mathematics

MDPI

Article

Multi Secret Image Sharing Scheme of General Access Structure with Meaningful Shares

Hongliang Cai [1,2] and Dan Tang [1,2,*]

[1] School of Software Engineering, Chengdu University of Information Technology, Chengdu 610225, China; caihl@cuit.edu.cn

[2] The Software Engineering Technology Research Support Center of Informatization Application of Sichuan, Chengdu 610225, China

* Correspondence: tangdan@cuit.edu.cn; Tel.: +86-028-85622926

Received: 23 July 2020; Accepted: 7 September 2020; Published: 14 September 2020

Abstract: A Multi Secret Image sharing scheme can share several secret images among certain participators securely. Boolean-based secret sharing schemes are one kind of secret sharing method with light-weighted computation compared to the previous complex algebraic-based methods, which can realize the sharing of multi secret images. However, the existing Boolean-based multi secret sharing schemes are mostly restricted to the particular case of (2, n) and (n, n), only few Boolean-based multi secret sharing schemes study the general access structure, and the shares are mostly meaningless. In this paper, a new Boolean-based multi secret sharing scheme with the general access structure is proposed. All the shares are meaningful, which can avoid attracting the attention of adversaries, and the secret images can be recovered in a lossless manner. The feasibility of the scheme is proven, the performance is validated by the experiments on the gray images, and the analysis of the comparison with other methods is also given out.

Keywords: image secret sharing; multi secret sharing; lossless recovery; Boolean operation

1. Introduction

The secret sharing scheme was firstly proposed by Shamir [1] and Blakley [2] in 1979. Unlike the traditional encryption methods such as RSA which encrypt a piece of original plaintext into a piece of ciphertext, in the secret sharing scheme, the secret information is split into several pieces called shares using the secret sharing method and distributed between a group of participants, and only the participants in the qualified set can retrieve the secret information. Secret sharing can be used in many fields, such as the key management [3], access control [4], intelligent transportation [5], distributed computing in the cloud [6], and so forth. Recently, a new kind of secret division and sharing method called cognitive cryptography [7–10] was developed; it is a novel approach with the individual biometric features of each participator, which is an innovative solution in the sharing process allowing the owner of one share to be verified using the biometric feature, and can improve the security of the secret sharing.

In 1994, Shamir developed Visual Cryptography (VC) [11] which can encrypt binary images into several shares with random black and white pixels. The basic idea of VC is to use different binary matrices to represent the black and white pixel; the shares are generated based on the binary matrices by each pixel and printed on the transparencies, and the secret image can be recovered by simply overlapping the transparencies and can be recognized by the Human Vision System (HVS). The advantage of VC is that is can easily recover the secret image without any compute device, but it also has the disadvantage of pixel expansion which means the size of the shares is always much bigger

than the original secret image, and another drawback is the low contrast, which means the recovered image is always has low recovery quality.

To deal with the problem of pixel expansion, probabilistic Visual Cryptography [12] was firstly proposed by Yang. With this method, the size of the share can be reduced to be the same as the secret image, but the quality of the recovered image is still low. Another secret sharing method which is based on the random grid [13] also can deal with the pixel expansion problem, but it is in fact equivalent to the probabilistic Visual Cryptography, so the quality of the recovered image is also poor.

Another way to overcome the problem of VC is polynomial-based Image Secret Sharing (ISS) [14], which introduced the Lagrange polynomial method into the image sharing. The pixel value of the shares is generated by the polynomial, and the secret is recovered by the polynomial interpolation. It overcomes the pixel expansion problem; the shares are even smaller than the secret image, and the recovered image is mostly the same as the secret image. However, the drawback is its highly complex computation due to the polynomial operation.

Boolean-based Image Secret sharing can achieve a better tradeoff between the pixel expansion, image quality, and the computation complex. In 2006, Wang et al. [15] proposed two XOR-based Image Secret Sharing Schemes for a single secret image; one is a probabilistic (2, n) threshold scheme for the binary image, and the other is a deterministic (n, n) threshold scheme for the gray-scale image. The size of the shares is the same as the secret image, and the recovered secret image is the same as the original secret image. Some other Boolean-based Image Secret sharing schemes are developed in [16–20], all these schemes have no or little pixel expansion, and the decryption is easy.

To realize sharing several secret images simultaneously, multi secret sharing schemes are developed. Some works focus on the particular (n, n) or the (k, n) threshold multi secret sharing scheme, only a few works focus on the multi secret sharing with the general access structure. The literature on the multi secret sharing schemes is covered in Section 2.

2. Related Work

Multi secret sharing schemes can share many secret images at one time. There are many kinds of the multi secret sharing scheme using different methods. In [21], the paradigm of the multi secret sharing was given out by Padiya et al. and the genetic method was developed as a kind of encryption. Weir et al. [22] proposed a scheme based on Visual Cryptography method, but the quality of the recovered secret images was very poor. Aarti et al. [23] used the extended Visual Cryptography method and mixing method to realize multi secret sharing.

Another way to construct the multi secret sharing is to use the matrix methods. Wang et al. [24] used the matrix projection methods to share multi secret images, and Fereshte et al. [25] used matrix multiplication method to realize the construction.

Some other research has been developed based on the polynomial methods or modulo method. Yang et al. [26] used the Lagrange interpolation polynomial method to share multi secret images, while Adachi et al. [27] constructed a (t, n) multi secret sharing scheme by Hermite interpolation, which can analyze the image more precisely than the Lagrange interpolation, but is more complex. Harn et al. [28] used another polynomial method which is the bivariate polynomial to share the multi secrets which can generate keys between the pair of the share owners. Chang et al. [29] applied the Chinese remainder method and the Lagrange Interpolation method in the sharing. Deshmukh et al. [30] realized the multi secret sharing combining with XOR operation. Mohit et al. [31] used the additive modulo method to realize the (n, n + 1) multi secret sharing scheme.

The researchers mentioned above constructed multi secret sharing schemes based on the different methods. Different kinds of schemes have their advantage, but they each also have some drawbacks. For example, the schemes based on the visual cryptography have the advantage of low computation complexity, but they always suffer from the problem of the poor recovery quality and the pixel expansion. The schemes based on the algebraic methods such as matrix methods, polynomial methods,

and Chinese remainder method can get much better recovery quality, but they always have the disadvantage of the high computation complexity.

Boolean-based multi secret sharing schemes are the new method of multi secret sharing using simple Boolean operations with high recovered quality and no pixel expansion. Some research focused on the threshold scheme. Chen [32] gave out the first Boolean-based multi secret sharing scheme; all the shares are random, and it has (n + 1, n + 1) threshold which means all the n + 1 shares are necessary in the recovery of the n secret images. Later, Chen [33] proposed (n, n) multi secret sharing based on XOR operation and bit shift method. Yang et al. [34] constructed an n out of n multi secret sharing scheme, where no information can be recovered when there are less than n participants. Chen et al. [35] proposed a novel multi secret sharing scheme using Boolean operation and the hash method which can share different sizes of secret images. Deshmukh [36] proposed the (n, n) multi secret sharing scheme based on the XOR operation and modulo operation. Kabirirad et al. [37] developed a scheme with the random shares with low complexity based on Boolean operations. Prasetyo and Guo [38] proposed a multi secret sharing scheme based on the XOR and the Chinese remainder method which can share n secret images using n shares.

Some other research works focus on the secret sharing scheme with the general access structure. There are several works about sharing one secret with the general access structure [39,40]. Only a few works concern the multi secret sharing scheme with the general access structure. Das [41] proposed a multi secret sharing scheme with general access through the hash method. Yan [42] proposed the progressive sharing with general access structure using the Boolean operation. In 2019, Nag [43] proposed a multi secret sharing scheme with general access based on the Boolean operation; the shares are meaningless, and the concept of the public share is introduced, which come from the idea in [44]—the public share having high privilege participates in the recovery together with the owners' meaningless shares, which does not violate the basic principle of secret sharing. Meghrajani et al. [45] shared multi secret sharing using Boolean operation using the public share. In 2020, Chen [46] proposed a multi secret sharing scheme with the general access structure, which does not need to collect all the shares, and where the defined qualified participators can recover the secret images, and the shares are meaningless.

From the literature survey, we notice that there are many multi secret sharing schemes with different characteristics, but there is no multi secret sharing scheme with the general access structure that can recover the secret exactly and at the same time the shares are all meaningful. As such, in this paper, we propose a multi secret image sharing scheme with general access structure and meaningful shares based on the Boolean operation.

3. Preliminary

3.1. General Access Structure

Suppose there are N participators, $O = \{1, 2, 3, \ldots, N\}$, which is the identity number of the participators, each participator will own one share, $OW = \{OW_i\}$ is the owners of the shares, $i \in [1, n]$.

Suppose the qualified part is P_{qual}, $P_{qual} = \{QS_1, QS_2, \ldots, QS_n\}$, where QS_i is the ith qualified subset $i \in [1, n]$, $QS_i = \{i_1, i_2, \ldots, i_t\}$, which means the ith qualified subset QS_i consists of the t owners whose identity number is $i_1, i_2, \ldots, i_t$, so the $OW_{i_1}, OW_{i_2}, \ldots, OW_{i_t}$ can recover the ith secret. The forbidden part is P_{forbid}, $P_{forbid} = \{FS_1, FS_2, \ldots, FS_m\}$, where FS_i is the ith forbidden subset $i \in [1, m]$, $FS_j = \{j_1, j_2, \ldots, j_r\}$, which means the j_1th, j_2th, $\ldots$, j_rth owner are forbidden to recover the secret. P_{qual} and P_{forbid} is not empty, $P_{qual} \subset 2^O$, $P_{forbid} \subset 2^O$, and $P_{qual} \cap P_{forbid} = \varnothing$.

Denote P_0 as the set of the minimum qualified set:

$$P_0 = \left\{ Q \in P_{qual} : Q' \notin P_{qual}, \forall Q' \subset Q \right\} \tag{1}$$

As such, each element of P_{qual} is the minimum qualified subset.

The element C in O is called as the valid element, when there is at least one qualified subset concluding this element, i.e.,

$$\left\{D|D \cup \{C\} \in P_{qual}, D \notin P_{qual}\right\} \neq \varnothing \tag{2}$$

In this paper, we suppose all the elements or owners are valid, there is no element not participating in the sharing.

3.2. Relationship between the Operation on GF(2^m) and Bit-Wise XOR Operation

As we know, the pixels of the image can be expressed by m bits. For example, the pixels of the black-and-white image are expressed by 1 bit, and the pixels of the 256 gray level image are always expressed by 8 bits. For the 256 gray level image, the gray value is in fact isomorphic to the element over $GF(2^8)$. Thus, the operations of the pixels of the images are executed on the $GF(2^8)$. The operation on the Galois field can be found in [47].

In this paper, the additional operation on the $GF(2^m)$ is used in the secret sharing process and the recovery process, and the addition operation on the different elements is in fact the XOR operation of the coefficients of the polynomials for the different elements; so, for the pixel of m bits, the addition operation between the images is equivalent to the m bit-wise XOR operation.

Suppose there are two images X and Y which are m gray level and the size of each image $A \times B$, the pixel value in the rowth row and the colth column of OS_i is $px^X_{(row,col)}$, which is integer, $px^X_{(row,col)} \in [0, 2^m - 1]$, $row \in [1, A]$, and $col \in [1, B]$. As each pixel of the image X can be turned into $\log_2 m$ bits, suppose $px^X_{(row,col)} = \left\{bx_1, bx_2, \ldots, bx_{\log_2 \mathrm{m}}\right\}$, similarly, each pixel of the image Y can be expressed by $px^Y_{(row,col)} = \left\{by_1, by_2, \ldots, by_{\log_2 \mathrm{m}}\right\}$, so the addition operation between the pixel of the image X and Y in the same position is defined as below,

$$\begin{aligned} px^X_{(row,col)} \oplus px^Y_{(row,col)} &= \left\{bx_1, bx_2, \ldots, bx_{\log_2 \mathrm{m}}\right\} \oplus \left\{by_1, by_2, \ldots, by_{\log_2 \mathrm{m}}\right\} \\ &= \left\{bx_1 \oplus by_1, bx_2 \oplus by_2, \ldots, bx_{\log_2 \mathrm{m}} \oplus by_{\log_2 \mathrm{m}}\right\} \end{aligned} \tag{3}$$

And the image X can be expressed by the matrix $MX_{A\times B}$.

$$MX_{A\times B} = \begin{bmatrix} px^X_{(1,1)} & \cdots & px^X_{(1,\mathrm{B})} \\ \cdots & px^X_{(row,col)} & \cdots \\ px^X_{(\mathrm{A},1)} & \cdots & px^X_{(A,B)} \end{bmatrix} \tag{4}$$

The image Y can be expressed by the matrix $MY_{A\times B}$.

$$MY_{A\times B} = \begin{bmatrix} px^Y_{(1,1)} & \cdots & px^Y_{(1,\mathrm{B})} \\ \cdots & px^Y_{(row,col)} & \cdots \\ px^Y_{(\mathrm{A},1)} & \cdots & px^Y_{(A,B)} \end{bmatrix} \tag{5}$$

As such, the addition of the image X and Y can be expressed by the XOR between the matrix $MX_{A\times B}$ and $MY_{A\times B}$,

$$\begin{aligned} MX_{A\times B} \oplus MY_{A\times B} &= \begin{bmatrix} px^X_{(1,1)} & \cdots & px^X_{(1,\mathrm{B})} \\ \cdots & px^X_{(row,col)} & \cdots \\ px^X_{(A,1)} & \cdots & px^X_{(A,B)} \end{bmatrix} \oplus \begin{bmatrix} px^Y_{(1,1)} & \cdots & px^Y_{(1,\mathrm{B})} \\ \cdots & px^Y_{(row,col)} & \cdots \\ px^Y_{(\mathrm{A},1)} & \cdots & px^Y_{(A,B)} \end{bmatrix} \\ &= \begin{bmatrix} px^X_{(1,1)} \oplus px^Y_{(1,1)} & \cdots & px^X_{(1,\mathrm{B})} \oplus px^Y_{(1,\mathrm{B})} \\ \cdots & px^X_{(row,col)} \oplus px^Y_{(row,col)} & \cdots \\ px^X_{(\mathrm{A},1)} \oplus px^Y_{(\mathrm{A},1)} & \cdots & px^X_{(A,B)} \oplus px^Y_{(A,B)} \end{bmatrix} \end{aligned} \tag{6}$$

For each $px^X_{(row,col)} \oplus px^Y_{(row,col)}$, $row \in [1, A]$, and $col \in [1, B]$, the addition is executed as the definition above.

4. Proposed Scheme

4.1. Multi Secret Sharing Process

Suppose there are m secret gray images to be shared, the secret images are OS_1, OS_2, ... OS_n. All the secret images are 256 gray level and share the same size. There are n participators and n qualified subsets, The qualified part is P_{qual}, $P_{qual} = \{QS_1, QS_2, \ldots, QS_n\}$, where QS_i is the ith qualified subset $i \in [1, n]$, and the ith qualified subset QS_i have access to recover the ith secret image OS_i. $QS_i = \{i_1, i_2, \ldots, i_t\}$ means that the i_1th, i_2th, ... , i_tth participators can be recover the secret image OS_i. Moreover, the forbidden part is P_{forbid}, $P_{forbid} = \{FS_1, FS_2, \ldots, FS_{\mathrm{m}}\}$.

In the multi secret sharing process the universal shares and the personal shares of the same size as the secret images will be generated. The personal shares are owned by the individual owners and the universal shares are kept by the committee members with high privilege. In the recovery process, the personal owners and the committee members with universal shares will participate in the recovery. The process about the secret sharing process is described as Algorithm 1.

Algorithm 1: The secret sharing process of the proposed scheme.

Input: The secret images OS_1, OS_2, ... , OS_n; for the general access structure, the qualified part is P_{qual}, $P_{qual} = \{QS_1, QS_2, \ldots, QS_n\}$, and the forbidden part is P_{forbid}, $P_{forbid} = \{FS_1, FS_2, \ldots, FS_m\}$

Output: The personal shares PS_1, PS_2, ... , PS_n; the universal shares US_1, US_2, ... , US_n.

Step 1: Suppose the size of each secret image OS_i is $A \times B$, the pixel value in the rowth row and the colth column of OS_i is $pxO^i_{(row,col)}$, and $pxO^i_{(row,col)}$ is integer, $pxO^i_{(row,col)} \in [0, 255]$, $row \in [1, A]$, and $col \in [1, B]$. As each pixel can be expressed into an element with 8 bits in $GF(2^8)$,
suppose $pxO^i_{(row,col)} = \{bo_1, bo_2, bo_3, bo_4, bo_5, bo_6, bo_7, bo_8\}$, split the bits of each pixel into the 4 MSB bits and the 4 LSB bits, $pxOM^i_{(row,col)} = \{bo_1, bo_2, bo_3, bo_4\}$, and $pxOL^i_{(row,col)} = \{bo_5, bo_6, bo_7, bo_8\}$. Thus, the MSB part of the secret image OS_i can be regarded as the matrix $SM^i_{A\times B}$.

$$SM^i_{A\times B} = \begin{bmatrix} pxOM^i_{(1,1)} & \cdots & pxOM^i_{(1,B)} \\ \cdots & pxOM^i_{(row,col)} & \cdots \\ pxOM^i_{(A,1)} & \cdots & pxOM^i_{(A,B)} \end{bmatrix} \tag{7}$$

And the LSB part of the secret image OS_i can be regarded as the matrix $SL^i_{A\times B}$.

$$SL^i_{A\times B} = \begin{bmatrix} pxOL^i_{(1,1)} & \cdots & pxOL^i_{(1,\mathrm{B})} \\ \cdots & pxOL^i_{(row,col)} & \cdots \\ pxOL^i_{(\mathrm{A},1)} & \cdots & pxOL^i_{(A,B)} \end{bmatrix} \tag{8}$$

Step 2: Select n gray images $\{PO_1, PO_2, \ldots, PO_n\}$ from a mass of images randomly which are the same size and the same gray level with the secret images, and select another n gray images $\{UO_1, UO_2, \ldots, UO_n\}$ from a mass of images randomly which are the same size and the same gray level with the secret images, $\{UO_1, UO_2, \ldots, UO_n\}$ need to be different with $\{PO_1, PO_2, \ldots, PO_n\}$.

Step 3: Find out the essential id for each qualified subset QS_i in P_{qual} by Algorithm 2, $i \in [1, n]$, $QS_i = \{i_1, i_2, \ldots, i_t\}$, the essential id is specific element of the set QS_i, denote it as id_i.

Step 4: For the images $\{PO_1, PO_2, \ldots, PO_n\}$, for each image PO_i with the size $A \times B$, suppose the pixel value in the rowth row and the colth column of PO_i is $pxP^i_{(row,col)}$, and $pxP^i_{(row,col)}$ is the integer, $pxP^i_{(row,col)} \in [0, 255]$, $row \in [1, A]$, and $col \in [1, B]$. Each pixel can be expressed as $pxP^i_{(row,col)} = \{bp_1, bp_2, bp_3, bp_4, bp_5, bp_6, bp_7, bp_8\}$, separate 4 MSB bits and the 4 LSB bits of each pixel, $pxPM^i_{(row,col)} = \{bp_1, bp_2, bp_3, bp_4\}$, and $pxPL^i_{(row,col)} = \{bp_5, bp_6, bp_7, bp_8\}$. Thus, the matrix of the MSB is denoted as $PM^i_{A\times B}$.

$$PM^i_{A\times B} = \begin{bmatrix} pxPM^i_{(1,1)} & \cdots & pxPM^i_{(1,B)} \\ \cdots & pxPM^i_{(row,col)} & \cdots \\ pxPM^i_{(A,1)} & \cdots & pxPM^i_{(A,B)} \end{bmatrix} \tag{9}$$

And the matrix about LSB is denoted as $SL^i_{A\times B}$.

$$PL^i_{A\times B} = \begin{bmatrix} pxPL^i_{(1,1)} & \cdots & pxPL^i_{(1,B)} \\ \cdots & pxPL^i_{(row,col)} & \cdots \\ pxPL^i_{(A,1)} & \cdots & pxPL^i_{(A,B)} \end{bmatrix} \tag{10}$$

Step 5: For the images $\{UO_1, UO_2, \ldots, UO_n\}$, suppose the pixel value in the rowth row and the colth column of PO_i is $pxU^i_{(row,col)}$, and $pxU^i_{(row,col)}$ is integer, $pxU^i_{(row,col)} \in [0, 255]$, $row \in [1, A]$, and $col \in [1, B]$. Each pixel can be expressed as $pxU^i_{(row,col)} = \{bu_1, bu_2, bu_3, bu_4, bu_5, bu_6, bu_7, bu_8\}$, separate 4 MSB bits and the 4 LSB bits of each pixel, $pxUM^i_{(row,col)} = \{bu_1, bu_2, bu_3, bu_4\}$, and $pxUL^i_{(row,col)} = \{bu_5, bu_6, bu_7, bu_8\}$. The matrices are denoted as the $UM^i_{A\times B}$ for the MSB part and $UL^i_{A\times B}$ for the LSB part.

$$UM^i_{A\times B} = \begin{bmatrix} pxUM^i_{(1,1)} & \cdots & pxUM^i_{(1,B)} \\ \cdots & pxUM^i_{(row,col)} & \cdots \\ pxUM^i_{(A,1)} & \cdots & pxUM^i_{(A,B)} \end{bmatrix} \tag{11}$$

And the matrix of LSB $SL^i_{A\times B}$ is as below.

$$UL^i_{A\times B} = \begin{bmatrix} pxUL^i_{(1,1)} & \cdots & pxUL^i_{(1,B)} \\ \cdots & pxUL^i_{(row,col)} & \cdots \\ pxUL^i_{(A,1)} & \cdots & pxUL^i_{(A,B)} \end{bmatrix}$$

Step 6: For the secret image OS_i and the qualified subset is $QS_i = \{i_1, i_2, \ldots, i_t\}$, perform the following operation about the MSB part of the secret image OS_i:

$$TU^i_{A\times B} = \sum SM^i_{A\times B} + PM^{i_1}_{A\times B} + PM^{i_2}_{A\times B} + \ldots + PM^{i_t}_{A\times B} + UM^i_{A\times B} \tag{12}$$

The addition operation is defined as in Section 3.2. Suppose $TU^i_{A\times B}$ is shown as below,

$$TU^i_{A\times B} = \begin{bmatrix} pxTU^i_{(1,1)} & \cdots & pxTU^i_{(1,B)} \\ \cdots & pxTU^i_{(row,col)} & \cdots \\ pxTU^i_{(A,1)} & \cdots & pxTU^i_{(A,B)} \end{bmatrix} \tag{13}$$

Apply the Arnold transform [48] method to each matrix $TU^i_{A\times B}$ to realize the element scrambling, and the scrambled matrix is denoted as $ETU^i_{A\times B}$,

$$ETU^i_{A\times B} = \begin{bmatrix} pxETU^i_{(1,1)} & \cdots & pxETU^i_{(1,B)} \\ \cdots & pxETU^i_{(row,col)} & \cdots \\ pxETU^i_{(A,1)} & \cdots & pxETU^i_{(A,B)} \end{bmatrix} \tag{14}$$

Perform another operation for the LSB part of the secret image OS_i:

$$TP^{id_i}_{A\times B} = \sum SL^{i}_{A\times B} + PM^{i_{g_1}}_{A\times B} + \ldots + PM^{i_{g_{t-1}}}_{A\times B} + UM^{i}_{A\times B} \tag{15}$$

where $\left\{i_{g_1}, \ldots, i_{g_{t-1}}\right\} = GP_i$, $GP_i = \{GP_i | GP_i \cup id_i = QS_i, id_i \notin GP_i\}$, $QS_i = \{i_1, \ldots i_t\}$. Suppose $TP^{id_i}_{A\times B}$ is shown as below,

$$TP^{id_i}_{A\times B} = \begin{bmatrix} pxTP^{i}_{(1,1)} & \cdots & pxTP^{i}_{(1,\mathrm{B})} \\ \cdots & pxTP^{i}_{(row,col)} & \cdots \\ pxTP^{i}_{(A,1)} & \cdots & pxTP^{i}_{(A,B)} \end{bmatrix} \tag{16}$$

Apply the Arnold transform method to each matrix $TP^{id_i}_{A\times B}$ to realize the element scrambling, and the scrambled matrix is denoted as $ETP^{id_i}_{A\times B}$,

$$ETP^{id_i}_{A\times B} = \begin{bmatrix} pxETP^{i}_{(1,1)} & \cdots & pxETP^{i}_{(1,\mathrm{B})} \\ \cdots & pxETP^{i}_{(row,col)} & \cdots \\ pxETP^{i}_{(\mathrm{A},1)} & \cdots & pxETP^{i}_{(A,B)} \end{bmatrix} \tag{17}$$

Step 7: For the images $\{UO_1, UO_2, \ldots, UO_n\}$, replace the 4 LSBs of each pixel of UO_i with the element of $ETU^{i}_{A\times B}$ in the same position, which means join each element $pxUM^{i}_{(row,col)}$ of $UM^{i}_{A\times B}$ and $pxETU^{i}_{(row,col)}$ of $TU^{i}_{A\times B}$ together, and get the pixel matrix expression $US^{i}_{A\times B}$ of US_i,

$$US^{i}_{A\times B} = \begin{bmatrix} pxUM^{i}_{(1,1)} \cup pxETU^{i}_{(1,1)} & \cdots & pxUM^{i}_{(1,\mathrm{B})} \cup pxETU^{i}_{(1,\mathrm{B})} \\ \cdots & pxUM^{i}_{(row,col)} \cup pxETU^{i}_{(row,col)} & \cdots \\ pxUM^{i}_{(\mathrm{A},1)} \cup pxETU^{i}_{(\mathrm{A},1)} & \cdots & pxUM^{i}_{(A,B)} \cup pxETU^{i}_{(A,B)} \end{bmatrix} \tag{18}$$

Suppose $pxUM^{i}_{(row,col)} = \{bu_1, bu_2, bu_3, bu_4\}$, and $pxTU^{i}_{(row,col)} = \{btu_1, btu_2, btu_3, btu_4\}$, so

$$\begin{aligned} pxUM^{i}_{(row,col)} \cup pxTU^{i}_{(row,col)} &= \{bu_1, bu_2, bu_3, bu_4\} \cup \{btu_1, btu_2, btu_3, btu_4\} \\ &= \{bu_1, bu_2, bu_3, bu_4, btu_1, btu_2, btu_3, btu_4\} \end{aligned} \tag{19}$$

The renewed images are the universal shares $\{US_1, US_2, \ldots, US_n\}$.

Step 8: For the images $\{PO_1, PO_2, \ldots, PO_n\}$, replace the 4 LSBs of each pixel of PO_i with the element of $ETP^{i}_{A\times B}$ in the same position, which means join each element $pxPM^{i}_{(row,col)}$ of $PM^{i}_{A\times B}$ and $pxETP^{i}_{(row,col)}$ of $ETP^{i}_{A\times B}$ together, and get the pixel matrix expression $PS^{i}_{A\times B}$ of PS_i,

$$PS^{i}_{A\times B} = \begin{bmatrix} pxPM^{i}_{(1,1)} \cup pxETP^{i}_{(1,1)} & \cdots & pxPM^{i}_{(1,\mathrm{B})} \cup pxETP^{i}_{(1,\mathrm{B})} \\ \cdots & pxPM^{i}_{(row,col)} \cup pxETP^{i}_{(row,col)} & \cdots \\ pxPM^{i}_{(\mathrm{A},1)} \cup pxETP^{i}_{(\mathrm{A},1)} & \cdots & pxPM^{i}_{(A,B)} \cup pxETP^{i}_{(A,B)} \end{bmatrix} \tag{20}$$

The element joint operation is the similar as the last step, and the renewed images are the personal shares $\{PS_1, PS_2, \ldots, PS_n\}$.

Algorithm 2: The essential id selection process for the qualified subset of the general access.

Input: The general access structure, the qualified part is P_{qual}, $P_{qual} = \{QS_1, QS_2, \ldots, QS_n\}$, where QS_i is the ith qualified subset $i \in [1, n]$, $QS_i = \{i_1, i_2, \ldots, i_t\}$, $\{i_1, i_2, \ldots, i_t\} \in \{1, 2, \ldots, n\}$.
Output: The essential id $EID = \{id_1, id_2, \ldots, id_n\}$
Step 1: For each qualified subset QS_i, $i \in [1, n]$, $QS_i = \{i_1, i_2, \ldots, i_t\}$, denote the essential id of the set QS_i as id_i. Construct the vector of length n where all the elements are 0, set the i_1th, i_2th, ... , i_tth elements according to $\{i_1, i_2, \ldots, i_t\}$ to be 1, the vector is denoted as V_i. As such, the vector V_i is the logical presentation of the qualified subset QS_i.
Step 2: Regard the vector V_i as the ith row of the matrix QM, so the matrix QM is the presentation of the qualified access subsets.
Step 3: QM^1 is the start point of the searching, and $QM^1 = QM$.

For k = 1: n, calculate the hamming weights of each column and row of the matrix QM^k, the hamming wights of the columns are denoted as $\{hmc_1, hmc_2, \ldots, hmc_n\}$, and the hamming weights of the rows are denoted as $\{hmr_1, hmr_2, \ldots, hmr_n\}$, search for the smallest hamming weight of the column vector. There are different cases.

Case 1: If the smallest hamming weight of the column is 1 and unique, the non-zero element is the (sr, sc) element in the matrix QM, it shows that the essential id for the srth qualified subset QS_{sr} is sc.

Case 2: If the smallest hamming weight is not 1 and unique, compare the rows' hamming weights of the non-zero elements, select the element (sr, sc) which has the smallest hamming weight; if the rows' hamming weights are the same, select the element in which the row number is smaller, so the essential id for the srth qualified subset QS_{sr} is sc.

Case 3: If the smallest hamming weight is not 1 and not unique, compare all the rows' hamming weights of the non-zero elements in the different columns, select the element (sr, sc) which has the smallest hamming weight; if the rows' hamming weights are the same, select the element in which the row number is smallest, so the essential id for the srth qualified subset QS_{sr} is sc.

Step 4: Set all the elements of the srth row and the scth column to be zero, QM^k is renewed as QM^{k+1}.
Step 5: For the renewed matrix QM^{k+1}, execute the same operations as in Step 3 to fix the essential id for the other row, it is stopped when all the essential id for all the rows are fixed.
Step 6: The final essential id is denoted as $EID = \{id_1, id_2, \ldots, id_n\}$, which means the id_ith element is the essential element for the ith qualified subset QS_i.

Some observations and details for the steps are given below:

In step 1, as each pixel of the 256 gray secret image OS_i is expressed by 8 bits in the computer science, so the secret image OS_i can be regarded as the matrix $M^i_{A\times B}$ from the point of the mathematics, where the element is the bit expression of pixel value in $GF(2^8)$. If we divide the pixel into 4 MSBs and 4 LSBs part, the secret image OS_i can be regarded as the combination of matrix $SM^i_{A\times B}$ about the MSB part and $SL^i_{A\times B}$ about the LSB part, and all the elements of $SM^i_{A\times B}$ and $SL^i_{A\times B}$ is in $GF(2^4)$.

In step 2, the n gray images $\{PO_1, PO_2, \ldots, PO_n\}$ are the prepared images for the personal shares, and the n gray images $\{UO_1, UO_2, \ldots, UO_n\}$ are the prepared images for the universal shares; they are all selected randomly from a mass of images, so it is hard to predict which one is selected.

In step 3, the essential id is determined by Algorithm 2, the essential id $id_i = i_c$ for $QS_i = \{i_1, i_2, \ldots, i_t\}$ must be the id of the essential participator for the qualified subset QS_i, and the essential id for the different qualified subset is different. For the essential id id_i for QS_i and id_j for QS_j, $id_i \neq id_j$, if $j \neq i$.

In steps 4 and 5, the images $\{PO_1, PO_2, \ldots, PO_n\}$ and the images $\{UO_1, UO_2, \ldots, UO_n\}$ are divided into MSB and LSB part. $PM^i_{A\times B}$ for the MSB part and $PL^i_{A\times B}$ for the LSB part of PO_i, $UM^i_{A\times B}$ for the MSB part and $UL^i_{A\times B}$ for the LSB part of UO_i are generated from the point of matrix.

In step 6, in Equation (12), there are three parts taking part in the addition computation to generate $TU^i_{A\times B}$, the first part is the MSB part of the secret image $SM^i_{A\times B}$, the second part is $PM^{i_j}_{A\times B}$ $(j \in \{1, \ldots, t\})$ which are the MSB part of the images $\{PO_{i1}, POi_2, \ldots, PO_{it}\}$ according to the qualified subset QS_j, the third part is $UM^i_{A\times B}$ which is the MSB part of UO_i. A similar operation is executed as shown in Equation (15) to get $TP^{id_i}_{A\times B}$,where the set GP_i is in fact the subset of QS_i removing the element

id_i. The Arnold transform method is applied to $TU^i_{A\times B}$ and $TP^{id_i}_{A\times B}$ to scramble the pixels, which is important for enhancing the security. If $A = B$, the image is square, we can use the transform in [48] directly, if $A \neq B$, the image is not square, it needs to be extended to be square by supplying some zero pixel. Then, the Arnold transform method is carried out.

In step 7, the 4 LSBs of the each pixel of UO_i are replaced by the elements of $ETU^i_{A\times B}$, and the renewed image is the final universal share US_i. The id_ith personal share PS_{idi} can be obtained as shown in Equation (15) by replacing the LSBs of PS_{idi} bythe elements of $ETP^{id_i}_{A\times B}$.

Then the generated personal share PS_i is distributed to the owner OW_i, and the universal shares US_i are kept by the committee members having high privilege.

The example 1 is an example of the secret sharing process and the size of the image is small for the convenience to show the sharing process using the matrices.

Example 1.

Suppose there are 4 participants, the qualified part $P_{qual} = \{QS_1, QS_2, QS_3, QS_4\}$, and $QS_1 = \{1, 2, 3\}$, $QS_2 = \{1, 4\}$, $QS_3 = \{2, 4\}$, $QS_4 = \{3, 4\}$. The secret images with 256 gray level are OS_1, OS_2, OS_3, OS_4, and the size of the secret image is 2×2. As such, the participants in QS_i have access to recover the secret image OS_i.

The secret sharing process is described below:

- For the secret images, suppose the matrices of the pixel value is shown as below:

$$\begin{pmatrix} 154 & 35 \\ 69 & 247 \end{pmatrix}\begin{pmatrix} 227 & 141 \\ 165 & 46 \end{pmatrix}\begin{pmatrix} 142 & 64 \\ 237 & 37 \end{pmatrix}\begin{pmatrix} 118 & 148 \\ 49 & 97 \end{pmatrix}$$

- For each QS_i, there is one corresponding essential id id_i and universal share, so we take the generation of the personal share PS_{id_1} and the universal US_1 for example. First, turn the pixel value of the first secret image OS_1 into 8 bits, to get:

$$OM^1_{2\times 2} = \begin{pmatrix} 10011010 & 00100011 \\ 01000101 & 11110111 \end{pmatrix} \tag{21}$$

- Divide the MSB part and the LSB part of $OM^1_{2\times 2}$, So $SM^i_{A\times B}$ about the MSB parts and $SL^i_{A\times B}$ about LSB is shown below:

$$SM^1_{2\times 2} = \begin{pmatrix} 1001 & 0010 \\ 0100 & 1111 \end{pmatrix} \tag{22}$$

$$SL^1_{2\times 2} = \begin{pmatrix} 1010 & 0011 \\ 0101 & 0111 \end{pmatrix} \tag{23}$$

- Select 4 gray images randomly $\{PO_1, PO_2, PO_3, PO_4\}$ with the same size as the secret image from a set of thousands of images, and select another 4 gray images randomly $\{UO_1, UO_2, UO_3, UO_4\}$ with the same size as the secret image.
- Find out the essential id for the qualified subset based on Algorithm 2, the essential id for the qualified subsets is $\{id_1, id_2, id_3, id_4\} = \{2, 1, 4, 3\}$.
- For the image $\{PO_1, PO_2, PO_3, PO_4\}$, suppose $PM^i_{2\times 2}$ is the matrix for the MSB part of PO_i. As such, the matrices of the MSB parts of the images are as below:

$$PM^1_{2\times 2} = \begin{pmatrix} 0101 & 1100 \\ 0110 & 1001 \end{pmatrix} \tag{24}$$

$$PM^2_{2\times 2} = \begin{pmatrix} 1110 & 1000 \\ 1010 & 0010 \end{pmatrix} \tag{25}$$

$$PM^3_{2\times2} = \begin{pmatrix} 0100 & 0110 \\ 0111 & 1100 \end{pmatrix} \tag{26}$$

$$PM^4_{2\times2} = \begin{pmatrix} 1100 & 0110 \\ 0101 & 0111 \end{pmatrix} \tag{27}$$

- For the image UO_1, the matrix $UM^1_{2\times2}$ of the MSB parts is as below:

$$UM^1_{2\times2} = \begin{pmatrix} 0111 & 1000 \\ 1001 & 0101 \end{pmatrix} \tag{28}$$

- Thus, according to Equation (15) we can get $TU^1_{2\times2}$:

$$\begin{aligned} TU^1_{2\times2} &= \sum SM^1_{2\times2} + PM^1_{2\times2} + PM^2_{2\times2} + PM^3_{2\times2} + UM^1_{2\times2} \\ &= \begin{pmatrix} 1001 & 0010 \\ 0100 & 1111 \end{pmatrix} + \begin{pmatrix} 0101 & 1100 \\ 0110 & 1001 \end{pmatrix} + \begin{pmatrix} 1110 & 1000 \\ 1010 & 0010 \end{pmatrix} + \begin{pmatrix} 0100 & 0110 \\ 0111 & 1100 \end{pmatrix} + \begin{pmatrix} 0111 & 1000 \\ 1001 & 0101 \end{pmatrix} \\ &= \begin{pmatrix} 0001 & 1000 \\ 0110 & 1101 \end{pmatrix} \end{aligned} \tag{29}$$

- Apply the Arnold transform method to each matrix $TU^1_{2\times2}$ to realize the element scrambling, and the scrambled matrix is denoted as $ETU^1_{2\times2}$,

$$ETU^1_{2\times2} = \begin{pmatrix} 1101 & 0001 \\ 1000 & 0110 \end{pmatrix} \tag{30}$$

- Similarly, we can get:

$$TP^{id_1}_{2\times2} = TP^2_{2\times2} = \sum SL^1_{2\times2} + PM^1_{2\times2} + PM^3_{2\times2} + UM^1_{2\times2} = \begin{pmatrix} 0101 & 1110 \\ 1100 & 0110 \end{pmatrix} \tag{31}$$

- Apply the Arnold transform method to each matrix $TP^2_{2\times2}$ to realize the element scrambling, and the scrambled matrix is denoted as $ETP^2_{2\times2}$,

$$ETP^2_{2\times2} = \begin{pmatrix} 0110 & 0101 \\ 1110 & 1100 \end{pmatrix} \tag{32}$$

- So, for the image UO_1, replace the 4 LSBs of each pixel with the element in $ETU^1_{2\times2}$ to obtain the matrix of the universal share US_1 as below:

$$Ug^1_{2\times2} = \begin{pmatrix} 01111101 & 10000001 \\ 10011000 & 01010110 \end{pmatrix} \tag{33}$$

- The pixel presentation matrix is:

$$UG^1_{2\times2} = \begin{pmatrix} 125 & 129 \\ 152 & 86 \end{pmatrix} \tag{34}$$

- For the images $\{PO_1, PO_2, PO_3, PO_4\}$, select the essential id id_1 for the qualified subset QS_1 (the algorithm about the essential id for the qualified subset is shown in Algorithm 2), as $id_1 = 2$, so for the image PO_2, replace the 4 LSBs with $ETP_{2\times2}^{id_1}$, $id_1 = 2$ to get one personal share PS_2.

$$PS_{2\times2}^{2} = \begin{pmatrix} 11100110 & 10000101 \\ 10101110 & 00101100 \end{pmatrix} \tag{35}$$

$$PG_{2\times2}^{2} = \begin{pmatrix} 230 & 133 \\ 174 & 44 \end{pmatrix} \tag{36}$$

- The other universal shares UO_2, UO_3, UO_4 and the personal shares PO_1, PO_3, PO_4 can be obtained in the same way.

In the following, the definition of the essential id for the qualified subset and the algorithm for the determination of the essential id is given out.

As described in the beginning of Section 4.1, the number of the minimal qualified subset is the same as the number of the participants, so each participant is in one minimal qualified subset. The essential id id_i for the subset QS_i is defined as the representative element id in QS_i, for each qualified subset, there is one essential id and it is different from the essential id of other subsets; that is, the id_i for the subset QS_i is not equal to the id_j for the subset QS_j, $id_i \neq id_j$ if $i \neq j$. Thus, the id of each participator can be assigned as the essential id for one minimal qualified subset, and each essential id can be assigned to one secret image according to one qualified subset. The algorithm about the selection of the essential id is described below.

In step 1, the qualified subset $QS_i = \{i_1, i_2, \ldots, i_t\}$ means that the i_1th, i_2th, $\ldots$, i_tth participators have the ability to recovery the ith secret image, so the vector V_i is in fact the logical express of the qualified subset.

In step 2, the matrix QM is the binary matrix presentation of the general access structure, and the ith row is according to the ith qualified subset QS_i, and the jth column is corresponding to the jth participator, so the (i, j) element of QM is not zero shows that the jth participator takes part in the recovery the ith secret image.

In step 3, the essential id for each qualified subset is determined according to the comparison of the column hamming weights and the row hamming weights, and the matrix is renewed continuously in the iteration. After step 5, we can get the final essential id for all the qualified subsets.

The following is the example of the determination process of the essential id.

Example 2.

Suppose there are 4 participants, the qualified part $P_{qual} = \{QS_1, QS_2, QS_3, QS_4\}$, and $QS_1 = \{1, 2, 3\}$, $QS_2 = \{1, 4\}$, $QS_3 = \{2, 4\}$, $QS_4 = \{3, 4\}$.

- The vectors of the QS_i are shown as below:

$$\begin{aligned} V_1 &= [1, 1, 1, 0] \\ V_2 &= [1, 0, 0, 1] \\ V_3 &= [0, 1, 0, 1] \\ V_4 &= [0, 0, 1, 1] \end{aligned} \tag{37}$$

- As such, the matrix QM of the qualified access is shown as below:

$$QM = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \tag{38}$$

- Let $QM^1 = QM$ as the start point, calculate the hamming weight of each column, $\{hmc_1, hmc_2, hmc_3, hmc_4\} = \{2, 2, 2, 3\}$, and the hamming weight of each row is $\{hmr_1, hmr_2, hmr_3, hmr_4\} = \{3, 2, 2, 2\}$. As 2 is the smallest column hamming weight and not unique, compare all the {1, 2, 3} rows' hamming weights, $\{hmr_1, hmr_2, hmr_3, hmr_4\} = \{3, 2, 2, 2\}$, since the element (2, 1) element has the row number that is smallest in the rows with a smaller row hamming weight of 2, the essential id for the qualified subset QS_2 is 1;
- Then all the elements in the 2th row and the 1th column are set to be zero, the renewed matrix QM^2 is as below:

$$QM^2 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \tag{39}$$

- Compare the hamming weight of the non-zero columns in QM^2, $\{hmc_2, hmc_3, hmc_4\} = \{2, 2, 2\}$, as all the columns hamming weight is the same, so compare the row hamming weight, $\{hmr_1, hmr_3, hmr_4\} = \{2, 2, 2\}$, so select the (1, 2) element whose row number is smallest in the rows with hamming weight 2, which means the essential id for the qualified subset QS_1 is 2;
- Then, the 1th row and the 2rd column is set to be zero, the renewed matrix QM^3 is as blow:

$$QM^3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \tag{40}$$

- The hamming weight of the non-zero columns $\{hmc_3, hmc_4\} = \{1, 2\}$, the smallest rows' hamming weight is 1 and unique, so select the element (4, 3), the essential id for the qualified subset QS_4 is 3;
- Then the 4th row and the 3th column is set to be zero, the renewed matrix QM^4 is as blow:

$$QM^4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{41}$$

- Thus, it is easy to confirm the essential id for the qualified subset QS_3 is 4;
- At last, we can obtain the essential id $EID = \{id_1, id_2, \ldots, id_n\} = \{2, 1, 4, 3\}$.

4.2. Secret Recovery Process

In the secret sharing process, the personal shares $\{PS_1, PS_2, \ldots, PS_n\}$ are distributed to the personal owners and the universal shares $\{US_1, US_2, \ldots, US_n\}$ are kept by the privileged committee members. As per the definition of the general access structure, the qualified owners can recover the ith secret image use the personal shares $\{PS_{i1}, PSi_2, \ldots, PS_{it}\}$ according to the qualified subset QS_i, $i \in [1, n]$, $QS_i = \{i_1, i_2, \ldots, i_t\}$. The recovery process is shown in Algorithm 3.

Algorithm 3: The secret recovery process of the proposed scheme.

Input: The personal shares $PS_1, PS_2, \ldots, PS_n$; the universal shares $US_1, US_2, \ldots, US_{n.}$; the general access structure, the qualified part is P_{qual}, and the forbidden part is P_{forbid}.
Output: The secret images $RS_1, RS_2, \ldots, RS_n$
Step 1: Take the recovery of the ith secret image as the example. Retrieve the universal image UO_i from the committee after verification, or else the committee members can participate in the recovery taking the universal share $UO_{i.}$ Extract the 4 LSBs of the each pixel to get the matrix $ETU^i_{A\times B}$ over $GF(2^4)$, and 4 MSBs of the pixels of UO_i form the matrix $UM^i_{A\times B}$;
Step 2: Collect the qualified personal shares $\{PS_{i1}, PSi_2, \ldots, PS_{it}\}$ based on the qualified subset QS_i, $i \in [1, n]$, $QS_i = \{i_1, i_2, \ldots, i_t\}$. For each qualified personal share, extract the 4 MSBs of each pixel of the share, as in Algorithm 1. Obtain the matrix $PM^{i_j}_{A\times B}$ over $GF(2^4)$, $j \in [1, t]$, as $QS_i = \{i_1, i_2, \ldots, i_t\}$, so we can get the matrices $\left\{PM^{i_1}_{A\times B}, PM^{i_2}_{A\times B}, \ldots, PM^{i_t}_{A\times B}\right\}$;
Step 3: Apply the Arnold inverse transform on $ETU^i_{A\times B}$ to get $TU^i_{A\times B}$, and perform the following operation:

$$SM^i_{A\times B} = \sum TU^i_{A\times B} + PM^{i_1}_{A\times B} + PM^{i_2}_{A\times B} + \ldots + PM^{i_t}_{A\times B} + UM^i_{A\times B} \tag{42}$$

$SM^i_{A\times B}$ is shown as below:

$$SM^i_{A\times B} = \begin{bmatrix} pxSM^i_{(1,1)} & \cdots & pxSM^i_{(1,B)} \\ \cdots & pxSM^i_{(row,col)} & \cdots \\ pxSM^i_{(A,1)} & \cdots & pxSM^i_{(A,B)} \end{bmatrix} \tag{43}$$

where $pxSM^i_{(row,col)} = \{bm_1, bm_2, bm_3, bm_4\}$.
Step 4: Calculate the essential id id_i for the qualified set QS_i using Algorithm 2, and extract the 4 LSBs of each pixel in the $id_i th$ personal share to get the matrix $ETP^{id_i}_{A\times B}$, and apply the Arnold inverse transform on $ETP^{id_i}_{A\times B}$ to get $TP^{id_i}_{A\times B}$;
Step 5: From the construction of $TP^{id_i}_{A\times B}$, perform the following operation to get $SL^i_{A\times B}$:

$$SL^i_{A\times B} = \sum TP^{id_i}_{A\times B} + PM^{i_{g_1}}_{A\times B} + \ldots + PM^{i_{g_{t-1}}}_{A\times B} + UM^i_{A\times B} \tag{44}$$

where $\left\{i_{g_1}, \ldots, i_{g_{t-1}}\right\} = GP$, $GP = \{GP | GP \cup id_i = QS_i, id_i \notin GP\}$, $QS_i = \{i_1, \ldots i_t\}$ and $SL^i_{A\times B}$ is shown as below:

$$SL^i_{A\times B} = \begin{bmatrix} pxSL^i_{(1,1)} & \cdots & pxSL^i_{(1,B)} \\ \cdots & pxSL^i_{(row,col)} & \cdots \\ pxSL^i_{(A,1)} & \cdots & pxSL^i_{(A,B)} \end{bmatrix} \tag{45}$$

where $pxSL^i_{(row,col)} = \{bl_1, bl_2, bl_3, bl_4\}$.
Step 6: For each element in matrix $SM^i_{A\times B}$ and $SL^i_{A\times B}$, join the element of the matrix $SM^i_{A\times B}$ and the element of the matrix $SL^i_{A\times B}$ in the same position to form a new matrix $RM^i_{A\times B}$:

$$RM^i_{A\times B} = \begin{bmatrix} pxSM^i_{(1,1)} \cup pxSL^i_{(1,1)} & \cdots & pxSM^i_{(1,B)} \cup pxSL^i_{(1,B)} \\ \cdots & pxSM^i_{(row,col)} \cup pxSL^i_{(row,col)} & \cdots \\ pxSM^i_{(A,1)} \cup pxSL^i_{(A,1)} & \cdots & pxSM^i_{(A,B)} \cup pxSL^i_{(A,B)} \end{bmatrix} \tag{46}$$

where $pxSM^i_{(row,col)} \cup pxSL^i_{(row,col)} = \{bm_1, bm_2, bm_3, bm_4, bl_1, bl_2, bl_3, bl_4\}$.
Step 7: Transform each element of the matrix $RM^i_{A\times B}$ into the decimal number, which is the pixel value of the ith recovered secret image RSi which is 256 gray level. For example, if the element of $RM^i_{A\times B}$ is $\{bm_1, bm_2, bm_3, bm_4, bl_1, bl_2, bl_3, bl_4\}$, the pixel value is in fact $\left\{2^7 \cdot bm_1 + 2^6 \cdot bm_2 + 2^5 \cdot bm_3 + 2^4 \cdot bm_4 + 2^3 \cdot bl_1 + 2^2 \cdot bl_2 + 2^1 \cdot bl_3 + 2^0 \cdot bl_4\right\}$. Finally, we can get the recovered ith secret image, and the recovery of other secret images can be realized in the same manner.

In step 1 and 2, we collect the qualified personal shares responding to QS_i, and the universal share is also collected. The matrices of the shares are divided into the MSB part and the LSB part, and the recovery can be realized by Equations (42) and (44). The example is shown as below.

Example 3.

As shown in example 1, in the secret sharing process, the personal shares $\{PS_1, PS_2, PS_3, PS_4\}$ are distributed to the personal owners and the universal shares $\{US_1, US_2, US_3, US_4\}$ are kept by the committee members with high privilege. The qualified access is $P_{qual} = \{QS_1, QS_2, QS_3, QS_4\}$, and $QS_1 = \{1, 2, 3\}$, $QS_2 = \{1, 4\}$, $QS_3 = \{2, 4\}$, $QS_4 = \{3, 4\}$, which is the same as the sharing process. The secret image recovery process is shown as below, take the recovery of the first secret image for example.

Get the according universal share UO_1, change the pixel expression value into the bits expression.

$$UG^1_{2\times2} = \begin{pmatrix} 125 & 129 \\ 152 & 86 \end{pmatrix} \tag{47}$$

$$Ug^1_{2\times2} = \begin{pmatrix} 01111101 & 10000001 \\ 10011000 & 01010110 \end{pmatrix} \tag{48}$$

Split each pixel into 2 parts, so the matrix about MSB and LSB is as shown below:

$$UM^1_{2\times2} = \begin{pmatrix} 0111 & 1000 \\ 1001 & 0101 \end{pmatrix} \tag{49}$$

$$ETU^1_{2\times2} = \begin{pmatrix} 1101 & 0001 \\ 1000 & 0110 \end{pmatrix} \tag{50}$$

Apply the Arnold inverse transform on $ETU^i_{A\times B}$ to get $TU^i_{A\times B}$, and $TU^1_{A\times B} = \begin{pmatrix} 0001 & 1000 \\ 0110 & 1101 \end{pmatrix}$.

As the qualified subset $QS_1 = \{1, 2, 3\}$, collect the 1st, 2nd, and 3rd personal shares, and obtain the matrices of MSBs:

$$PM^1_{2\times2} = \begin{pmatrix} 0101 & 1100 \\ 0110 & 1001 \end{pmatrix} \tag{51}$$

$$PM^2_{2\times2} = \begin{pmatrix} 1110 & 1000 \\ 1010 & 0010 \end{pmatrix} \tag{52}$$

$$PM^3_{2\times2} = \begin{pmatrix} 0100 & 0110 \\ 0111 & 1100 \end{pmatrix} \tag{53}$$

Thus, we can get $SM^1_{2\times2}$ based on the Equation (42).

$$\begin{aligned} SM^1_{2\times2} &= \sum TU^1_{2\times2} + PM^1_{2\times2} + PM^2_{2\times2} + PM^3_{2\times2} + UM^1_{2\times2} \\ &= \begin{pmatrix} 0001 & 1000 \\ 0110 & 1101 \end{pmatrix} + \begin{pmatrix} 0101 & 1100 \\ 0110 & 1001 \end{pmatrix} + \begin{pmatrix} 1110 & 1000 \\ 1010 & 0010 \end{pmatrix} + \begin{pmatrix} 0100 & 0110 \\ 0111 & 1100 \end{pmatrix} + \begin{pmatrix} 0111 & 1000 \\ 1001 & 0101 \end{pmatrix} \\ &= \begin{pmatrix} 1001 & 0010 \\ 0100 & 1111 \end{pmatrix} \end{aligned} \tag{54}$$

Additionally, as the essential id $id_1 = 2$, extract the 4 LSBs of the 2nd personal share to get $ETP^2_{2\times2} = \begin{pmatrix} 0110 & 0101 \\ 1110 & 1100 \end{pmatrix}$. Apply the Arnold inverse transform on $ETP^2_{2\times2}$ to get $TP^2_{2\times2}$, and $TP^2_{2\times2} = \begin{pmatrix} 0101 & 1110 \\ 1100 & 0110 \end{pmatrix}$, and we can get $SL^1_{2\times2}$ based on Equation (44).

$$SL^1_{2\times2} = \sum TP^2_{2\times2} + PM^1_{2\times2} + PM^3_{2\times2} + UM^1_{2\times2} = \begin{pmatrix} 1010 & 0011 \\ 0101 & 0111 \end{pmatrix} \tag{55}$$

Then, join the element of the matrix $SM^1_{2\times2}$ and the element of the matrix $SL^1_{2\times2}$ in the same position to get the bits expression of the first secret RS_1,

$$OM^1_{2\times2} = \begin{pmatrix} 10011010 & 00100011 \\ 01000101 & 11110111 \end{pmatrix} \tag{56}$$

Finally, transform the element of $OM^1_{2\times2}$ into a decimal number to obtain the pixel value matrix of the first secret image:

$$RS_1 = \begin{pmatrix} 154 & 35 \\ 69 & 247 \end{pmatrix} \tag{57}$$

The other secret images can be recovered in the same way according to their qualified subsets.

5. Proof and Analysis

5.1. Correctness Proof

Theorem 1. *The secret images can be successfully recovered by the personal shares in the qualified subset inP_{qual} and the universal shares.*

In other words, we need to prove that each secret image OS_i can be recovered by the personal shares according to the qualified subset QS_i, $QS_i = \{i_1, i_2, \ldots, i_t\}$ and the universal share US_i, $i \in [1, n]$.

As shown in the secret sharing process, all the images are turned into the matrix form after transforming the pixel between 0 to 255 into the element with 8 bits in $GF(2^8)$ from the point of mathematics. The matrix $OM^i_{A\times B}$ about the secret image OS_i is divided into two matrix $SM^i_{A\times B}$ about the MSB part and $SL^i_{A\times B}$ about the LSB part. Thus, in the recovery process we need to recover the two matrices.

Each of the prepared random selected images PO_i corresponding to $QS_i = \{i_1, i_2, \ldots, i_t\}$ are also divided into two parts in the same way as the secret image. The MSB matrices are denoted as the $PM^{i_j}_{A\times B}$, and the LSB matrices are $PL^{i_j}_{A\times B}$, $j \in [1, n]$. The matrix $PM^{i_j}_{A\times B}$ of the MSB part will participate in the sharing, and the LSB space is reserved.

Another prepared image for the universal share UO_i is also divided into $UM^i_{A\times B}$ and $UL^i_{A\times B}$ respectively.

The matrices' computation for the secret image and the prepared images for the personal shares and the universal share are shown as below in Equation (12),

$$TU^i_{A\times B} = \sum SM^i_{A\times B} + PM^{i_1}_{A\times B} + PM^{i_2}_{A\times B} + \ldots + PM^{i_t}_{A\times B} + UM^i_{A\times B}$$

Then the Arnold transform is applied on $TU^i_{A\times B}$ and the scrambling matrix $ETU^i_{A\times B}$ is generated. Based on the basic idea that the LSBs have the little effect on the image quality, the LSBs of the UO_i can be replaced by $ETU^i_{A\times B}$ and will not effect on the meaning of the image, so we can get the universal share US_i.

Another operation for the LSB part of the secret image is executed as below in Equation (15):

$$TP_{A\times B}^{id_i} = \sum SL_{A\times B}^{i} + PM_{A\times B}^{i_{g_1}} + \ldots + PM_{A\times B}^{i_{g_{t-1}}} + UM_{A\times B}^{i}$$

where $\left\{i_{g_1}, \ldots, i_{g_{t-1}}\right\} = GP$, $GP = \{GP | GP \cup id_i = QS_i, id_i \notin GP\}$, $QS_i = \{i_1, \ldots i_t\}$.

And the matrix $TP_{A\times B}^{id_i}$ is scrambled into $ETP_{A\times B}^{id_i}$ by the Arnold transform.

From the definition of the essential id, each QS_i has an only essential id, and the id_i for the QS_i is different from the others; if $i \neq j$, $id_i \neq id_j$, then each QS_i has a different essential id_i, so for each qualified subset, the 4-bits elements of $TP_{A\times B}^{id_i}$ can be used to replace the LSBs of the id_ith image in $\{PO_1, PO_2, \ldots, PO_n\}$, so we can get the final id_ith personal share PS_{id_i}.

In the recovery process, the owners of personal shares of $QS_i = \{i_1, i_2, \ldots, i_t\}$ participate in the recovery, they offer the personal shares $PS_{i1}, PS_{i2}, \ldots, PS_{it}$, and the corresponding universal share US_i is obtained from the universal panel, so we can get the matrices $PM_{A\times B}^{i_1}, PM_{A\times B}^{i_2}, \ldots, PM_{A\times B}^{i_t}$ from PS_{i1}, $PS_{i2}, \ldots, PS_{it}$, and $TU_{A\times B}^{i}, UM_{A\times B}^{i}$ can be obtained from the US_i.

As shown in Equation (12), the share generation can be expressed as follows:

$$0 = \sum TU_{A\times B}^{i} + SM_{A\times B}^{i} + PM_{A\times B}^{i_1} + PM_{A\times B}^{i_2} + \ldots + PM_{A\times B}^{i_t} + UM_{A\times B}^{i} \quad (58)$$

Move $SM_{A\times B}^{i}$ to another side of the equation to get the expression of $SM_{A\times B}^{i}$ as shown below:

$$SM_{A\times B}^{i} = \sum TU_{A\times B}^{i} + PM_{A\times B}^{i_1} + PM_{A\times B}^{i_2} + \ldots + PM_{A\times B}^{i_t} + UM_{A\times B}^{i} \quad (59)$$

In fact, Equation (59) used in the recovery, by which we can retrieve the MSB part of the secret image of OS_i.

As in Equation (15), the share generation can be expressed as below:

$$0 = \sum TP_{A\times B}^{id_i} + SL_{A\times B}^{i} + PM_{A\times B}^{i_{g_1}} + \ldots + PM_{A\times B}^{i_{g_{t-1}}} + UM_{A\times B}^{i} \quad (60)$$

Move $SL_{A\times B}^{i}$ to another side of the equation to get the expression of $SL_{A\times B}^{i}$ as shown below:

$$SL_{A\times B}^{i} = \sum TP_{A\times B}^{id_i} + PM_{A\times B}^{i_{g_1}} + \ldots + PM_{A\times B}^{i_{g_{t-1}}} + UM_{A\times B}^{i} \quad (61)$$

where $\left\{i_{g_1}, \ldots, i_{g_{t-1}}\right\} = GP$, $GP = \{GP | GP \cup id_i = QS_i, id_i \notin GP\}$, $QS_i = \{i_1, \ldots i_t\}$.

In fact, Equation (44) is used in the recovery, by which we can retrieve the LSB part of the secret image of OS_i.

Combining the $SM_{A\times B}^{i}$ and $SL_{A\times B}^{i}$ together, we can get the exact pixel value of the secret image, and the secret image RS_i is recovered, which is the same as the original secret image OS_i.

5.2. Security Analysis

In this section, we will discuss the security of the proposed multi secret sharing scheme through theoretical analyses.

Theorem 2. *The personal are meaningful and the security of the share are reasonably good.*

Regarding the personal shares, they are generated by the prepared meaningful images $\{PO_1, PO_2, \ldots, PO_n\}$ which are selected randomly from lots of images. Although all the shares are not meaningless shares in which the pixels values are random, they still have strong randomness, so it is hard to know which images will be selected from a set of images.

From the point of the visual assessment, the replacement of LSBs has little influence on the visual quality of the image; the change is so minuscule it can barely be detected by the human visual system. An example of the original image and the modified image of 4 LSBs is shown in Figure 1.

(**a**) (**b**)

Figure 1. The figures of the original image and the modified image: (**a**) the original gray image with 256 gray level; (**b**) the modified image with the replacement of the 4 LSBs.

From the comparison in Figure 1, we can see that the modified image is still a meaningful image that looks like a nature image and it is almost the same as the original image.

The high security of the personal shares can be ensured by two aspects.

Firstly, the personal shares with 4 LSBs replaced by the elements in the matrix $ETP^i_{A\times B}$ are meaningful as the nature images, so they can avoid attracting any adversary's attention more so than the random meaningless shares.

Secondly, from the point of the computation analysis, the MSBs of the personal share are the original bits of the original image, and the LSBs are $ETP^i_{A\times B}$ which is the random permutation result of $TP^i_{A\times B}$, $TP^{id_i}_{A\times B} = \sum SL^i_{A\times B} + PM^{i_{g_1}}_{A\times B} + \ldots + PM^{i_{g_{t-1}}}_{A\times B} + UM^i_{A\times B}$; if one participant intends to analyze the single personal share to get some information about $SL^i_{A\times B}$, from the generation of $TP^i_{A\times B}$, he needs to get the MSB information $\{PM^{i_2}_{A\times B}, \ldots, PM^{i_t}_{A\times B}\}$ about the other qualified personal shares and the MSB information $\{UM^i_{A\times B}\}$ about the according universal share. Without the help of this information, only use $\{TP^{id_i}_{A\times B}, PM^{id_i}_{A\times B}\}$, the single personal share cannot retrieve the secret information, so it is not possible to analyze the content or the bits of the single personal share to get any information about the secret image. Furthermore, the result of Equation (15) is permuted and embedded; the embedded bits are scrambled, and it is hard to get the original bits because it is not known which transform is used.

Theorem 3. *The universal shares are meaningful, and the security of the shares are reasonably good.*

For the universal shares, they still have strong randomness because the prepared images $\{UO_1, UO_2, \ldots, UO_n\}$ are selected randomly from lots of images. Also, the universal share UO_i is still meaningful image as a nature image and is almost the same as the original image US_i, $i \in [1, n]$.

The high security of the universal shares can be ensured by three point.

First, the universal shares are kept by the committee members with high privilege, who are trusted. The universal share for each qualified subset only can be used after the authentication, or in the recovery where the committee members take the universal share and participate in the recovery.

Secondly, the universal share looks like the nature image, which can avoid attracting the adversary's attention more so than the random meaningless shares.

Thirdly, from the point of the computation analysis, the LSBs of the pixels are $ETU^i_{A\times B}$ which is the random permutation result of $TU^i_{A\times B}$. They are scrambled and it is hard

to get the original bits because the transform is unknown. From the generation of $TU^i_{A\times B}$, $TU^i_{A\times B} = \sum SM^i_{A\times B} + PM^{i_1}_{A\times B} + PM^{i_2}_{A\times B} + \ldots + PM^{i_t}_{A\times B} + UM^i_{A\times B}$, the MSB part $SM^i_{A\times B}$ the MSB information $\{PM^{i_1}_{A\times B}, PM^{i_2}_{A\times B}, \ldots, PM^{i_t}_{A\times B}\}$ about the other qualified personal shares and the MSB information $\{UM^i_{A\times B}\}$ about the according universal share take part in the generation. If one committee member intends to analyze the single universal share to get some information about $SM^i_{A\times B}$, from the generation of $TU^i_{A\times B}$, he can get the MSB information $\{UM^i_{A\times B}\}$ about the universal share, he still needs to get the MSB information $\{PM^{i_1}_{A\times B}, PM^{i_2}_{A\times B}, \ldots, PM^{i_t}_{A\times B}\}$ about the qualified personal shares. Without the information of personal share, he can only use $\{TU^i_{A\times B}, UM^i_{A\times B}\}$ about the single universal share and cannot retrieve the secret information. It is established that even the qualified subset is very simple. Since there must be an essential id id_i for the qualified subset QS_i, there is at least one matrix $PM^{id_i}_{A\times B}$ and the $UM^i_{A\times B}$ participating in the generation of $TU^i_{A\times B}$, so $TU^i_{A\times B} \neq SM^i_{A\times B}$. After applying the Arnold transform to $TU^i_{A\times B}$, the embedded bits are the scrambling bits, so the MSB bits of the secret images will not be revealed directly and are hard to be calculated.

It is also not possible to use different universal shares to reveal some information about the secret images, because each $TU^i_{A\times B}$ is scrambling by the Arnold transform and XOR. Two or more universal shares only can get some useless random permutation result on $ETU^i_{A\times B}$.

Theorem 4. *The shares of the part of each subset QS_i cannot reveal the information about the secret image.*

Suppose the qualified subset is $QS_i = \{i_1, i_2, \ldots, i_t\}$, and the subset of QS_i is $\{i_1, i_2, \ldots, i_w\}$, where $w < t$, $\{i_1, i_2, \ldots, i_w\} \subset \{i_1, i_2, \ldots, i_t\}$. From the definition of the minimum qualified subset, $\forall Q' \subset Q$, and $Q \in P_{qual}$, $Q' \notin P_{qual}$. As the P_{qual} is the minimum qualified subset, for any part of the subset of the qualified subset QS_i, it is not possible to be a qualified access.

From the generation equation of the personal shares for the subset $QS_i = \{i_1, i_2, \ldots, i_t\}$, $TU^i_{A\times B} = \sum SM^i_{A\times B} + PM^{i_1}_{A\times B} + PM^{i_2}_{A\times B} + \ldots + PM^{i_t}_{A\times B} + UM^i_{A\times B}$, we can derive that, for the $\{i_1, i_2, \ldots, i_w\}$, where $w < t$, $SM^i_{A\times B} \neq \sum TU^i_{A\times B} + PM^{i_1}_{A\times B} + PM^{i_2}_{A\times B} + \ldots + PM^{i_w}_{A\times B}$; thus, it cannot recover the secret image OS_i for $\{i_1, i_2, \ldots, i_w\}$, where $w < t$ for the secret image.

Theorem 5. *The shares according to the forbidden subset FS_i cannot reveal any information about the secret image.*

From the definition of the forbidden subset, $P_{forbid} = \{FS_1, FS_2, \ldots, FS_m\}$, where FS_i is the ith forbidden subset $i \in [1, m]$, $FS_j = \{j_1, j_2, \ldots, j_r\}$, which means the j_1th, j_2th, ... , j_rth owner is forbidden from recovering the secret, so we can know that the shares in the forbidden subset obviously cannot retrieve any information about the secret images.

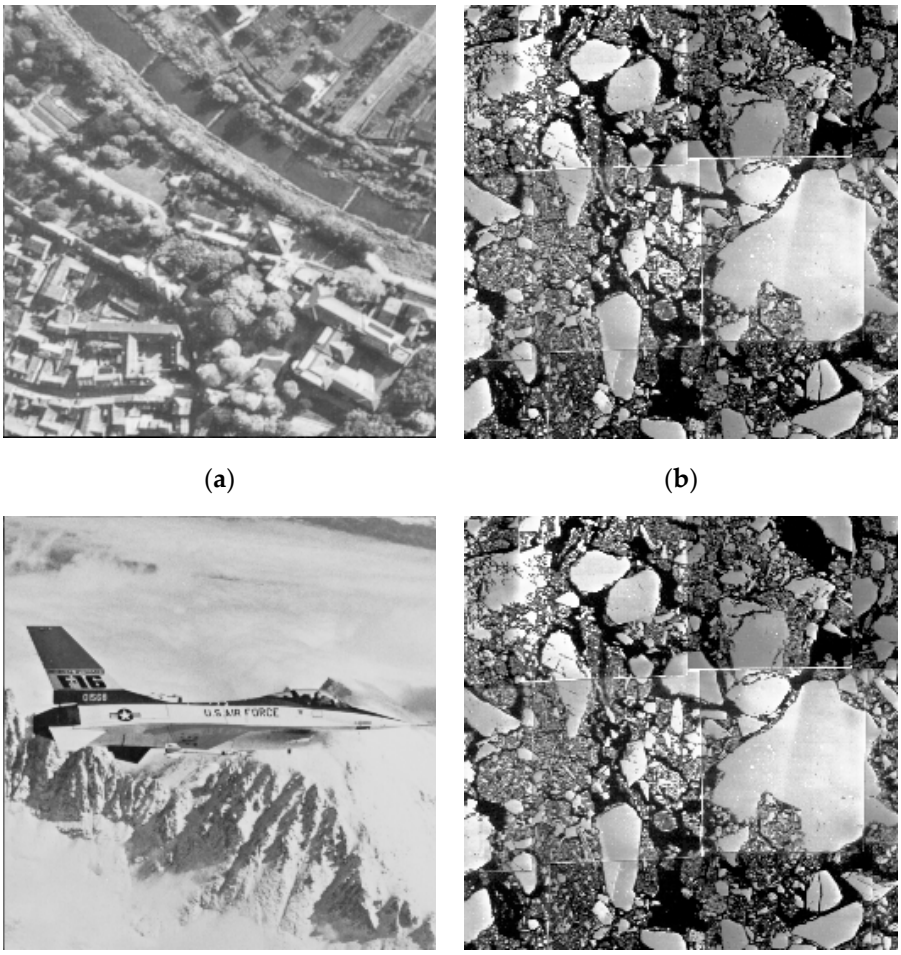
6. Experiments

In this part, some experiments about the performance of the sharing and the recovery are given to evaluate the proposed multi secret sharing scheme with general access structure.

6.1. Secret Sharing and Recovery

Suppose there are 4 secret images with 256 gray level $\{OS_1, OS_2, OS_3, OS_4\}$ to be shared, there are 4 participators $OW = \{OW_1, OW_2, OW_3, OW_4\}$, the qualified part $P_{qual} = \{QS_1, QS_2, QS_3, QS_4\}$, and $QS_1 = \{1, 2, 3\}$, $QS_2 = \{1, 4\}$, $QS_3 = \{2, 4\}$, $QS_4 = \{3, 4\}$ as shown in Example 2.

The secret images are shown in Figure 2.



(**a**) (**b**)

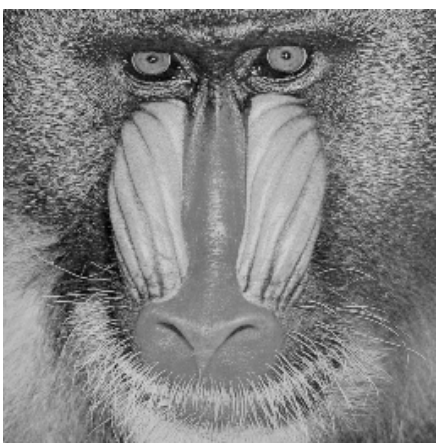
(**c**) (**d**)

Figure 2. The figures of the secret images: (**a**) the secret image OS_1; (**b**) the secret image OS_2; (**c**) the secret image OS_3; (**d**) the secret image OS_4.

Randomly select 4 gray images $\{PO_1, PO_2, PO_3, PO_4\}$ with the same size as the secret image. The images are shown in Figure 3.

(**a**) (**b**)

Figure 3. *Cont.*

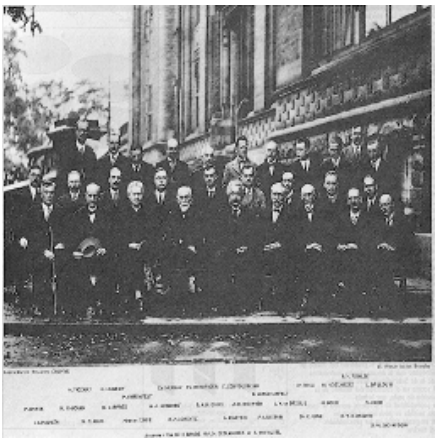


(**c**)

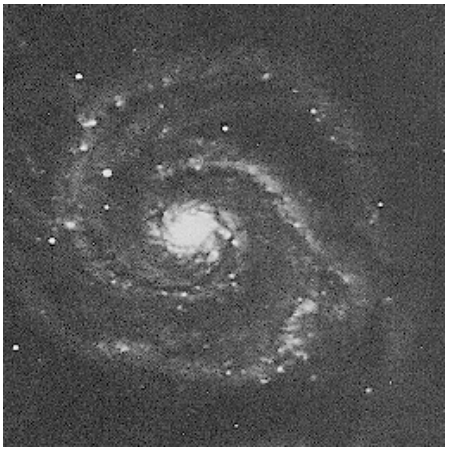
(**d**)

Figure 3. The random selected gray images: (**a**) the gray image PO_1; (**b**) the gray image PO_2; (**c**) the gray image PO_3; (**d**) the gray image PO_4.

Select another 4 gray images randomly $\{UO_1, UO_2, UO_3, UO_4\}$ with the same size. The images are shown in Figure 4.

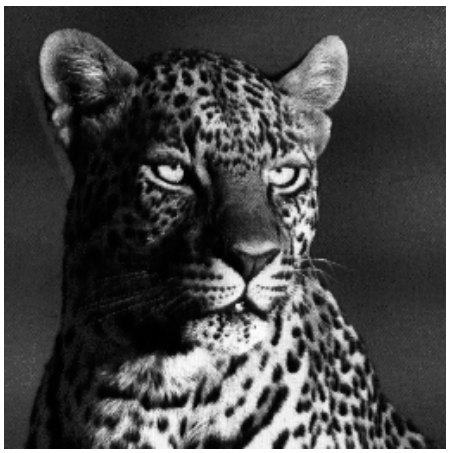


(**a**)



(**b**)

(**c**)

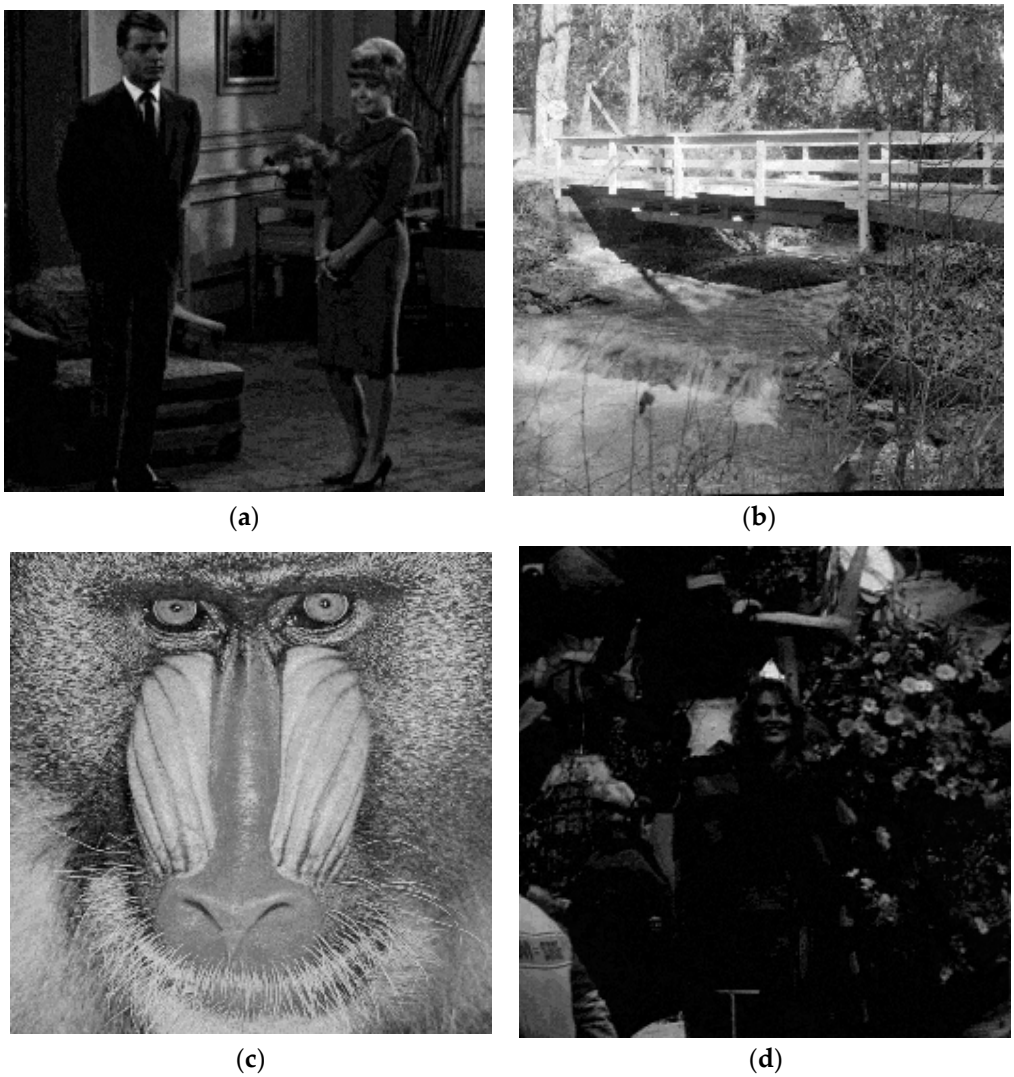


(**d**)

Figure 4. The random selected gray images: (**a**) the gray image UO_1; (**b**) the gray image UO_2; (**c**) the gray image UO_3; (**d**) the gray image UO_4.

Select the essential id of the qualified subsets, $\{id_1, id_2, id_3, id_4\} = \{2, 1, 4, 3\}$.

Transform the secret images $\{OS_1, OS_2, OS_3, OS_4\}$ and the randomly selected images $\{PO_1, PO_2, PO_3, PO_4\}$ and $\{UO_1, UO_2, UO_3, UO_4\}$ into the matrix format over $GF(2^8)$, get the matrix $SM^i_{A\times B}$ about the MSB part of the secret image OS_i, the matrix $SL^i_{A\times B}$ about the LSB part of the secret image OS_i, the matrix $PM^i_{A\times B}$ about the MSB part of the image PO_i, the matrix $UM^i_{A\times B}$ about the MSB part of the secret image US_i, $i \in [1, 4]$, and execute the additional operation as per Equations (12) and (15) to get $TU^i_{A\times B}$ and $TP^{id_i}_{A\times B}$. After the Arnold transform and the bits replacement in Algorithm 1, we can get the final personal shares $\{PS_1, PS_2, PS_3, PS_4\}$ and the universal shares$\{US_1, US_2, US_3, US_4\}$, which are shown in Figures 5 and 6.



(**a**) (**b**)

(**c**) (**d**)

Figure 5. The personal share images: (**a**) the personal share PS_1; (**b**) the personal share PS_2; (**c**) the personal share PS_3; (**d**) the personal share PS_4.

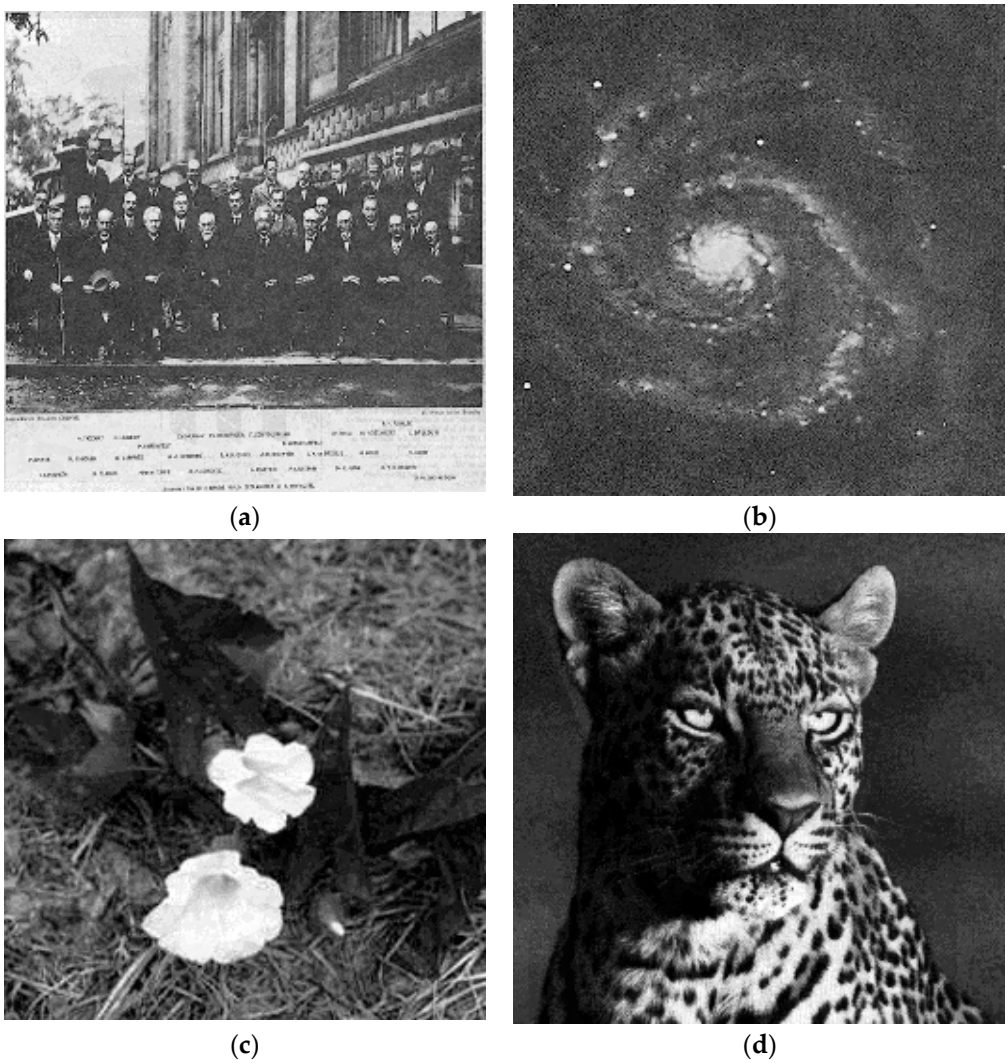
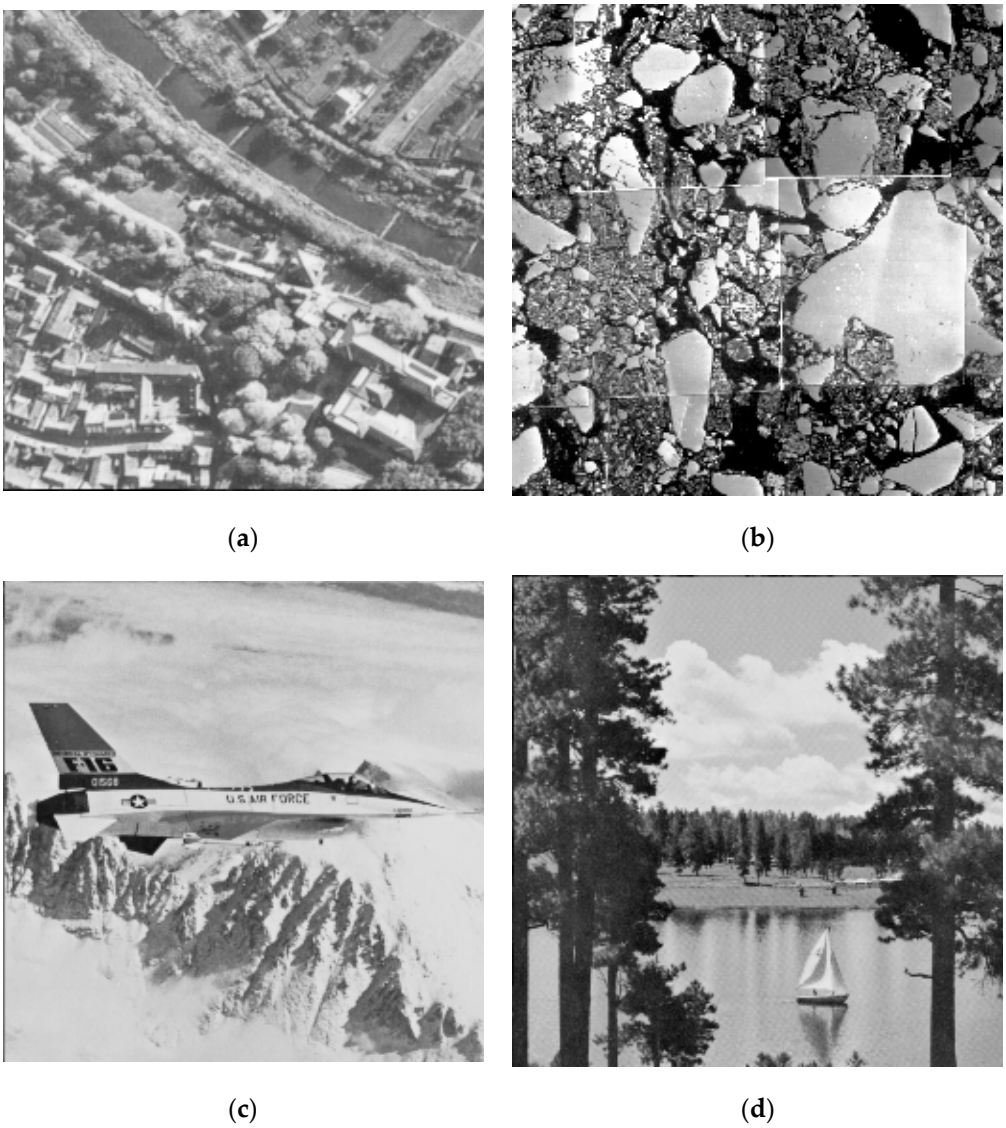


Figure 6. The universal share images: (**a**) the universal share US_1; (**b**) the universal share US_2; (**c**) the universal share US_3; (**d**) the universal share US_4.

The universal shares are shown in Figure 6.

The personal shares are distributed to the owners; each owner OW_i owns a personal share PS_i, and the universal shares US_i are kept by the committee members with high privilege.

In the recovery process, each secret image can be recovered based on the qualified subset. To recover the ith secret image, the owners according to the qualified subset QS_i offer their share images $\{PS_{i1}, PSi_2, \ldots, PS_{it}\}$, and retrieve the universal share UO_i after the verification, or the committee members participate in the recovery by taking the universal share UO_i and execute the matrix operation as shown in Algorithm 3. The retrieved secret images are shown in Figure 7a–d. Figure 7a is the recovered 1th secret image QS_1 used the personal shares$\{PS_1, PS_2, PS_3\}$ and the universal share US_1, Figure 7b is the recovered 2th secret image QS_2 used the personal shares$\{PS_1, PS_4\}$ and the universal share US_2, Figure 7c is the recovered 3th secret image QS_3 used the personal shares$\{PS_2, PS_4\}$ and the universal share US_3, Figure 7d is the recovered 4th secret image QS_4 used the personal shares$\{PS_3, PS_4\}$ and the universal share US_4.



(**a**) (**b**)

(**c**) (**d**)

Figure 7. The recovered secret images: (**a**) the recovered secret image RS_1 by the qualified subset QS_1; (**b**) the recovered secret image RS_2 by the qualified subset QS_2; (**c**) the recovered secret image RS_3 by the qualified subset QS_3; (**d**) the recovered secret image RS_4 by the qualified subset QS_4.

From the experiments results, we can see that all the personal share images and the universal share images are meaningful and look like the nature image, and the recovered secret image is exactly the same as the original secret image.

6.2. Analysis about the Experiments

Although all the shares and the recovered secret image can be recognized easily by the human visual system, we still evaluate the performance of the quality of the shares and the recovered secret images by quantitative analysis. To measure the quality of the share images and the recovered images, the peak signal-to-noise rate (PSNR) is used. The PSNR can evaluate the quality of the modified image compared to the original image, and in general the quality of the image is better if the PSNR is higher.

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})dB \tag{62}$$

where MSE is the mean-square error of the image with the size of $row \times col$. Suppose the pixel value of the modified image and the original image are $p(i, j)$ and $P(i, j)$ respectively, MSE can be expressed as:

$$MSE = \frac{1}{row \times col} \sum_{i=1}^{row} \sum_{j=1}^{col} (P(i, j) - p(i, j))^2 \tag{63}$$

The PSNR of the personal share images in the experiments are shown in Table 1.

Table 1. The quality evaluation of the personal shares by peak signal-to-noise rate (PSNR).

The Personal Share	PSNR
PS_1	31.62 dB
PS_2	32.02 dB
PS_3	31.84 dB
PS_4	30.58 dB

Moreover, the PSNR of the universal share images in the experiment are shown in Table 2.

Table 2. The quality evaluation of the universal shares by PSNR.

The Universal Share	PSNR
US_1	31.83 dB
US_2	31.84 dB
US_3	31.75 dB
US_4	31.63 dB

From the result we can see that the PSNR value of the shares which the 4 LSBs are replaced is about 32 dB. From the point of image process, if PSNR is bigger than 30 dB, we generally consider the quality is good enough to be recognized, and there is tiny difference between the original prepared images and the generated personal share images as shown in Figures 3 and 5, and the original images and the universal shares is also almost looks like the same as shown in Figures 4 and 6.

The quality of the recovered secret images are shown as the Table 3.

Table 3. The quality evaluation of the recovered secret images by PSNR.

The Recovered Secret Images	PSNR
RS_1	∞
RS_2	∞
RS_3	∞
RS_4	∞

From Table 3, we can see that all the PSNR of the recovered secret images result is ∞; this is because that the recovered secret images can be exactly the same as the original secret images from the theoretical analysis and the experiment results, which means there is no lossless in the recovery as shown in Figure 7.

In the secret sharing scheme, to measure the correlation between the secret image and the share image, we use the SSIM (structural similarity index measure) [49] to evaluate the similarity between the different images. SSIM uses the structure combined with the luminance and the contrast to measure the similarity. The value of SSIM is between 0 to 1, and the lower SSIM means that there is less similarity. In this part, we evaluate the similarity between the secret images and all the personal and universal shares. The result is shown in Table 4.

Table 4. The structural similarity index measure (SSIM) between the secret images and the shares.

	PS_1	PS_2	PS_3	PS_4	US_1	US_2	US_3	US_4
OS_1	0.0421	0.0591	0.0528	0.0231	0.0560	0.0620	0.0543	0.0602
OS_2	0.0163	0.0250	0.0342	0.0196	0.0280	0.0776	0.0322	0.0261
OS_3	0.0678	0.0782	0.0874	0.0406	0.0992	0.0715	0.0882	0.0842
OS_4	0.0816	0.0679	0.0811	0.0445	0.0758	0.0693	0.0841	0.0883

From the table, we can observe that the similarity between the secret images and the share images are very low and close to 0, so the shares have nearly no similarity with the secret images.

7. Discussion

There are different methods to construct the different kinds of multi secret sharing schemes with different properties; as such, in this part we will compare our proposed scheme with the typical multi secret sharing schemes from the secret image type, the pixel expansion, access type, the operation type, meaningful share, and lossless recovery.

The secret image type means that the secret images can be binary or gray or color image; the pixel expansion means if the size of the share is bigger than the size of the secret image; access type means that the access is the threshold access or the general access; the operation means that the mathematics computation methods are used in the schemes; meaningful share determines if the shares are meaningful or not; and the lossless recovery determines if the quality of the recovered secret images is lossless or not. The comparison is shown in Table 5.

Table 5. The comparison about the different multi secret sharing schemes.

The Schemes	Secret Image	Pixel Expansion	Access Type	Operation	Meaningful Share	Lossless Recovery
Weir, J [22]	Binary	yes	(n, n)	OR	no	no (low quality)
Chang C C [29]	Gray or color	no	(k, n)	Chinese remainder mathod and Lagrange interpolation	no	yes
Rajput M [31]	Gray or color	no	(n, n+1)	Additive Modulo(256)	no	no
Chen [32]	Binary or gray	no	(n+1, n+1)	XOR	no	yes
Chen [33]	Gray	no	(n, n)	XOR	no	yes
Yang C N [34]	Gray	no	(n, n)	XOR and bit shift	no	yes
Chen C C [35]	Gray (different size)	no	(n, n)	XOR and hash	no	yes
Deshmukh M [36]	Gray	no	(n, n)	XOR and arithmetic modulo	no	yes
Kabirirad S [37]	Gray	no	(n, n)	XOR	no	yes
Nag A [43]	Gray	no	General access	XOR	no	yes
Chen T [46]	Gray	no	General access	XOR	no	yes
Proposed scheme	Gray or color	no	General access	XOR	yes (good enough)	yes

From the comparison of the schemes we can see that, compared with the multi secret sharing schemes based on the visual cryptography, our proposed multi image secret sharing scheme has better performance in terms of the pixel expansion, recovery quality, secret image type, meaningful share, and more general access. It is not like visual cryptography, which does not need any external device and the secret is obtained by overlapping the printed transparent shares. The proposed scheme need to execute the Boolean operations for the pixels of the images with the help of the computers, so it is more complex than the visual cryptography method. Compared with the multi secret sharing schemes based on the polynomial or other algebraic method, it also has the advantages of more simple computation, meaningful share, and more general access. Compared with other Boolean based multi secret sharing schemes, our method can realize more flexible general access not restricted on

the fixed (n, n) or other threshold, and all the shares are meaningful which is not achieved in other methods. Moreover, the quality of the share images is higher than 30 dB which is good enough, the recovery is lossless and is exactly the same as the original secret images. In this paper, we focus on describing the construction of the sharing and recovery process from the point of mathematics operation. However, there are still some point in the proposed scheme that can be improved for example, the 4 LSBs of the original prepared images are replaced in the generation of personal shares and the universal share. In the future we can use some method to reduce the embedded data and obtain a better steganography method to make the embedding more unnoticeable.

8. Conclusions

In this paper, we proposed a multi secret sharing scheme with the general access structure based on the Boolean operation. There is no pixel expansion as in visual cryptography, and the recovery is lossless. Also, there is no distortion in the recovered secret images, and one secret image can be recovered by the owners in the qualified subset, or all the secret images can be recovered by all the owners. All the shares including the personal shares and the universal shares are meaningful and the quality is good enough which will not attract the attention of any adversaries. Furthermore, our scheme can be easily extended to the color images, which will be the focus of our future work.

Author Contributions: Conceptualization, H.C.; Methodology, H.C.; Supervision, D.T.; Validation, D.T.; Writing of original draft, H.C. The authors contributed equally to the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Sichuan Province Science and Technology Support Program (China), grant number 2020YFG0150 and 2019YFG0103.

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

References

1. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
2. 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; IEEE Computer Society: Washington, DC, USA, 1979.
3. Harn, L.; Lin, C. Authenticated Group Key Transfer Protocol Based on Secret Sharing. *IEEE Trans. Comput.* **2010**, *59*, 842–846. [CrossRef]
4. Naor, M.; Wool, A. Access control and signatures via quorum secret sharing. *IEEE Trans. Parallel Distrib. Syst.* **1998**, *9*, 909–922. [CrossRef]
5. Liu, Y.; Yang, C.; Sun, Q. Thresholds based Image Extraction Schemes in Big Data Environment in Intelligent Traffic Management. *IEEE Trans. Intell. Transp. Syst.* **2020**. [CrossRef]
6. Ermakova, T.; Fabian, B. Secret Sharing for Health Data in Multi-provider Clouds. *IEEE Conf. Bus. Inform.* **2013**, 93–100. [CrossRef]
7. Ogiela, M.R.; Ogiela, L. Cognitive Keys in Personalized Cryptography. *IEEE Int. Conf. Adv. Inf. Netw. Appl.* **2017**, 1050–1054. [CrossRef]
8. Ogiela, M.R.; Ogiela, L. Cognitive cryptography techniques for intelligent information management. *Int. J. Inf. Manag.* **2018**, *40*, 21–27. [CrossRef]
9. Ogiela, L.; Ogiela, M.R. Bio-Inspired Cryptographic Techniques in Information Management Applications. In Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 23–25 March 2016; pp. 1059–1063. [CrossRef]
10. Ogiela, M.R.; Ogiela, L. On using cognitive models in cryptography. In Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 23–25 March 2016.
11. Naor, M.; Shamir, A. Visual Cryptography. *Lect. Notes Comput. ENCE* **1994**, *950*, 1–12. [CrossRef]
12. Yang, C.N. New visual secret sharing schemes using pro babilistic method. *Pattern Recognit. Lett.* **2004**, *25*, 481–494. [CrossRef]
13. Shyu, S.J. Image encryption by random grids. *Pattern Recognit.* **2007**, *40*, 1014–1031. [CrossRef]

14. Thien, C.C.; Lin, J.C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [CrossRef]
15. Wang, D.; Zhang, L.; Ma, N. Two secret sharing schemes based on Boolean operations. *Pattern Recognit.* **2007**, *40*, 2776–2785. [CrossRef]
16. Liu, Y.; Yang, C.; Wu, S.; Chou, Y. Progressive (k,n) secret image sharing schemes based on Boolean operations and covering codes. *Signal Process. Image Commun.* **2018**, 77–86. [CrossRef]
17. Yan, X.; Wang, S.; Abd El-Latif, A.A.; Niu, X. Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery. *Multimed. Tools Appl.* **2015**, *74*, 3231–3252. [CrossRef]
18. Han, Y.; He, W.; Dong, H. A verifiable visual cryptography scheme based on XOR algorithm. In Proceedings of the 2012 IEEE 14th International Conference on Communication Technology, Chengdu, China, 9–11 November 2012.
19. Verma, M.; Rani, R. Strong threshold secret image sharing based on Boolean operation. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 29–30 April 2016.
20. Wang, Z.; Jin, H.; Wang, X. An Adaptable (n, n) Secret Image Sharing Mechanism Based on Boolean Operation. *Int. J. Netw. Secur.* **2014**, *16*, 487–493.
21. Isha, M.P.; Dadvi, G.D. Encrypting multiple images using visual secret sharing scheme. *Int. J. Sci. Res. (IJSR)* **2014**, *3*, 107–111.
22. Weir, J.; Yan, W. Sharing multiple secrets using visual cryptography. *IEEE Int. Symp. Circuits Syst. IEEE* 2009. [CrossRef]
23. Aarti, A. Multiple Secret Sharing Scheme with Gray-Level Mixing using EVCS. In Proceedings of the International Conference on Issues and Challenges in Networking, Intelligence and Computing Technologies (ICNICT-2012), Ghaziabad, India, 7–8 September 2012.
24. Wang, K.; Zou, X.; Sui, Y. A Multiple Secret Sharing Scheme based on Matrix Projection. *IEEE Int. Comput. Softw. Appl. Conf. IEEE Comput. Soc.* **2009**, 400–405. [CrossRef]
25. Fereshte, S. Reviewing multiple secret image sharing scheme based on matrix multiplication. *Int. J. Comput. Technol. Appl.* **2013**, *4*, 494–501.
26. Yang, C.-C.; Chang, T.-Y.; Hwang, M.-S. A (t,n) multi-secret sharing scheme. *Appl. Math. Comput.* **2004**, *151*, 483–490. [CrossRef]
27. Adachi, T.; Okazaki, C. A Multi-Secret Sharing Scheme with Many Keys Based on Hermite Interpolation. *J. Appl. Math. Phys.* **2014**, *2*, 1196–1201. [CrossRef]
28. Harn, L.; Hsu, C.-F. (t, n) Multi-Secret Sharing Scheme Based on Bivariate Polynomial. *Wirel. Pers. Commun.* **2017**. [CrossRef]
29. Chang, C.C.; Huynh, N.T.; Le, H.D. Lossless and unlimited multi-image sharing based on Chinese remainder theorem and Lagrange interpolation. *Signal Process.* **2014**, *99*, 159–170. [CrossRef]
30. Deshmukh, M.; Nain, N.; Ahmed, M. A Novel Approach for Sharing Multiple Color Images by Employing Chinese Remainder Theorem. *J. Vis. Commun. Image Represent.* **2017**, *49*, 291–302. [CrossRef]
31. Rajput, M.; Deshmukh, M. Secure (n, n + 1)-Multi Secret Image Sharing Scheme Using Additive Modulo. *Procedia Comput. ENCE* **2016**, *89*, 677–683. [CrossRef]
32. Chen, T.H.; Wu, C.S. Efficient multi-secret image sharing based on Boolean operations. *Signal Process.* **2011**, *91*, 90–97. [CrossRef]
33. Chen, C.C.; Wu, W.J. A secure Boolean-based multi-secret image sharing scheme. *J. Syst. Softw.* **2014**, *92*, 107–114. [CrossRef]
34. Yang, C.-N.; Hua, C. Enhanced Boolean-based multi secret image sharing scheme. *J. Syst. Softw.* **2016**. [CrossRef]
35. Chen, C.C.; Chen, J.L. A new Boolean-based multiple secret image sharing scheme to share different sized secret images. *J. Inf. Secur. Appl.* **2017**, *33*, 45–54. [CrossRef]
36. Deshmukh, M.; Nain, N.; Ahmed, M. Efficient and secure multi secret sharing schemes based on Boolean XOR and arithmetic modulo. *Multimed. Tools Appl.* **2016**. [CrossRef]
37. Kabirirad, S.; Eslami, Z. Improvement of (n,n)-Multi-Secret Image Sharing Schemes Based on Boolean Operations. *J. Inf. Secur. Appl.* **2019**, *47*, 16–27. [CrossRef]
38. Prasetyo, H.; Guo, J.M. A Note on Multiple Secret Sharing Using Chinese Remainder Theorem and Exclusive-OR. *IEEE Access* **2019**, *7*, 37473–37497. [CrossRef]

39. Wu, X.; Lai, Z.R. Random grid based color visual cryptography scheme for black and white secret images with general access structures. *Signal Process. Image Commun.* **2019**, *75*, 100–110. [CrossRef]
40. Lian, C.; Pang, L.; Liang, J. Generalized Random Grid-Based Visual Secret Sharing for General Access Structures. *Comput. J.* **2015**, *58*, 2426. [CrossRef]
41. Das, A.; Adhikari, A. An efficient multi-use multi-secret sharing scheme based on hash function. *Appl. Math. Lett.* **2010**, *23*, 993–996. [CrossRef]
42. Yan, X.; Lu, Y. Progressive visual secret sharing for general access structure with multiple decryptions. *Multimed. Tools Appl.* **2017**, *77*, 1–20. [CrossRef]
43. Nag, A.; Singh, J.P.; Singh, A.K. An efficient Boolean based multi-secret image sharing scheme. *Multimed. Tools Appl.* **2019**, 1–25. [CrossRef]
44. Fang, W.; Lin, J. Universal share for the sharing of multiple images. *J. Chin. Inst. Eng.* **2007**, *30*, 753–757. [CrossRef]
45. Meghrajani, Y.K.; Mazumdar, H.S. Universal Share for Multisecret Image Sharing Scheme Based on Boolean Operation. *IEEE Signal Process. Lett.* **2016**, *23*, 1429–1433. [CrossRef]
46. Chen, T.; Wu, X. Multiple secret image sharing with general access structure. *Multimed. Tools Appl.* **2020**, 1–19. [CrossRef]
47. Rudolf, L.; Harald, N. *Finite Fields*, 2nd ed.; Cambridge University Press: Cambridge, UK, 1997.
48. Arnol'd, V.I. *Ergodic Problems of Classical Mechanics*; Benjamin: New York, NY, USA, 1968.
49. 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] [PubMed]