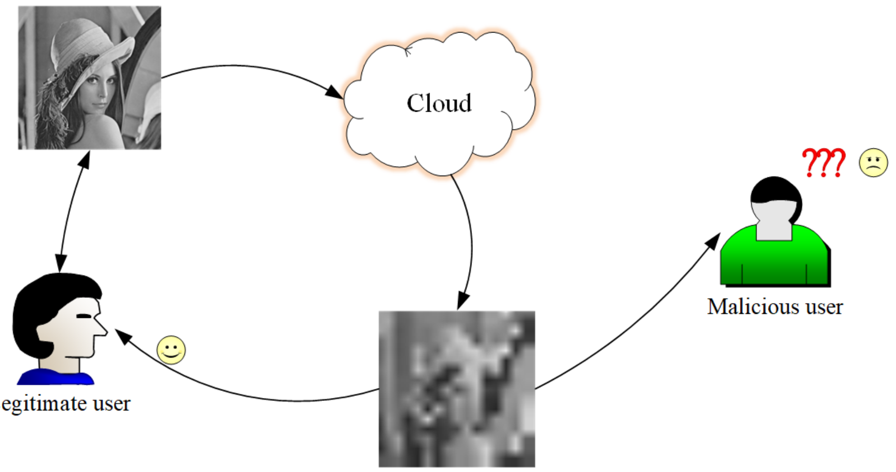


Figure 2. Thumbnail-preserving encryption.

The first TPE scheme was designed by Wright et al. [21], and then many scholars made improvements to further the recognition and organization of cipher images [24–26]. Zhao et al. [27] improved the original scheme [25,26] and further optimized the practicability and efficiency of TPE, but their scheme still did not solve the problem of image integrity. Therefore, we carried out further design and optimization.

1.2. Discussion

Organizations and individuals use the cloud to store their data and applications and trust it to be safe and reliable. However, the cloud is not perfect, and even the most reliable cloud provider will suffer data loss, which is inevitable. Cyberattacks or equipment failures are important reasons for data loss. Similarly, human error, such as simply an incorrect instruction, may lead to data loss. However, none of the above schemes can deal with data loss well, which is the main concern of users.

The traditional encryption scheme protects the privacy of secret images, but it brings about the problems of the difficult management of cipher images and data loss, leading to data unavailability. Although TPE solves the management problem of cipher images, it cannot prevent data loss and data damage, which seriously affects the integrity of data. In order to further improve the security of cloud storage and increase users' trust in cloud storage, we adopt the idea of SS to perform encryption. The image is encrypted into multiple cipher images by secret image sharing (SIS) [28–30] and then stored in different cloud spaces by distributed storage. SIS has the property of loss tolerance, so it can prevent data loss and data damage [29,31]. The traditional SIS cipher image and encrypted image are noise images [32].

The current work cannot meet the security and management needs of images in the cloud, so we use the knowledge of secret sharing (SS) [33,34] and thumbnails to realize the perfect protection and convenient management of images. Proposed scheme mainly uses approximate thumbnails and control sharing models. Approximate thumbnails are mainly used to solve the usability problem of encrypted images. Controlling secret sharing is performed to ensure the integrity of the secret and change the situation that the original shared cipher image is noise, which is based on approximate thumbnail sharing. We specifically describe the contributions of the proposed scheme in the CIA of information security below.

1. Confidentiality: This paper uses the method of SS to encrypt the secret image to realize the protection of image privacy.
2. Integrity: Compared with previous schemes, our scheme has the characteristics of loss tolerance, which is critical for the complete recovery and utilization of secrets, greatly improving the security of cloud storage.

3. Availability: The cipher image generated by the proposed scheme is visually identifiable and achieves the management of the cipher image. Compared with meaningful SIS, our scheme greatly improves the efficiency of sharing.

The rest of the paper is organized as follows. Section 2 introduces the basic concepts and related knowledge needed in this paper. The proposed scheme is introduced in Section 3, including the general overview of the scheme, the design of the scheme and algorithm, and the security analysis. Section 4 gives the experimental result and data. Finally, Section 5 concludes this paper.

2. Preliminary

In this section, we introduced the basic definitions and preliminaries used in this paper, including secret sharing, polynomial-based SIS, and thumbnail-preserving.

2.1. Secret Sharing

SS [33,34] encrypts the secret information into several shares and secretly distributes them to a number of participants. At the same time, it requires that the authorized subset of participants can be combined to recover the secret information by using the shares held. Other unauthorized subsets cannot recover secret information by shares.

An SS scheme can be described as a six-tuple $\{\mathcal{P}, \Gamma_Q, \mathcal{K}, \mathcal{S}, \mathcal{E}, \mathcal{D}\}$, where

1. $\mathcal{P}$ is the finite set of secret sharing participants, and $\mathcal{P} = \{P_1, \ldots, P_n\}$, where n is the number of participants, namely $n = |\mathcal{P}|$;
2. Γ_Q is an access structure, which is composed of participant authorization subsets;
3. $\mathcal{K}$ is a finite set of possible secret values, and the number of elements in the secret value space is defined as $\eta = |\mathcal{K}|$;
4. $\mathcal{S}$ is a finite set of possible shared values. Since each shared value may have a different value space, let $\mathcal{S} = \{S_1, \cdots, S_n\}$;
5. The sharing function $\mathcal{E}$ is a probabilistic algorithm, denoted as $\{\beta_1, \cdots, \beta_n\} \leftarrow \mathcal{E}(\mathcal{P}, \Gamma_Q, \alpha)$. Among them, the secret value $\alpha \in \mathcal{K}$; the output is n shared values, and $\beta_i \in \mathcal{S}_i (1 \leq i \leq n)$;
6. The recovery function $\mathcal{D}$ is a deterministic algorithm, denoted as $\alpha' \leftarrow \mathcal{D}(\mathcal{A})$. Assuming that e participates in recovery, $\mathcal{A}$ is the set of shared values participating in secret recovery, $\mathcal{A} = \{\beta_{t_1}, \cdots, \beta_{t_e}\} = \mathcal{E}(\mathcal{P}, \Gamma_Q, \alpha)[\mathcal{P}]$, and $\mathcal{P} = \{\mathcal{P}_{t_1}, \cdots, \mathcal{P}_{t_e}\} \subseteq 2^{\mathcal{P}}$.

SS has the advantages of unconditional security, loss tolerance, and access control. Considering that SS has many advantages, the technology is widely used in the field of security, such as key management, password sharing, electronic voting, group signature authentication, and secure multi-party calculation, etc.

2.2. Polynomial-Based SIS

In 1979, Shamir proposed the polynomial-based SS. The sharing algorithm of the scheme is shown in Algorithm 1, and its recovery algorithm can be realized by Lagrangian interpolation. The core of polynomial-based SIS is $k-1$ order sharing polynomial $f(x) = a + a_1 x + \cdots + a_{k-1} x^{k-1} mod\ p$, where the value space is a finite field $\mathcal{K} = Z_p$, the modulus p is a prime power, the secret value $a \in \mathcal{K}$, and the random factors $a_1, \cdots, a_{k_1} \in \mathcal{K}$. Since the sharing and recovery algorithms are simple and efficient and there are few public parameters, the polynomial-based SIS is widely used and is often used as the basic algorithm for security protocol design [35–37].

```
**Algorithm 1** The polynomial-based SS
**Input**: $a,\ k,\ n.$
**Output**: $n$ cipher images $\beta_n$
**Step 1:** Select $n$ different non-zero elements in the finite field $Z_p$, denoted as $x_i$, $1 \le xi \le p-1$ ($p \ge n+1$ and $p$ is a prime number). $x_i$ can be made public.
**Step 2:** Randomly and independently select $k-1$ elements in the finite space $Z_p$, denoted as $a_1, \cdots, a_{k-1}$.
**Step 3:** Calculate $\beta_i = f(x_i), (1 \le i \le n)$ respectively, where $f(x) = a + \sum_{j=1}^{k-1} a_j x^j mod\ p$.
**Step 4:** The shared value $\beta_i$ is secretly sent to the corresponding participant $P_i$, $(1 \le i \le n)$.
```

Thien and Lin [38] introduced SS into the image field in 2002. The difference between SIS and SS is as follows:

1. a_i is the i_{th} pixel value of each group in each SS process.
2. p is selected as 251, and the pixels above 250 are treated as 250.

Thien–Lin's scheme shares a cipher image whose size is only $1/k$ of the original image, but in some cases, the cipher image will leak information about the original secret image. In order to avoid the security problem of Thien–Lin's scheme, our paper uses the original polynomial-based SIS scheme, that is, only a_0 is embedded with a pixel. In order to avoid the loss and distortion of secret pixels, this paper chooses $p = 257$. However, the maximum storage pixel of an image is 256, which means that if $\beta_i = 256$ occurs, it must be re-shared in the same way. The encryption scheme of SIS can effectively protect the privacy of secret images and can also protect against the loss of secrets. However, the cipher images generated by SIS are noise images, which is not convenient for management and use, and the efficiency is also very low. These are the factors that this article needs to improve and upgrade.

2.3. Thumbnail-Preserving Encryption

Wright et al. [21] proposed the concept of thumbnail-preserving encryption, that is, the cipher image presents the same visual content as the low-resolution version of the original image. The algorithm is shown in Algorithm 2.

```
**Algorithm 2** Thumbnail-preserving encryption
**Input**: Secret image of size $M \times N, K, B$.
**Output**: Cipher image.
**Step 1:** Use the passphrase to derive a secret symmetric key $K$ using a password based key derivation function.
**Step 2:** Color space transformation.
**Step 3:** Divide the secret image into blocks of $B \times B$ pixels and encrypt the pixels in each block by first permuting the order in which they appear.
```

The goal of TPE is to encrypt each block such that the cipher image reveals the average pixel value in the block but nothing more. This allows an untrusted third party who does not possess the key to reconstruct an accurate $M/B \times N/B$ pixel thumbnail, where each block in the cipher image corresponds to a single pixel in the thumbnail. The legal owner of the image has prior knowledge of the original image's visual characteristics, so the image owner can accurately identify and preview the image based on these low-resolution encrypted images [39,40].

TPE can not only protect the privacy of cloud-stored images but also can easily use today's cloud services to achieve a satisfactory balance between image privacy and usability. It is worth noting that the existing TPE scheme cannot resist information loss, which is worth promoting.

3. The Proposed Scheme

Our scheme fully considers the three elements of information security and realizes the full protection of secret images. Legitimate users can use our scheme to encrypt the secret image into meaningful cipher images. These cipher images have the characteristics of loss tolerance, which means that the loss of $n - k$ cipher images will not affect the recovery of the secret image, and fully protect the availability of the secret image. Even if a malicious user obtains up to $k - 1$ cipher images, the malicious user does not obtain any information of the secret image through visual information or computation and does not have any impact on the confidentiality of the secret image. The legitimate user can easily manage cipher images through visual features, and when at least k cipher images are obtained, the legitimate user can restore the secret image losslessly, ensuring the integrity of the secret. The detailed process can be referred to Figures 3 and 4.

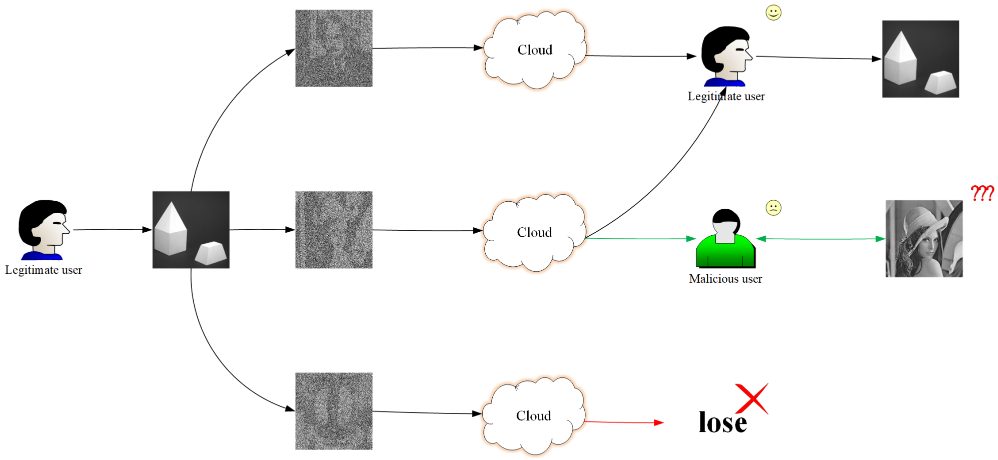


Figure 3. Our scheme, $k = 2, n = 3$.

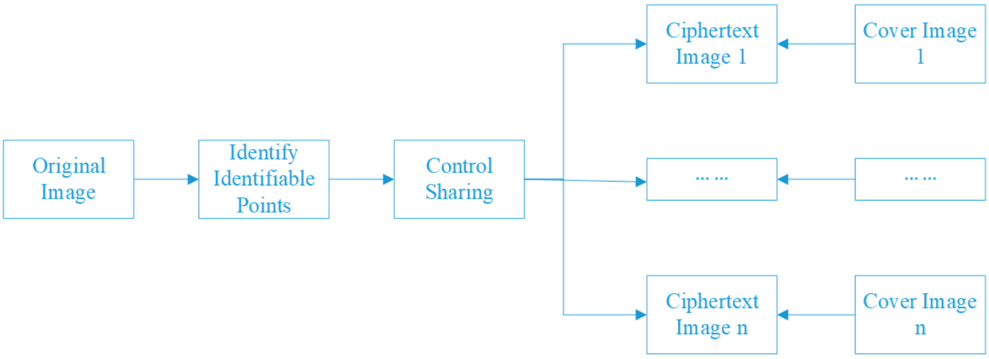


Figure 4. Flow chart of our scheme.

Our scheme is suitable for most high-value digital images, such as gray-scale images and color images. These images are composed of one or more channels, and each channel is a two-dimensional matrix array. Since the structure and value range of channels are the same, this paper mainly focuses on the single-channel image, that is, a gray-scale image. The range of gray image pixels is 0–255, that is, eight bits (one byte), which means that any data that can be represented by the binary stream are converted into a gray image. Therefore, through simple coding, any valuable binary data stream can be shared using the scheme presented in this paper.

The symbol description of the proposed scheme is shown in Table 1.

Table 1. Nomenclature.

Symbol	Description
P	Plain image
C	Secret image
M	Meaningful image carrier
i, j	The pixel values of i-th row and j-th column in the image
r, c	The number of rows and columns of the image
k, n	Threshold of the control sharing models
X	The serial number of the control sharing models
SC_X	Cipher image

3.1. Description of the Proposed Scheme

The scheme proposed in this paper mainly uses the knowledge of SS and thumbnails to realize the highly secure storage of secrets, which means that the confidentiality and integrity protection of secret images can be realized. Our proposed scheme mainly uses approximate thumbnails and control sharing models. Approximate thumbnails are mainly used to solve the usability problem of encrypted images. Unlike previous TPEs, the accuracy of our TPE images can be controlled on the premise that legitimate users with prior knowledge can be identified, and the overall pixel quality of the TPE image is lower than that of the original thumbnail. Controlling secret sharing is performed to solve the integrity of the secret and change the situation that the original shared cipher image is noise, which is based on approximate thumbnail sharing.

3.2. Approximate Thumbnails

Approximate thumbnails and thumbnails are visually similar, but the pixel accuracy is less than that of the original image.

In order to accurately describe the quality of approximate thumbnails, we introduce the following definitions.

Definition 1. *Thumbnail ratio: The thumbnail ratio $\Re$ refers to the ratio of the length (width) of the secret image to the length (width) of the original image. General thumbnails do not change the aspect ratio (the ratio of length to width) of the original image, so the usual thumbnail ratio is $\Re = C_r/P_r = C_c/P_c$.*

Definition 2. *Identification points: The identification point $[A : (i', j')]$ is the position of the pixel in the encrypted or shared cipher image that is similar to the meaningful image. The identification points can be calculated by Formula (1).*

$$A_{(i',j')} = \begin{cases} i' = \lfloor P_i \times \Re \rfloor \\ j' = \lfloor P_j \times \Re \rfloor \end{cases} \tag{1}$$

Corresponding to the identification points are the unidentification points $(\overline{A} : (i', j'))$. Through the definition and formula, it can be concluded that the identification point is only a part of the cipher image, and the cipher image is composed of identification points and unidentification points. That is, $C_{(i,j)} = A : (i', j') + \overline{A} : (i', j')$.

Definition 3. *High-level same bit number: The high-level same bit number is the maximum equal bit number of two integers from high to low in the binary representation of the same bit number, and its calculation formula is denoted as $\Omega(a, b)$.*

Definition 4. *Accuracy: Precision is the numerical similarity between the cipher image and the carrier image. The higher the precision is, the clearer the cipher image is, and vice versa. Precision* *only represents the numerical accuracy of the cipher image and the meaningful image, which can reflect the visual characteristics to a certain extent and can be obtained by Formula (2).*

$$\Phi = \Re^2 \times (1 - \frac{\sum_{g=1}^{\Omega(C_A,M_A)} 2^{8-g}}{2^8}) \tag{2}$$

The algorithm for approximate thumbnails is shown in Algorithm 3:

Algorithm 3 Approximate thumbnails

Input: $\Re, \Omega(C_A, M_A), M$

Output: Approximate thumbnails R.

Step 1: Determine the identifiable point A according to Re and Formula (1).

Step 2: Read the pixels value $M(i', j')$ of the carrier image according to the identifiable point.

Step 3: According to $M(i', j')$, $\Omega(C_A, M_A)$ determine the range R_1. The binary representation of $M(i', j')$ is $m_0 m_1 \ldots m_7$. The lower limit of R_1 is Formula (3),

$$\sum_{g=1}^{\Omega(C_A,M_A)} m_{g-1} \times 2^{8-g} \tag{3}$$

and the upper limit of R_1 is Formula (4)

$$2^{\Omega(C_A,M_A)} + \sum_{g=1}^{\Omega(C_A,M_A)} m_g \times 2^{8-g} \tag{4}$$

Step 4: The range of pixel values of non-identifiable point is $R_2 \subseteq [0, 255]$.

Step 5: R is obtained according to R_1 and R_2, shown as Formula (5).

$$R \begin{cases} R_1 = [\sum_{g=1}^{\Omega(C_A,M_A)} m_{g-1} \times 2^{8-g}, & \\ \quad 2^{\Omega(C_A,M_A)} + \sum_{g=1}^{\Omega(C_A,M_A)} m_g \times 2^{8-g}) & M(i', j') \\ R_2 = [0, 255] & \bar{M}(i', j') \end{cases} \tag{5}$$

3.3. Control Sharing Models

There are a large number of available random numbers in the multiple sharing of SS. Using these variable random numbers can make the range of sharing pixel values meet the expected requirements, which is often used in SIS with meaningful shadows.

Different from the SIS with meaningful shadows [41,42], controlling secret sharing only needs to control the value range of location pixels, and the sharing of non-location pixels can be uncontrolled. This controllable secret sharing is more operable and flexible than the original SIS.

The specific steps of controlling the sharing model are shown in Algorithm 4.

3.4. Security Analysis

SS has the perfect security feature of one secret at a time. When the number of shadows is less than k, no one can recover the secret, which has been proved in many works [43,44]. The main point of this scheme is the security equivalence of SS. However, the meaningful screening of pixels may have a certain impact on the security of the solution. Therefore, we conduct security analysis from the following two aspects.

```
**Algorithm 4** Control sharing models
**Input**: $k, n, X$, Secret image, Approximate thumbnail
**Output**: $n$ identifiable cipher images.
**Step 1:** Share each pixel in the secret image $P$.
**Step 2:** Judge whether $(i, j)$ is the identifiable point.
**Step 3:** If $(i, j)$ is a identifiable point, randomly adjust the value of $a_i$ until the value range of $f(x)$ is $C$; if it is not a identifiable point, just generate it directly.
And its basic principle is Formula (6).
    $$f(x) \in R \quad \left\{ \begin{array}{c} f(x) = M(i', j') + \sum_{j=1}^{k-1} a_j x^j mod\ p \\ a_j \in Z_p, a_j \in [0, p) \\ x \in Z_p \end{array} \right. \qquad (6)$$
**Step 4:** Repeat 1, 2, 3 until all pixels of the secret image are encrypted.
```

3.4.1. Security of Single Pixel

Suppose $k-1$ participants try to recover the master secret value α. According to the security conditions of threshold secret sharing, since there are only $k-1$ shared values, participants cannot obtain any secret value-related information. If the participant tries to guess the value of the $k-th$ shared value β_{i_k}, β_{i_k} has a total of η values, and the $n-element$ sharing sequence composed of known shared values corresponds to η possible secret values, that is, the recovered secret value obeys uniformity on a $\mathcal{K}$ distribution.

3.4.2. Security of Cipher Image

Due to the strong correlation between adjacent or close pixels of the secret image, even if the secret value is difficult to recover accurately, the special probability distribution characteristics of the shared sequence may leak visual information, such as texture features and contour information, posing certain security risks.

Theorem 1. *The hidden danger of visual information leakage increases with the increase of accuracy.*

Proof. Accuracy is determined by the high-level same bit number and the thumbnail ratio. The greater the high-level same bit number, the smaller the a_i space that meets the conditions. The larger the thumbnail ratio, the more positioning points, and the corresponding conditions to be met also increase, which means that the matching a_i space is reduced. When the value space of a_i becomes smaller, we believe that there is a security risk in a certain sense. □

In fact, without k shadows in the recovery stage, it is also impossible to recover the secret image. In this paper, by selecting the identifiable point, the correlation between the adjacent pixels of the secret image is destroyed to a certain extent, and the definition is further reduced. Compared with the original meaningful secret sharing, the proposed scheme has higher security.

3.5. Efficiency Analysis

Our scheme only needs to control the sharing process of $(M \times \Re)\ times(N \times \Re)$ pixels. Therefore, compared with the SIS with meaningful shadows, our scheme can effectively improve the efficiency of sharing. Assuming that the time for sharing a meaningful pixel is t_1, the total time for traditional meaningful sharing is shown in Formula (7), and T refers to the time used by other modules.

$$T_O = M * N * t_1 + T \qquad (7)$$

The time required for our scheme is shown in Formula (8).

$$T_N = (M \times \Re) \times (N \times \Re) \times t_1 + T \tag{8}$$

The time efficiency of improvement is shown in Formula (9). When T is negligible relative to $M * N * t_1$, $\approx$ holds. In fact, this is the case in most cases.

$$\frac{T_O}{T_N} = \frac{M * N * t_1 + T}{(M \times \Re) \times (N \times \Re) \times t_1 + T} \approx \frac{1}{\Re^2} \tag{9}$$

This is a comparison of theoretical efficiency, and we also give a comparison of the actual time efficiency in the experiment.

4. Experiments

In this section, the experimental data and results prove that the proposed scheme can achieve the expected effect and realize the effective protection of secret images. The experiment part includes four parts—thumbnail secret sharing, parametric analysis, efficiency comparison, and the thumbnail secret sharing of color images—that prove our scheme from different angles. As a single-channel image, a gray-scale image is the basis of the image and has strong scalability. Therefore, our experiment includes most gray-scale images and a few color images. For the impact of parameters, we also give the relevant data and analysis. In order to compare with the original meaningful secret sharing, we carried out the experimental comparison on the basis of theoretical analysis.

The relevant images used in this paper are shown in Figure 5a–g.

(**a**) *Peppers* (**b**) *Lena* (**c**) *Avion* (**d**) *Baboon*

(**e**) *Indor* (**f**) *Cameraman* (**g**) *Einstein*

Figure 5. Relevant images.

Our implementation is written in Python, and we use the NumPy library for both 64 bit integer and float-point computations. We conduct our experiments on a desktop computer equipped with a 16-core Intel i7-10 CPU and 16 Gb RAM.

4.1. Thumbnail Secret Sharing

In order to verify the universality of the scheme, we select two groups of thumbnail sharing experimental results with different thresholds, high-level same bit number, and image size.

The secret image is Figure 6a, the size is 128 × 128, the thumbnail ratio $\Re$ is 0.5, the high-level same bit number $\Omega(S, SC_i)$ is 2, the sharing threshold is $(2, 3)$, the value of the serial number is $[103, 145, 177]$, and the shared cipher images are shown in Figure 6b–d.

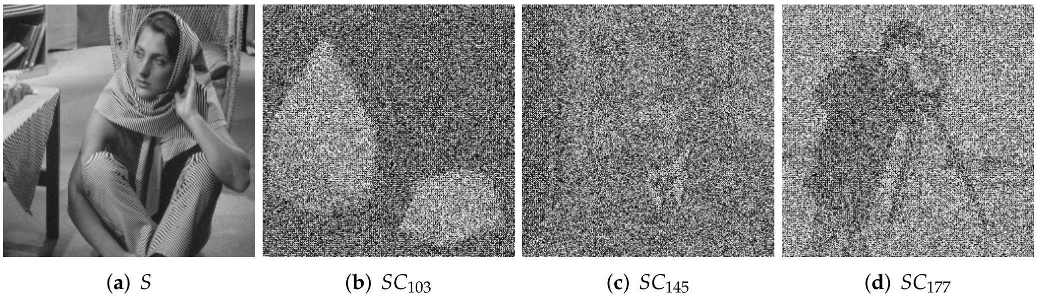
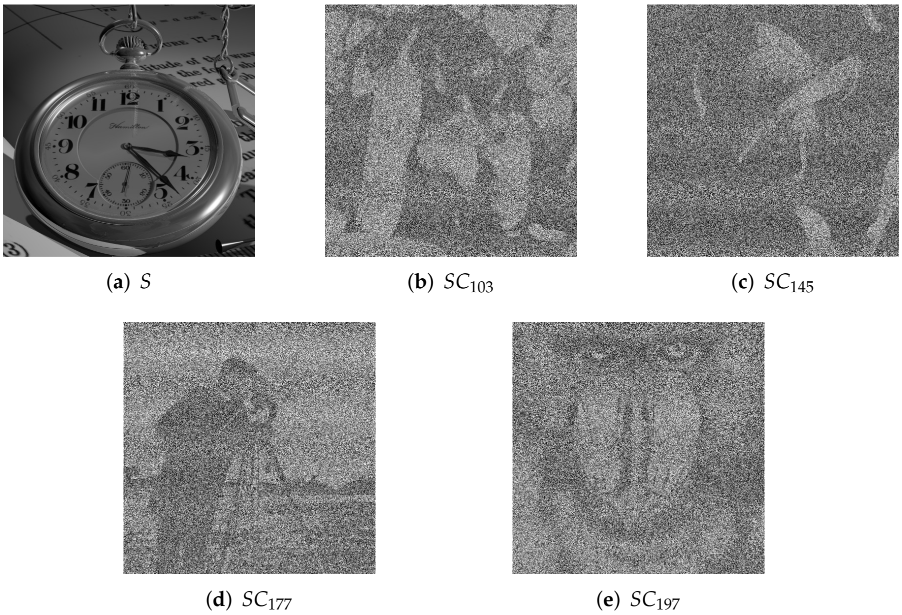

(**a**) S (**b**) SC_{103} (**c**) SC_{145} (**d**) SC_{177}

Figure 6. Experiment 1 of thumbnail secret sharing.

The secret image is Figure 7a, the size is 256 × 256, the thumbnail ratio $\Re$ is 0.5, the high-level same bit number $\Omega(S, SC_i)$ is 1, the sharing threshold is $(3, 4)$, the value of the serial number is $[103, 145, 177, 197]$, and the shared cipher images are shown in Figure 7b–e. Any three of the cipher images can be selected to restore the secret image in Figure 7a.


(**a**) S (**b**) SC_{103} (**c**) SC_{145}

(**d**) SC_{177} (**e**) SC_{197}

Figure 7. Experiment 2 of thumbnail secret sharing.

The secret image is Figure 8a, the size is 512 × 512, the thumbnail ratio $\Re$ is 0.5, the high-level same bit number $\Omega(S, SC_i)$ is 3, the sharing threshold is $(3, 3)$, the value of the serial number is $[103, 145, 177]$, and the shared cipher images are shown in Figure 8b–d. All cipher images can restore the secret image in Figure 8a.

We adjust the thumbnail ratio $\Re$ and high-level same bit number $\Omega(a, b)$ through the algorithm so that the accuracy of the cipher image is Φ. It is very easy for legitimate users with prior knowledge to identify the cipher images by adjusting the accuracy.

Experiments show that the visual characteristics of the cipher images can quickly identify the thumbnails corresponding to different serial numbers, and at the same time, the secret can be recovered when one of them is lost, which realizes the management of the cipher images and loss tolerance.

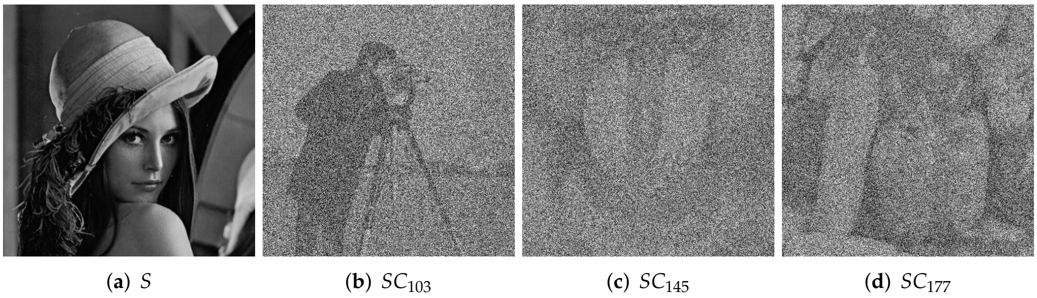


Figure 8. Experiment 1 of thumbnail secret sharing.

4.2. Thumbnail Secret Sharing of Color Images

To verify the availability of the scheme for color images (multi-channel images), we performed this experiment. The experimental results are similar to those of a single channel, which proves that our scheme can be applied to most digital images. The secret image is Figure 9a, the size is 512 × 512, the thumbnail ratio $\Re$ is 0.5, the high-level same bit number $\Omega(S, SC_i)$ is 1, the sharing threshold is $(3, 3)$, the value of the serial number is $[103, 145, 177]$, and the shared cipher images are shown in Figure 9b–d.

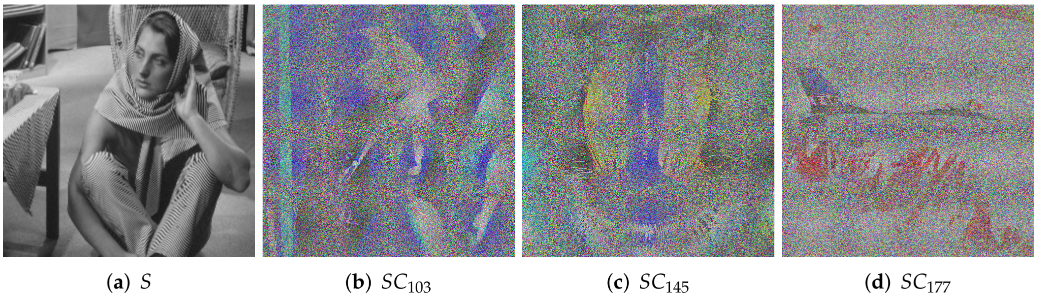


Figure 9. Thumbnail Secret Sharing of color images.

The color image is composed of RGB three channels, and its basic principle is similar to that of a single channel image. Therefore, our scheme is suitable for the protection of most digital images, which is well proved in this experiment.

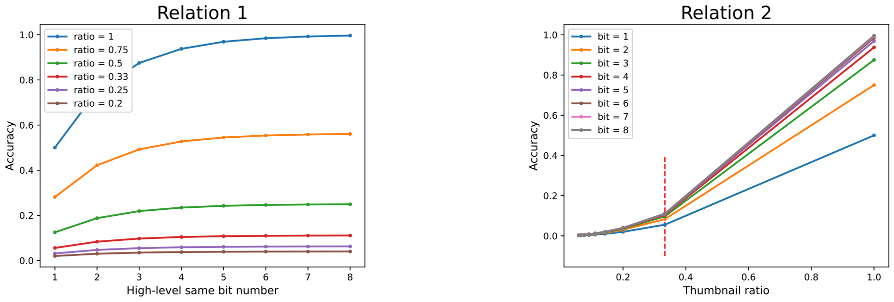
4.3. Parametric Analysis

According to Formula (2), we draw the relationship between the high-level same bit number and accuracy in Figure 10a, with the relationship between compression rate and accuracy in Figure 10b. By analyzing the visual quality of relation graphs and cipher images, we obtain the following conclusions and suggestions. Compared with the high-level same bit number, the thumbnail rate has a greater impact on accuracy and visual quality. When the thumbnail ratio is greater than 0.33, the accuracy will decrease rapidly as the compression ratio decreases, and the recognition rate will drop rapidly.

We obtain the following parameter relationship:

1. When the thumbnail rate is greater than 0.33, the high-level same bit number can be appropriately reduced.
2. When the thumbnail rate is below 0.33, the high-level same bit number should be appropriately increased.

We analyze the relationship among the high-level same bit number, thumbnail ratio, and accuracy and obtain the regular characteristics between them. According to our conclusion, users can choose parameters flexibly according to their needs.



(**a**) Relation between $\Omega(a, b)$ and Φ

(**b**) Relation between $\Re$ and Φ

Figure 10. Relation between $\Omega(a, b)$,$\Re$ and Φ.

4.4. Comparison

4.4.1. Efficiency Comparison

The theoretical efficiency is analyzed in our paper. In this section, through the comparison of the time used in the listed experiments, it can be proved that our scheme can effectively improve efficiency. We select the classic SIS with meaningful shadows for comparison, which are used in multiple schemes [41,42]. We compare several dimensions, including threshold, compression ratio $\Re$, and the highest bit number $\Omega(a, b)$, and obtain the running time (T_N, T_O) and efficiency comparison (T_N/T_0). It can be seen from Table 2 that the efficiency comparison(T_N/T_0) of our scheme is better than that of the SIS with meaningful shadows, and the efficiency improvement of some experimental results is very obvious, which fully shows the efficiency of the proposed scheme.

Table 2. Time comparison.

Threshold	$\Re$	$\Omega(a, b)$	$T_O(s)$	$T_N(s)$	$T_N/T_0(\%)$
(2,3)	0.5	1	11.41	4.16	36.46
(3,4)	0.5	1	23.61	7.51	31.81
(2,3)	0.25	1	11.67	2.54	21.77
(3,4)	0.25	1	23.22	3.18	13.69
(2,3)	0.5	2	92.80	25.10	27.05
(3,4)	0.5	2	367.13	94.64	25.78
(2,3)	0.25	2	90.83	7.41	8.16
(3,4)	0.25	2	362.51	25.44	7.02
(2,2)	0.5	3	82.92	22.76	27.45
(3,3)	0.5	3	690.28	181.46	26.28
(3,3)	0.25	3	759.38	51.80	6.82
The image size is 256 × 256					
Threshold	$\Re$	$\Omega(a, b)$	$T_O(s)$	$T_N(s)$	$T_N/T_O(\%)$
(3,3)	0.5	1	44.06	16.58	37.63
(3,4)	0.5	1	92.96	28.88	31.07
(3,4)	0.25	1	93.11	12.56	13.49
(3,4)	0.25	2	1445.35	100.24	6.94
(3,3)	0.5	2	339.13	91.22	26.90
(3,3)	0.5	3	35,723.44	693.56	1.94
(3,4)	0.25	3	124,172.21	1576.81	1.27
The image size is 512 × 512					

4.4.2. Functional Comparison

Our scheme has the complete functions and the fastest efficiency among all the current schemes. The comparison of specific functions is shown in Table 3.

Table 3. Functional comparison.

Scheme	Confidentiality	Management	Loss Tolerance
Upload directly	No	Yes	No
Direct encryption	Yes	No	No
TPE	Yes	Yes	No
SIS	Yes	No	Yes
SIS with meaningful shadows	Yes	Yes	Yes
Our scheme	Yes	Yes	Yes

Confidentiality refers to the encryption of the image, which is the basic requirement of image security. In addition to uploading directly, other schemes are encrypted. Management is performed to manage images in the cloud through uploaded images. Directly encryption and SIS are noise images that cannot be directly managed; while uploaded directly, TPE and SIS with meaningful shadows and our scheme are all visually distinguishable images, showing that the management of images is possible. Loss tolerance refers to the ability to restore the secret image without loss after the uploaded image is lost. Uploading directly, direct encryption, and TPE have only one uploaded image, and the secret image cannot be restored after the file is lost. Only the functions of our scheme and SIS with meaningful shadows are the most comprehensive. In combination with the efficiency comparison in Table 2, we find that our scheme is the best at present.

5. Conclusions

Aiming at resolving the problem of secret image management and loss in cloud space, this paper proposes a thumbnail secret sharing scheme based on thumbnail encryption and secret sharing, which mainly includes approximate thumbnails and control sharing models. The cipher image of the proposed scheme has the characteristics of visual recognition and loss tolerance. Visual recognition solves the management problem of cipher images and improves the availability of cipher images. Loss tolerance ensures the integrity and availability of important confidential images. The security and efficiency of the proposed scheme are analyzed and discussed. In addition, experiments and comparisons show that the proposed scheme has good visual characteristics and loss tolerance, and the efficiency of the scheme is significantly improved, which greatly improves the secret availability and security. In the future, reducing data redundancy and communication overheads are problems that need to be solved.

Author Contributions: Conceptualization, Y.Y. and X.Y.; methodology, Y.Y.; validation, S.W., X.W. and H.L.; formal analysis, S.W.; investigation, X.W.; data curation, H.L.; writing—original draft preparation, Y.Y.; writing—review and editing, S.W., X.W. and H.L.; supervision, X.Y.; funding acquisition, X.Y. 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.

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

References

1. Dong, Y.; Ding, Z.; Chiclana, F.; Herrera-Viedma, E. Dynamics of Public Opinions in an Online and Offline Social Network. *IEEE Trans. Big Data* **2021**, *7*, 610–618. [CrossRef]
2. Banerjee, S.; Jenamani, M.; Pratihar, D.K. A survey on influence maximization in a social network. *Knowl. Inf. Syst.* **2020**, *62*, 3417–3455. [CrossRef]
3. Osman, M. Wild and Interesting Facebook Statistics and Facts (2021). Available online: https://kinsta.com/blog/facebook-statistics/ (accessed on 3 January 2021).

4. Aslam, S. Facebook by the Numbers: Stats, Demographics & Fun Facts. Available online: https://www.omnicoreagency.com/facebook-statistics/ (accessed on 22 February 2022).
5. Pantic, N. How Many Photos Will Be Taken in 2021? 2021 Available online: https://blog.mylio.com/how-many-photos-will-be-taken-in-2021-stats/ (accessed on 18 July 2022).
6. Li, J.; Yan, H.; Zhang, Y. Certificateless Public Integrity Checking of Group Shared Data on Cloud Storage. *IEEE Trans. Serv. Comput.* **2021**, *14*, 71–81. [CrossRef]
7. Zhang, Y.; Xu, C.; Lin, X.; Shen, X. Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors. *IEEE Trans. Cloud Comput.* **2021**, *9*, 923–937. [CrossRef]
8. Zhang, Y.; Yu, J.; Hao, R.; Wang, C.; Ren, K. Enabling Efficient User Revocation in Identity-Based Cloud Storage Auditing for Shared Big Data. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 608–619. [CrossRef]
9. Shen, W.; Qin, J.; Yu, J.; Hao, R.; Hu, J. Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure Cloud Storage. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 331–346. [CrossRef]
10. Aslam, S. Main Cloud Security Issues and Threats in 2021. 2021. Available online: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/ (accessed on 18 July 2022).
11. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
12. Lakshmi, V.S.; Deepthi, S.; Deepthi, P.P. Collusion resistant secret sharing scheme for secure data storage and processing over cloud. *J. Inf. Secur. Appl.* **2021**, *60*, 102869. [CrossRef]
13. Meng, S.; Huang, W.; Yin, X.; Khosravi, M.R.; Li, Q.; Wan, S.; Qi, L. Security-Aware Dynamic Scheduling for Real-Time Optimization in Cloud-Based Industrial Applications. *IEEE Trans. Ind. Inform.* **2021**, *17*, 4219–4228. [CrossRef]
14. Mishra, P.; Varadharajan, V.; Pilli, E.S.; Tupakula, U. VMGuard: A VMI-Based Security Architecture for Intrusion Detection in Cloud Environment. *IEEE Trans. Cloud Comput.* **2020**, *8*, 957–971. [CrossRef]
15. Masood, F.; Driss, M.; Boulila, W.; Ahmad, J.; Jan, S.U.; Qayyum, A.; Buchanan, W. A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations. *Wirel. Pers. Commun.* **2021**. [CrossRef]
16. Guo, S.; Xiang, T.; Li, X.; Yang, Y. PEID: A Perceptually Encrypted Image Database for Visual Security Evaluation. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 1151–1163. [CrossRef]
17. Hua, Z.; Zhu, Z.; Chen, Y.; Yuanman, L. Color image encryption using orthogonal Latin squares and a new 2D chaotic system. *Nonlinear Dyn.* **2021**, *104*, 1–18. [CrossRef]
18. Hua, Z.; Zhang, K.; Li, Y.; Zhou, Y. Visually secure image encryption using adaptive-thresholding sparsification and parallel compressive sensing. *Signal Process.* **2021**, *183*, 107998. [CrossRef]
19. Yang, C.N.; Lin, Y.C.; Li, P. Cheating immune k-out-of-n block-based progressive visual cryptography. *J. Inf. Secur. Appl.* **2020**, *55*, 102660. [CrossRef]
20. Yan, X.; Liu, X.; Yang, C.N. An enhanced threshold visual secret sharing based on random grids. *J. Real-Time Image Process.* **2018**, *14*, 61–73. [CrossRef]
21. Wright, C.V.; Feng, W.C.; Liu, F. Thumbnail-Preserving Encryption for JPEG. In Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, Portland, OR, USA, 17–19 June 2015; IH&MMSec '15; Association for Computing Machinery: New York, NY, USA, 2015; pp. 141–146. [CrossRef]
22. Marohn, B.; Wright, C.V.; Feng, W.C.; Rosulek, M.; Bobba, R.B. Approximate Thumbnail Preserving Encryption. In Proceedings of the 2017 on Multimedia Privacy and Security, Dallas, TX, USA, 30 October 2017; MPS '17; Association for Computing Machinery: New York, NY, USA, 2017; pp. 33–43. [CrossRef]
23. Chai, X.; Wang, Y.; Chen, X.; Gan, Z.; Zhang, Y. TPE-GAN: Thumbnail Preserving Encryption Based on GAN With Key. *IEEE Signal Process. Lett.* **2022**, *29*, 972–976. [CrossRef]
24. Bellare, M.; Ristenpart, T.; Rogaway, P.; Stegers, T. Format-Preserving Encryption. In *Selected Areas in Cryptography*; Jacobson, M.J., Rijmen, V., Safavi-Naini, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 295–312.
25. Tajik, K.; Gunasekaran, A.; Dutta, R.; Ellis, B.; Bobba, R.; Rosulek, M.; Wright, C.; Feng, W.C. Balancing Image Privacy and Usability with Thumbnail-Preserving Encryption. In Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, USA, 24–27 February 2019. [CrossRef]
26. Zhang, Y.; Zhao, R.; Xiao, X.; Lan, R.; Liu, Z.; Zhang, X. HF-TPE: High-Fidelity Thumbnail- Preserving Encryption. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 947–961. [CrossRef]
27. Zhao, R.; Zhang, Y.; Xiao, X.; Ye, X.; Lan, R. TPE2 : Three-Pixel Exact Thumbnail-Preserving Image Encryption. *Signal Process.* **2021**, *183*, 108019. [CrossRef]
28. Houmani, H.; Mejri, M. Secrecy by interpretation functions. *Knowl.-Based Syst.* **2007**, *20*, 617–635. [CrossRef]
29. Yan, X.; Lu, Y.; Yang, C.N.; Zhang, X.; Wang, S. A Common Method of Share Authentication in Image Secret Sharing. *IEEE Trans. Circuits Syst. Video Technol.* **2021**, *31*, 2896–2908. [CrossRef]
30. Li, P.; Ma, J.; Ma, Q. (t, k, n) XOR-based visual cryptography scheme with essential shadows. *J. Vis. Commun. Image Represent.* **2020**, *72*, 102911. [CrossRef]
31. Yan, X.; Li, J.; Pan, Z.; Zhong, X.; Yang, G. Multiparty verification in image secret sharing. *Inf. Sci.* **2021**, *562*, 475–490. [CrossRef]
32. Wu, X.; Yang, C.N.; Li, J.M. Secure image secret sharing over distributed cloud network. *Signal Process.* **2021**, *178*, 107768. [CrossRef]

33. Shamir, A. How to Share a Secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
34. Blakley, G.R. Safeguarding cryptographic keys. In Proceedings of the 1979 International Workshop on Managing Requirements Knowledge (MARK), New York, NY, USA, 4–7 June 1979; pp. 313–318. [CrossRef]
35. Yan, X.; Lu, Y.; Liu, L.; Song, X. Reversible Image Secret Sharing. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3848–3858. [CrossRef]
36. Li, L.; Hossain, M.S.; El-Latif, A.A.A.; Alhamid, M.F. Distortion Less Secret Image Sharing Scheme for Internet of Things System. *Clust. Comput.* **2019**, *22*, 2293–2307. [CrossRef]
37. Yan, X.; Liu, L.; Li, L.; Lu, Y. Robust Secret Image Sharing Resistant to Noise in Shares. *ACM Trans. Multimedia Comput. Commun. Appl.* **2021**, *17*, 1–22. [CrossRef]
38. Thien, C.C.; Lin, J.C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [CrossRef]
39. Jiang, D.; Liu, L.; Zhu, L.; Wang, X.; Rong, X.; Chai, H. Adaptive embedding: A novel meaningful image encryption scheme based on parallel compressive sensing and slant transform. *Signal Process.* **2021**, *188*, 108220. [CrossRef]
40. Yang, C.N.; Tsai, P.Y.; Liu, Y. A (k, n) secret document sharing with meaningful shares. *J. Inf. Secur. Appl.* **2021**, *62*, 102973. [CrossRef]
41. Ateniese, G.; Blundo, C.; Santis, A.D.; Stinson, D.R. Extended capabilities for visual cryptography. *Theor. Comput. Sci.* **2001**, *250*, 143–161. [CrossRef]
42. Cheng, J.; Yan, X.; Liu, L.; Jiang, Y.; Wang, X. Meaningful Secret Image Sharing with Saliency Detection. *Entropy* **2022**, *24*, 340. [CrossRef] [PubMed]
43. Pedersen, T.P. Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In Proceedings of the Advances in Cryptology—CRYPTO'91, 11th Annual International Cryptology Conference, Santa Barbara, CA, USA, 11–15 August 1991; Feigenbaum, J., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1991; Volume 576, pp. 129–140. [CrossRef]
44. Cramer, R.; Damgård, I.; Nielsen, J.B. *Secure Multiparty Computation and Secret Sharing*; Cambridge University Press: Cambridge, UK, 2015.