mathematics

MDPI

Article

Two-in-One Secret Image Sharing Scheme with Higher Visual Quality of the Previewed Image

Xin Wang, Peng Li * and Zihan Ren

Department of Mathematics and Physics, North China Electric Power University, Baoding 071003, China; wang_20_20@163.com (X.W.); renzihanrzh@163.com (Z.R.)
* Correspondence: lphit@163.com

Abstract: Secret image sharing (SIS) scheme is a secret image encoding and decoding scheme that reconstructs the secret image only if the number of participants is sufficient. In contrast, inadequate participants gain no information about the secret image. Two-in-one secret image sharing (TiOSIS) scheme is a kind of SIS scheme with two decoding options, quick preview without computation and accurate recovery with computer. For higher decoding speed, Li et al. proposed an improved two-in-one secret image sharing scheme, utilizing Boolean operation for less computational complexity, where the visual quality of the previewed image is deteriorated. In this paper, we use q-bit gray visual cryptography to build a mathematical model for better visual quality of the previewed image based on Li et al.'s TiOSIS scheme. The black sub-pixels of shadows corresponding to a black secret pixel are replaced by a q-bit grayscale value rather than an 8-bit grayscale value where q is a positive integer smaller than 8. The theoretical analysis and experiments are exhibited to guarantee feasibility and effectiveness of the proposed scheme.

Keywords: Boolean operation; q-bit gray visual cryptography; fast preview; secret image sharing

check for updates

Citation: Wang, X.; Li, P.; Ren, Z. Two-in-One Secret Image Sharing Scheme with Higher Visual Quality of the Previewed Image. *Mathematics* **2022**, *10*, 678. https://doi.org/10.3390/math10050678

Academic Editor: Angel Martín-del-Rey

Received: 24 January 2022
Accepted: 20 February 2022
Published: 22 February 2022

1. Introduction

With the advent of big data, information security has become a vital issue that needs to be solved urgently. Secret information and images specifically play a critical role in both military and commercial applications. The encryption and decryption processes are given to ensure the safety of image information, namely secret image sharing (SIS) scheme. The key idea of SIS is to distribute a secret image to multiple participants for safekeeping. Only the participants that meet the decryption conditions can restore the secret image, otherwise the information about the secret image cannot be obtained. Secret image sharing schemes are mainly divided into two categories due to the decryption method: one is polynomial-based secret image sharing (PSIS) scheme relying on Lagrange's interpolation, and the other is visual cryptographic scheme (VCS) depending on human visual system.

Polynomial-based secret sharing was first proposed by Shamir [1] at the European Cryptography Summit. Thien and Lin [2] proposed an enhanced (k, n)-PSIS scheme, with $k \leq n$, where the secret image is shared among n shadow images and any k shadows can reveal the secret image by computation. Each shadow image is $1/k$ times of the original secret image. PSIS scheme takes advantage of perfectly decoding, holding an optimal visual quality of the recovered image, where it has to run with the help of computer device. Naor and Shamir [3] put forward VCS in 1994. Without any complex calculations, VCS gets the revealed image by superposition using only the human visual system. For higher security of authenticity and accuracy of secret images, Hu et al. [4] proposed cheating prevention VCS. Zhou et al. [5] proposed halftone VCS for creating meaningful image sharing techniques that reduce attacker suspicion of encrypted data. For different authority levels of participants, present a VCS with essential participants [6]. However, the visual quality of the restored image is not ideal.

One of increasing SIS performance methods is to apply exclusive-*OR* (*XOR*) operation instead of *OR* operation in decryption process. Scheme [7] has good resolution on contrast and vision properties. Chao and Lin [8] put forward a novel technology of Boolean-based secret image sharing (BSIS) scheme combining benefits of perfect decoding and fast approaches. The encrypted sub-image is twice the secret image, with less calculation time and lower computational complexity. In addition, Guo et al. [9] proposed a method based on *XOR* decryption. The improved encryption algorithm used the reflexivity property of *XOR* operation, which has nothing with base matrices designs. Scheme [10] gave an enhanced BSIS with less storage space. More *XOR*-based VCSs are devised for meaningful shadows and resolving various problems in [11] separately. The problems include pixel expansion, contrast loss, explicit codebook requirement and lossy recovery of secret image.

In recent years, researchers have proposed more SIS schemes, including schemes for color images [12,13], progressive decoding [14,15], meaningful shares [16], and minimizing pixel expansion [17,18], etc. In addition, there exist novel SIS schemes based on various theorems, like matrix theory [19], non-full rank linear model [20] and natural steganography (NS) [21]. More methods of steganography and multimedia security [22,23] are given in these years. It is worth noting that a specific SIS scheme is a collection of several types.

For higher requirements of application, it is possible to combine two SIS schemes to possess the advantages of these SIS schemes, called two-in-one secret image sharing (TiOSIS) scheme. PSIS scheme can be combined with VCS to achieve the purposes of fast preview and accurate decryption [24,25]. To resolve the problem of lossless reconstruction and improve the visual quality of the previewed image [26] and share more information [27], Li et al. gave improved SIS methods based on a gray mixing model separately. Additionally, the scheme [28] combined BSIS to construct a TiOSIS scheme, which reduces the computation times in decoding process. For convenience, we refer to the scheme [28] as BO-TiOSIS. More researchers are dedicated to studying TiOSIS schemes, including progressive recovery [29], and sharing multiple secrets based on random-grid visual cryptographic scheme (RGVCS) [30].

A typical feature of TiOSIS scheme is two decoding Phases: previewing capability by stacking shadows and lossless recovery by computation. In Phase one, adequate shadow images are printed on transparencies and superimposed on any authorized set of elements to visually restore the information of the secret image. During Phase two, the gray information embedded in shadow images is extracted. Then the original secret image is recovered by decryption algorithm. This article mainly ameliorates the visual quality of the previewed image. Based on the BO-TiOSIS scheme, we utilize a gray visual cryptography scheme with q-bit grayscale values (qGVCS) to change the embedding method for improving recognition of the previewed image in Phase one. Therefore, we establish a single model of the relationship between visual quality of the previewed image and size expansion of shadows.

The rest of the structure of this paper is as follows. Next, we briefly introduce the definitions of VCS, PBVCS, gray visual cryptography scheme (GVCS) and qGVCS. Li et al.'s BO-TiOSIS scheme is reviewed in Section 2.2. Section 3 indicates the model building of an improved TiOSIS scheme, including motivation, design concept and theoretical analysis. Related experimental results and discussion are presented in Section 4, and the performance comparison of the scheme is also in this part. Finally, concise conclusions are formulated in Section 5.

2. Related Works

2.1. VCS and GVCS

The (k, n)-VCS is a typical threshold secret image sharing scheme. A secret image is shared into n shadow images printed on transparencies and then distributed to the corresponding n participants. If no fewer than k participants gather, secret information can be recovered by stacking their shadows. Nothing about the secret is reconstructed if there are less than k shares. Let *OR* ($D\,|\,r$) denote the '*OR*'-ed vector of any r rows of matrix $D \in \mathbb{Z}^{n \times m}$, with $r \leq n$, and $H(\boldsymbol{v})$ be the Hamming weight of vector $\boldsymbol{v}$. Let l and h be nonnegative integers, with $0 \leq l < h \leq m$. The notation m represents pixel expansion of (k, n)-VCS. Thus, the definition of VCS is exhibited as below:

Definition 1. *A (k, n)-VCS is composed of double sets: white set C_0 and black set C_1. The elements in sets C_0 and C_1 are both base Boolean matrices. Randomly choose a matric $B_0 \in \mathbb{Z}^{n \times m}$ from C_0 to encode a white pixel and extract a matric $B_1 \in \mathbb{Z}^{n \times m}$ from C_1 to encrypt a black pixel stochastically. The selected matrix confirms the color of m pixels corresponding to n shares. This scheme is deemed valid if the following conditions are met [3]:*

1. *(Contrast condition) $H\ (OR\ (B_0 \mid k)) \leq l$, and $H\ (OR\ (B_1 \mid k)) \geq h$;*
2. *(Security condition) $H\ (OR\ (B_0 \mid t)) = H\ (OR\ (B_1 \mid t))$, for any $0 < t < k$.*

A VCS is called a perfect black VCS (PBVCS) as well if $h = m$. All elements of the '*OR*'-ed vector of any k rows of black matrix are black pixels. Hence $H\ (OR\ (B_1 \mid k)) = m$.

Moreover, the modified VCS is the so-called gray visual cryptography scheme (GVCS) if all shadows are grayscale images. This construction method is concealing grayscale values into shares of VCS. In the revealing process, the stacking operation on grayscale shadows cannot be simulated by *OR* operation. Let us employ a formal definition of a gray mixing model to simulate the stacking operation on grayscale values.

Definition 2. *Let g_1 and g_2 be two grayscale values. Two transparencies with gray colors g_1 and g_2 are stacked. The resulting grayscale value g_3 can be approximately expressed as below [27]:*

$$g_3 = MX\ (g_1, g_2) = int\ (g_1 \times g_2/255) \tag{1}$$

where $MX\ (\cdot)$ represents the gray-mixed result of its arguments, and the $int\ (\cdot)$ function approximates its argument to the nearest integer.

Let G_0 and G_1 represent the share matrices used in GVCS. Let $MX\ (D \mid r)$ be the '*MX*'-ed vector of any r rows of $D \in \mathbb{Z}^{n \times m}$, with $r \leq n$, and $Avg(\boldsymbol{v})$ denote the average expected grayscale value of all elements in vector $\boldsymbol{v}$. Analogously, TiOSIS method based on GVCS should satisfy the following conditions:

1. (Contrast condition) $Avg\ (MX\ (G_1 \mid k)) > Avg\ (MX\ (G_0 \mid k))$;
2. (Security condition) $Avg\ (MX\ (G_0 \mid t)) = Avg\ (MX\ (G_1 \mid t))$, *for any* $0 < t < k$;
3. (Contrast condition) $H\ (OR\ (B_1 \mid k)) = m$, $H\ (OR\ (B_0 \mid k)) < m$;
4. (Security condition) $H\ (OR\ (B_1 \mid t)) < H\ (OR\ (B_1 \mid k))$, *for any* $0 < t < k$.

Thereinto, Conditions (1) and (2) illustrate the previewed image is identified with k shadows and nothing can be obtained if less than k shadows to take part in it. Conditions (3) and (4) state a black pixel block is able to extract the embedded information on any k shadows. In addition, there is no meaningful grayscale pixels in white pixel block.

Moreover, a GVCS is also called qGVCS if the concealed grayscale values are q bits. The GVCS embeds grayscale values into shadow images directly, where each grayscale value occupies 8 bits in the range of [0, 255]. Let each gray information convert into a q-bit grayscale value in qGVCS. As a consequence, the range of grayscale values is $[0, 2^q - 1]$.

2.2. Li et al.'s BO-TiOSIS Scheme

Li et al. proposed a BO-TiOSIS scheme by combining PBVCS, GVCS with BSIS [8]. The brief encoding structure is demonstrated in Figure 1. It shares two secret images: grayscale secret image by BSIS and binary secret image by PBVCS. Then embed the processed gray image into shares to obtain grayscale shadow images which are assigned to different participants. Replace the pixel '1' in black basis matrix with the processed grayscale value and replace pixel '1' in white basis matrix with grayscale values randomly selected from [0, 255]. All pixels '0' in basic matrices are replaced with 255. In the decryption process, it not only reveals a fuzzy previewed image by superimposing shadows, but also is able to decode the perfect grayscale secret image by fewer Boolean operations. In terms of the source of secret images, the binary secret image can be divided into two categories according to the different acquisition methods. One is a halftone image obtained by halftone processing technique of grayscale secret image, and the other is black-and-white image that has nothing to do with grayscale secret image. Compared with traditional polynomial-based TiOSIS scheme, BO-TiOSIS scheme is faster in the second decoding process.

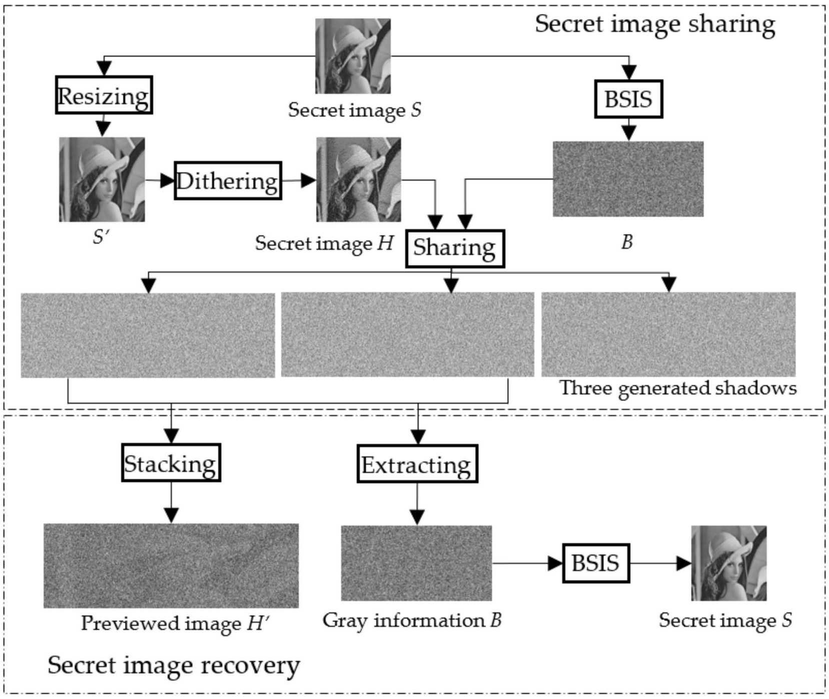

Figure 1. The brief diagram of (2, 3)-BO-TiOSIS scheme.

3. The Proposed Scheme

3.1. Motivation

In most cases, users have to know the brief structure of the secret image in advance. Hence, we propose a mathematical model for higher visual quality of the previewed image and to make a balance between size expansion and visual quality. BO-TiOSIS scheme has the advantage of lower computational complexity. One of this method's drawbacks is that the visual quality of the previewed image is extremely poor. When hiding the grayscale image, the embedded information may be a grayscale value 255, which may be confused with the white shadow pixels. To avoid the confusion of white pixel '0' and the embedded grayscale value 255, this scheme used two pixels to represent grayscale values larger than 253. The simplest method is using (254,0) to show grayscale value 254, and (254,1) to denote grayscale value 255. Furthermore, in the revealing process, we need an extra operation to add the extracted value 254 with the value behind it. These extra processes enlarge size expansion of shadows and make this scheme more complicated.

3.2. Design Concept

We propose a mathematical model for higher visual quality and lower size expansion based on BO-TiOSIS scheme. Model building contains three techniques: PBVCS, qGVCS [27] and BSIS scheme [8]. The principle of qGVCS is extremely simple that convert 8-bit grayscale values into q-bit grayscale values and conceal them into shares encoded by VCS. About the transformation of grayscale values, it is easy to implement. We first transform 8-bit gray values into bit stream, and then each q bits are converted to a q-bit gray value. For example, if we have W 8-bit grayscale values, we can have a bit stream with $8W$ bits. Since each q

bits should be converted to one gray value, we have $8W/q$ q-bit grayscale values. Example 1 states an accurate result that is easy to understand.

This model mainly enhances the visual quality of the previewed image by limiting q-bit gray values where q is a positive integer smaller than 8. Particularly, the model with 8GVCS is the same as BO-TiOSIS scheme. Figure 2 shows the basic framework of the proposed (k, n)-TiOSIS scheme. In the encoding process, secret image S is first shared by BSIS method to generate the corresponding shadow image B. The 8-bit image B is converted to q-bit grayscale values C. Then secret image H subjected to size compression is encrypted by (k, n)-PBVCS to obtain n shares $V_1, V_2, \ldots, V_n$. In terms of the source of secret image H, halftone processing is used to dither grayscale image and gain a binary image. Otherwise, secret image H is derived with no secret S from image database. Finally, the idea of qGVCS is important to embedding the q-bit grayscale image C into shadow images $V_1, V_2, \ldots, V_n$ so that we obtain shadow images of the whole TiOSIS scheme $G_1, G_2, \ldots, G_n$. The structure of the sharing scheme is demonstrated in Algorithm 1.

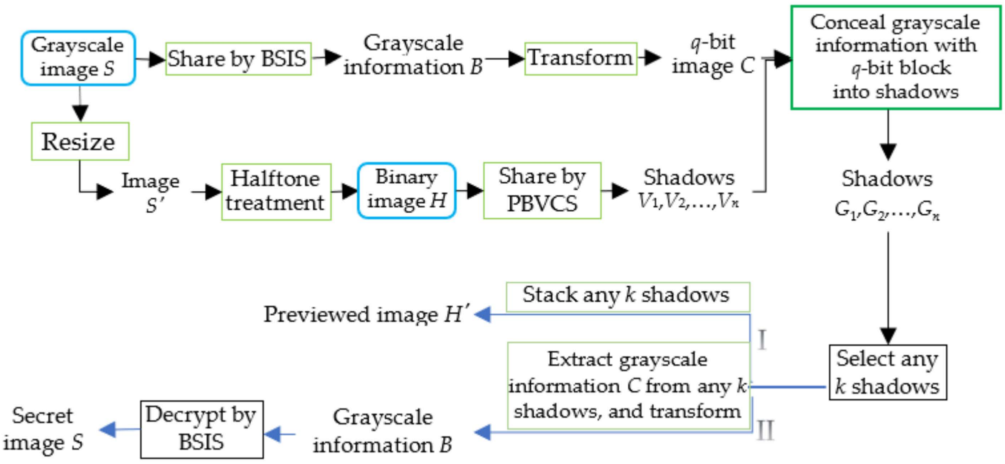
Grayscale image S
Share by BSIS
Grayscale information B
Transform
q-bit image C
Conceal grayscale information with q-bit block into shadows
Resize
Image S'
Halftone treatment
Binary image H
Share by PBVCS
Shadows $V_1, V_2, \ldots, V_n$
Shadows $G_1, G_2, \ldots, G_n$
Stack any k shadows
Previewed image H'
I
Extract grayscale information C from any k shadows, and transform
Select any k shadows
II
Secret image S
Decrypt by BSIS
Grayscale information B

Figure 2. The framework of the proposed (k, n)-TiOSIS method.

Algorithm 1. Secret image encoding process

Input: secret image S and H, value of q.
Output: shadow images $G_1, G_2, \ldots, G_n$.

Step 1: Utilize sharing scheme of BSIS given in [8] to encrypt secret image H. Then generate gray image B.
Step 2: Convert all secret information in B into q-bit pixel values through bit conversion and obtain q-bit grayscale values C. Suppose C has W pixels.
Step 3: Dither S to obtain halftone image H.
Step 4: If the number of black pixels in H is smaller than W/m, where m is the pixel expansion of (k, n)-PBVCS, then enlarge the size of secret image S, and go back to Step 3. Otherwise, go to Step5.
Step 5: Generate n shadow images $V_1, V_2, \ldots, V_n$ by sharing binary image H for (k, n)-PBVCS. When sharing black pixels of H, extract m unembedded pixels in C to replace all black sub-pixels in shadows. However, when sharing white pixels of H, generate random grayscale values within the range of $0\text{\textasciitilde}2^q\text{–}1$ to replace all black sub-pixels in shadows.
Step 6: Obtain n grayscale images $G_1, G_2, \ldots, G_n$.

There are two decoding options in the recovery process. One is to obtain a fuzzy secret image H' by superimposing transparencies with any k shadows. The other is to extract q-bit shadow information C from any k shadows and convert into 8-bit image B, thus exploiting the BSIS scheme to restore an accurate recovered image. The specific steps of decryption process are described in Algorithm 2.

```
Algorithm 2. Secret image decoding process
Input: $k$ shadow images $G_1, G_2, \ldots, G_k$.
Output: a vague image $H'$, secret image $S$.
Step 1: Print $k$ shadow images $G_1, G_2, \ldots, G_k$ on transparencies and stack together.
Step 2: Generate fuzzy image $H'$.
Step 3: Extract $q$-bit information from $k$ shadows $G_1, G_2, \ldots, G_k$.
Step 4: Convert the extracted $q$-bit information into 8-bit pixel values through bit conversion, and obtain $B$.
Step 5: Decrypt information $B$ by BSIS scheme [8] to generate secret image $S$.
```

For accurate analysis, the embedding principle and extracting principle are expressed as below. If secret pixel of binary image is black, then embed grayscale values into black sub-pixels while replace white sub-pixels with grayscale value 255. If secret pixel is white, then conceal randomly selected grayscale values into black sub-pixels and express white sub-pixels as grayscale value 255. Example 1 shows the process result in detail. Given B_0 and B_1:

$$B_0 = \begin{pmatrix} 1\,1\,0 \\ 1\,1\,0 \\ 1\,1\,0 \end{pmatrix}_{3\times 3}, \ B_1 = \begin{pmatrix} 1\,1\,0 \\ 1\,0\,1 \\ 0\,1\,1 \end{pmatrix}_{3\times 3} \tag{2}$$

denote white base matrix and black base matrix of a (2, 3)-PBVCS separately. Hence conceal q-bit grayscale values g_1, g_2, g_3 and obtain a pair of corresponding matrices G_0 and G_1:

$$G_0 = \begin{pmatrix} r\,r\,255 \\ r\,r\,255 \\ r\,r\,255 \end{pmatrix}_{3\times 3}, \ G_1 = \begin{pmatrix} g_1 & g_2 & 255 \\ g_1 & 255 & g_3 \\ 255 & g_1 & g_2 \end{pmatrix}_{3\times 3} \tag{3}$$

where r represents random number uniformly distributed in $[0, 2^q–1]$. The augmented Matrices in Equations (2) and (3) above have 3 rows, which means three participants, and 3 columns, which states the size ratio of shadows to binary secret image.

Example 1. *For (2,3)-TiOSIS based on 7GVCS, the embedded process is drawn as below, where gray information are 25, 234, 113. Then they are represented in binary form as '00011001', '11101010', '01110001'. Rearrange them in 7-bit as '0001100', '1111010', '1001110' to gain three 7-bit gray values 12, 122, 78. Besides, the two random numbers are randomly selected as 34, 56. Thus G_0 ang G_1 are given*:

$$G_0 = \begin{pmatrix} 34\ 56\ 255 \\ 34\ 56\ 255 \\ 34\ 56\ 255 \end{pmatrix}_{3\times 3}, \ G_1 = \begin{pmatrix} 12 & 122 & 255 \\ 12 & 255 & 78 \\ 255 & 122 & 78 \end{pmatrix}_{3\times 3} \tag{4}$$

In addition, extract a group of m unprocessed grayscale information on any k shadows and reconstruct matrix like G_1 or G_0 described in Equation (5). If there exists a column that all pixels are 255, then stop and continue extracting. If there is no such column, select grayscale values in one column other than 255 as embedded information in turn. Example 2 illustrates the specific extracting process of easy understanding.

Example 2. *For (2,3)-TiOSIS based on 7GVCS, the extracting process is drawn as below. From formula (5), there is no gray information in G_0. Extract grayscale values 12, 122, 78 from black matrix G_1.*

$$G_0 = \begin{pmatrix} 34\ 56\ 255 \\ 34\ 56\ 255 \end{pmatrix}_{2\times 3}, \ G_1 = \begin{pmatrix} 12 & 122 & 255 \\ 12 & 255 & 78 \end{pmatrix}_{2\times 3} \tag{5}$$

3.3. Theoretical Analysis

In this section, theorems and theoretical analysis are given for building modelling effectively. The following content illustrates the whole scheme in mathematical model relying on Conditions (1)-(4). The reason that we separate the cases $q < 8$ and $q = 8$ is coming from the information embedding method. When $q = 8$, the embedded information may be grayscale value 255, which may be confused with the white shadow pixels. The grayscale values larger than 253 are split into two values, the size of the processed gray image will increase a little bit. However, when q is less than 8, the largest q-bit grayscale value is 127. This step is not needed. Concrete proof processes of the conditions are given in BO-TiOSIS scheme while $q = 8$. Now prove that the proposed mathematical modelling satisfies these conditions with $q < 8$.

Theorem 1. *The (k, n)-TiOSIS scheme based on qGVCS meets threshold and security condition represented in Conditions (3) and (4) for q < 8.*

Proof. Based on the definition of (k, n)-VCS, any information of the secret image cannot be recovered with less than k shadow images. We have:

$$H\ (OR\ (B_0 \mid t)) = H\ (OR\ (B_1 \mid t)),\ 0 < t < k \tag{6}$$

and because of the contrast condition in Definition 1, we gain:

$$H\ (OR\ (B_0 \mid k)) < H\ (OR\ (B_1 \mid k)) \tag{7}$$

From the rule of (k, n)-PBVCS, we find that:

$$H\ (OR\ (B_1 \mid k)) = m \tag{8}$$

Then associate Equation (7) with Equation (8) and get:

$$H\ (OR\ (B_0 \mid k)) < m \tag{9}$$

So, Condition (3) is proved. Due to the above equations, acquire the tacit knowledge.

$$H\ (OR\ (B_1 \mid t)) < H\ (OR\ (B_1 \mid k)) \tag{10}$$

That is, the amount of black sub-pixels corresponding to a black secret pixel stacking k shares is better than that with t shares, where $t < k$. Thus, we have:

$$H\ (OR\ (B_0 \mid t)) < H\ (OR\ (B_1 \mid k)) \tag{11}$$

from Equation (6). However, both $H\ (OR\ (B_0 \mid k))$ and $H\ (OR\ (B_0 \mid t))$ are smaller than $H\ (OR\ (B_1 \mid k))$. Because of inequality, we cannot determine the magnitude of $H\ (OR\ (B_0 \mid k))$ and $H\ (OR\ (B_0 \mid t))$. That is why white secret pixels should not be the space for hiding grayscale values. Only black secret pixels conceal meaningful grayscale information. Condition (4) is verified. □

Theorem 2. *The (k, n)-TiOSIS scheme based on qGVCS meets Condition (2) for q < 8.*

Proof. Base matrices G_0 and G_1 of qGVCS are generated from B_0 and B_1, respectively, where B_0 and B_1 are the base matrices of (k, n)-PBVCS. Since B_0 and B_1 satisfy security condition of VCS, we show:

$$H\ (OR\ (B_0 \mid t)) = H\ (OR\ (B_1 \mid t)),\ 0 < t < k \tag{12}$$

It means they are the same in construction with less than k rows. All grayscale information embedded in shares are within the range of [0, 2^p–1]. Therefore, G_0 and G_1 also have the same structure with less than k rows. That is:

$$Avg\ (MX\ (G_0 \mid t)) = Avg\ (MX\ (G_1 \mid t)),\ 0 < t < k \tag{13}$$

The verification of this condition is completed. □

Condition (1) is extremely difficult to be verified in mathematical form. Since this condition tells us the average gray value of all black secret pixels is higher than all white secret pixels. We analyse this condition from two aspects: the visual quality of previewed image and size expansion.

3.3.1. Visual Quality of Previewed Image

In VCS, the revealed image is not the same as the secret image. The visual quality of the revealed image is degraded. Contrast is used to evaluate the visual quality of the revealed image. For GVCS, the contrast is evaluated by the difference of average grayscale values between the black pixel block and white pixel block. The definition of contrast is described as follows:

Definition 3. *Let r_1 and r_0 respectively denote the average grayscale values of the black pixel block and white pixel block in restored image. Then the contrast of restored image of GVCS is* [27]:

$$\alpha = \frac{r_0 - r_1}{2} \tag{14}$$

The result of stacking two grayscale colors is a darker gray image according to the grayscale mixing model. As q decreases, the maximum grayscale value and average gray value are lowered. Now, calculate the contrast of the proposed model for base matrices with corresponding base matrices of (2, n)-PBVCS. The structures are:

$$B_0 = \begin{pmatrix} 0 & 1 & \cdots & 1 & 1 \\ 0 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 1 & 1 \\ 0 & 1 & \cdots & 1 & 1 \end{pmatrix}_{n\times n},\ B_1 = \begin{pmatrix} 0 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 0 \end{pmatrix}_{n\times n} \tag{15}$$

Let $g_{i,j}$ denote the embedded grayscale information, with i = 1, 2. If i = 1, then $g_{1,j}$ represents gray value randomly selected and concealed in white base matrix B_0. Where j = 1, 2, . . . , n–1 except from zero column. If i = 2, then hide $g_{2,j}$ in black base matrix B_1, j = 1, 2, . . . , n. Let g' represent the MX-ed value of any two rows of the corresponding column. From embedding principle, G_0 and G_1 are:

$$G_0 = \begin{pmatrix} 255 & g_{1,1} & \cdots & g_{1,n-2} & g_{1,n-1} \\ 255 & g_{1,1} & \cdots & g_{1,n-2} & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 255 & g_{1,1} & \cdots & g_{1,n-2} & g_{1,n-1} \\ 255 & g_{1,1} & \cdots & g_{1,n-2} & g_{1,n-1} \end{pmatrix}_{n\times n},\ G_1 = \begin{pmatrix} 255 & g_{2,2} & \cdots & g_{2,n-1} & g_{2,n} \\ g_{2,1} & 255 & \cdots & g_{2,n-1} & g_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ g_{2,1} & g_{2,2} & \cdots & 255 & g_{2,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n-1} & 255 \end{pmatrix}_{n\times n} \tag{16}$$

Contrast equation of (2, n)-qGVCS for specific base matrices G_0 and G_1 is indicated in Theorem 3.

Theorem 3. *Suppose G_0 and G_1 are drawn as Equation (16) with respect to (2, n)-qGVCS, where pixel expansion of corresponding (2, n)-PBVCS is n. Symbols g_b and g_w denote the mean gray values of black pixel block and white pixel block separately. Then verify that the contrast of qGVCS is the following equation.*

$$\alpha_q = \frac{1}{255n}\left(\frac{(2^q-1)^2}{1020} + 256 - 2^q\right) \tag{17}$$

Proof. There are n grayscale values in a white pixel block of reconstructed image of (2, n)-qGVCS depending on base matrix G_0, denoted as $g'_{1,1}, g'_{1,2}, \ldots, g'_{1,n-2}, g'_{1,n-1}$, 255. Calculate them via gray mixing model:

$$g'_{1,i} = \frac{(g_{1,i} \times g_{1,i})}{255},\ i = 1,\ 2,\ \ldots,\ n–1 \tag{18}$$

Thus, obtain average grayscale value of white pixel block of renewed image, signified by g_w.

$$g_w = \frac{g'_{1,1} + g'_{1,2} + \cdots + g'_{1,n-1} + 255}{255} \tag{19}$$

Now turn to G_1 in a similar way. There exists n grayscale values in black pixel block of previewed image, denoted as $g'_{2,1}, g'_{2,2}, \ldots, g'_{2,n-1}, g'_{2,n}$, and show that:

$$g'_{2,j} = \begin{cases} \frac{(g_{2,j} \times g_{2,j})}{255}, & i = 3,\ 4,\ \cdots,\ n \\ g_{2,j}, & i = 1,\ 2 \end{cases} \tag{20}$$

Then derive mean grayscale value of black pixel block:

$$g_b = \frac{g'_{2,1} + g'_{2,2} + \cdots + g'_{2,n-1} + g'_{2,n}}{255} \tag{21}$$

According to the security of BSIS, the processed grayscale value satisfies uniform distribution. Hence, $g_{i,j}$ meets uniform distribution on $\{0, 1, \ldots, 2^q–1\}$, and the mathematical expectation of $g_{i,j}$ is equal to $(2^q–1)/2$. Let $E(\cdot)$ denote expectation function, then acquire:

$$E(g_{i,j}) = \frac{2^q-1}{2} \tag{22}$$

Moreover, expectation function is with the property of the linear feature. Derive the expectations $E(g_w)$ and $E(g_b)$ of grayscale values for white pixel block and black pixel block:

$$\begin{aligned} E(g_w) &= (n-1)\tfrac{(2^q-1)^2}{1020n} + \tfrac{255}{n} \\ E(g_b) &= (n-2)\tfrac{(2^q-1)^2}{1020n} + \tfrac{2^q-1}{n} \end{aligned} \tag{23}$$

Relying on Definition 3, the contrast α_q of (2, n)-qGVCS can be written as:

$$\alpha_q = \frac{(E(g_w) - E(g_b))}{255} = \frac{1}{255n}\left(\frac{(2^q-1)^2}{1020} + 256 - 2^q\right) \tag{24}$$

Hence, prove the theorem completely. □

The contrast of qGVCS for any given base matrices can be calculated in this way. The lower the value q, the darker the grayscale pixel color. Thus, gray level difference between white pixel block and black pixel block is larger. In other words, the contrast of the proposed model is higher as well. Table 1 results contrast trend with q changing, which increases as q decreases. It also does when n reduces. Hence the proposed model combining qGVCS can show better visual quality of the previewed image.

Table 1. The contrast α_q of the proposed model.

(k, n)	B'_0	B'_1	α_8	α_7	α_6	α_5	α_4	α_3	α_2	α_1
(2, 2)	$\begin{bmatrix} 1\,0 \\ 1\,0 \end{bmatrix}$	$\begin{bmatrix} 1\,0 \\ 0\,1 \end{bmatrix}$	0.125	0.282	0.384	0.441	0.471	0.486	0.494	0.498
(2, 3)	$\begin{bmatrix} 1\,1\,0 \\ 1\,1\,0 \\ 1\,1\,0 \end{bmatrix}$	$\begin{bmatrix} 1\,1\,0 \\ 1\,0\,1 \\ 0\,1\,1 \end{bmatrix}$	0.083	0.188	0.256	0.294	0.314	0.324	0.329	0.332
(2, 4)	$\begin{bmatrix} 1\,1\,1\,0 \\ 1\,1\,1\,0 \\ 1\,1\,1\,0 \\ 1\,1\,1\,0 \end{bmatrix}$	$\begin{bmatrix} 1\,1\,1\,0 \\ 1\,1\,0\,1 \\ 1\,0\,1\,1 \\ 0\,1\,1\,1 \end{bmatrix}$	0.063	0.141	0.192	0.221	0.236	0.243	0.247	0.249
(2, 5)	$\begin{bmatrix} 1\,1\,1\,1\,0 \\ 1\,1\,1\,1\,0 \\ 1\,1\,1\,1\,0 \\ 1\,1\,1\,1\,0 \\ 1\,1\,1\,1\,0 \end{bmatrix}$	$\begin{bmatrix} 1\,1\,1\,1\,0 \\ 1\,1\,1\,0\,1 \\ 1\,1\,0\,1\,1 \\ 1\,0\,1\,1\,1 \\ 0\,1\,1\,1\,1 \end{bmatrix}$	0.050	0.113	0.154	0.176	0.188	0.195	0.198	0.199

3.3.2. Size Expansion

The proposed model employs PBVCS as a building block. The size expansion of the proposed scheme partially relies on the choosen PBVCS. In addition, unlike ordinary VCS, the proposed scheme is a TiOSIS, which shares two secret images with two decoding options. The final shadow size is also effected by the information embedding efficiency. With higher information embedding efficiency, we can obtain a smaller shadow size. In this paper, we proposed a TiOSIS based on qGVCS, and we derive the shadow size with different value of q, where $1 \le q \le 8$. With a larger value of q, we can obtain a smaller shadow size. Given grayscale secret image S, processed 8-bit grayscale image B is $2 \times |S|$ bytes if $q < 8$. Otherwise, it is $2 \times |S| \times (1 + 2/256)$ bytes if $q = 8$. Since these grayscale values distribute uniformly and two grayscale values, 254 and 255, are split into double figures. That is

$$|B| = \begin{cases} 2\,|S|\ bytes, & q < 8 \\ \frac{129}{64}|S|\ bytes, & q = 8 \end{cases} \tag{25}$$

Because of the presence of transformation between 8-bit and q-bit, the size of image C is:

$$|C| = \begin{cases} \frac{16\,|S|}{q}\ bytes, & q < 8 \\ \frac{129\,|S|}{8q}\ bytes, & q = 8 \end{cases} \tag{26}$$

Assume there is p_b percentage of black pixels and p_w percentage of white pixels. Obviously, p_b and p_w have the following relationship:

$$p_b + p_w = 1 \tag{27}$$

Define *BHS* to denote the amount of embedded information in binary secret image as below:

Definition 4. *Let BHS denote the hiding space in binary secret image H. Then calculate BHS as follows*:

$$BHS = p_b \times m \times |H| \text{ bits} \tag{28}$$

Noted that one byte of grayscale value is concealed in one bit of black sub-pixels for black secret pixels. For the requirement of concealing information totally, the hiding space in binary secret image H must be larger than image size ∣C∣. Thus, BHS is no less than ∣C∣.

$$p \times \ m \ \times |H| \ \geq \begin{cases} \frac{16|S|}{q}, & q < 8 \\ \frac{129|S|}{8q}, & q = 8 \end{cases} \tag{29}$$

To get size ratio of image H to image S, move both sides of the inequation.

$$\frac{|H|}{|S|} \geq \begin{cases} \frac{16}{qmp_b}, & q < 8 \\ \frac{129}{8qmp_b}, & q = 8 \end{cases} \tag{30}$$

Definition 5. *Let SR denote size ratio of binary secret image H to grayscale secret image S. Use it to measure the size expansion and the information embedding efficiency. Then define SR as below*:

$$SR = \frac{|H|}{|S|} \tag{31}$$

Therefore gain SR of the proposed model:

$$SR \geq \begin{cases} \frac{16}{qmp_b}, & q < 8 \\ \frac{129}{8qmp_b}, & q = 8 \end{cases} \tag{32}$$

It results that SR is inversely proportional to the value q. The reduction of SR means less size expansion is produced in the proposed model, while the reduction in contrast deteriorates visual quality of previewed image. Hence, select a proper value q to make a balance between size expansion and visual quality in practical application.

4. Experimental Results and Discussion

In this section, we introduce experiments about (2, 3)-TiOSIS scheme to support the theoretical conclusion of the proposed model. In addition, we compare this model with the previous SIS schemes.

4.1. Experimental Results

Firstly, we give the experimental results when choosing different value q. Suppose that $k = 2$, $n = 3$ and $q = 7$. A (2, 3)-TiOSIS scheme is built with the grayscale base matrices shown in Equation (3). In addition, a binary secret image is obtained by halftone technique, having connection to the grayscale secret image. Use a typical picture, 'Lena', as the secret image S with 256 × 256 pixels drawn in Figure 3a. Then encode the secret by BSIS scheme based on several XOR operations to acquire Figure 3b. In the mathematical model, we conceal 7-bit grayscale values into three shares generated by (2, 3)-PBVCS. Hence convert the 8-bit grayscale information into 7-bit values as described in Figure 3c. The image is darker with lower grayscale values. This is the final image that hides in three white-and-black shares. We gain three gray shadows described in Figure 4a–c. In the first decryption phase, we stack the transparencies of any two or three shadows to preview the brief structure of grayscale secret image, drawn in Figure 4d–g. In Phase two, we extract the embedded gray information on any two shadows. Convert 7-bit grayscale information in 8-bit gray values. And we decode the information by BSIS method to get a perfect recovered image shown in Figure 4h. Moreover, this recovered image is the same as secret image S.

Pixel expansion m of (2, 3)-PBVCS equals 3, so the size of each shadow image and revealed image H' is three times binary secret image with 308 × 924 pixels. Depending on theoretical analysis of size expansion, SR should be no less than $16/(21p_b)$. Halftone secret image H with 308 × 308 pixels has 50,055 black pixels and 44,809 white pixels. Figure 5 represents the previewed images, corresponding to 8GVCS, 7GVCS, 6GVCS, 5GVCS and 4GVCS. Intuitively, visual quality of restored image using 7GVCS is better than 8GVCS. From Table 1, obtain $\alpha_7 = 0.188$. Therefore, the proposed model improves the contrast of previewed image by 126.5%. Table 2 indicates the size of binary image H for the proposed model. Binary secret image size is lower when q is going up. Also, if parameter n increases, then this size is going down.

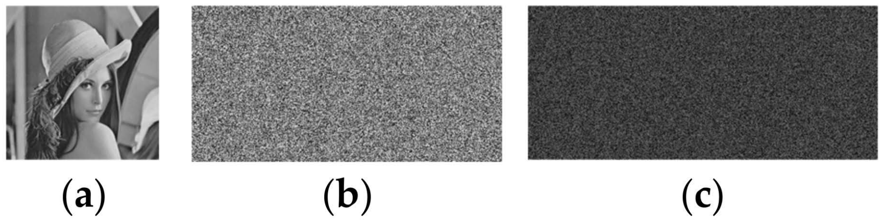

Figure 3. The secret image S and the encoded images. (**a**) The secret image S with 256 × 256 pixels. (**b**) The encoded image B with 256 × 512 pixels. (**c**) The encoded image C with 256 × 585 pixels.

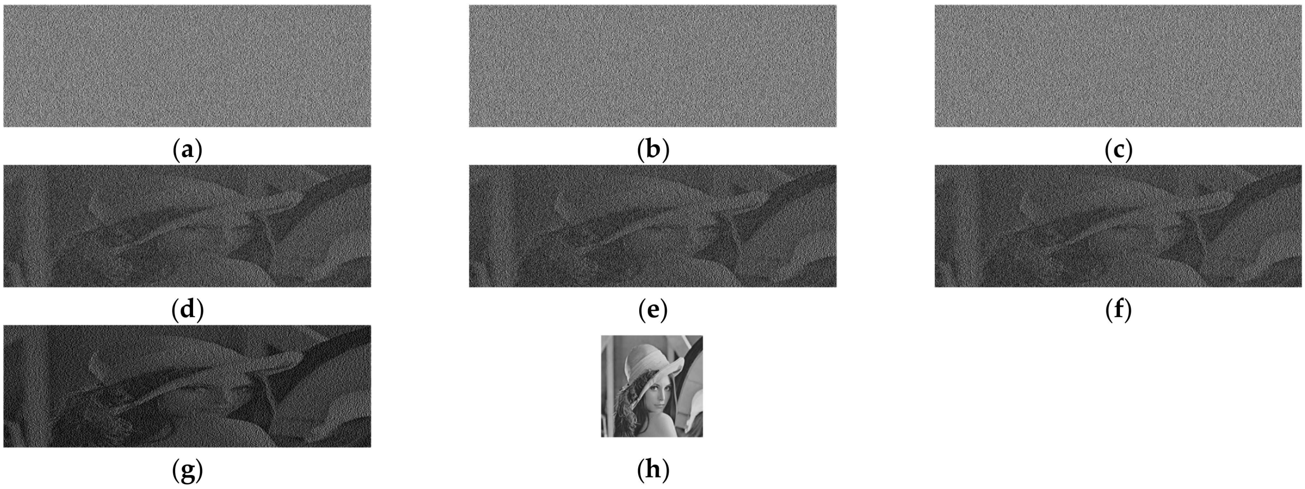

Figure 4. The experiment results of the proposed (2, 3)-TiOSIS scheme. (**a**–**c**) Three generated shadows with 308 × 924 pixels. (**d**–**g**) The revealed image by stacking (**a**,**b**), (**a**,**c**), (**b**,**c**) and (**a**–**c**), separately. (**h**) The recovered secret image S with 256 × 256 pixels.

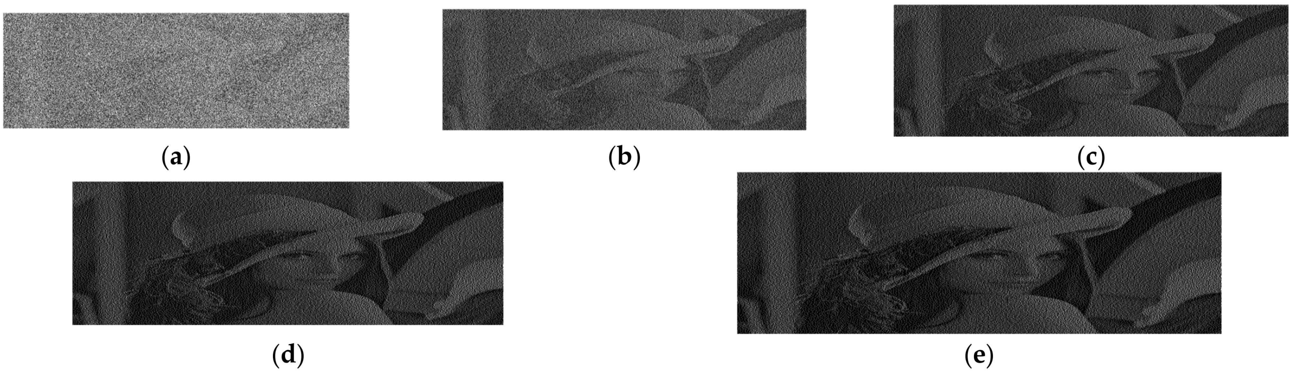

Figure 5. The comparison of the revealed image by (2, 3)-TiOSIS. (**a**) The revealed image of 8GVCS with 290 × 870 pixels. (**b**) The revealed image of 7GVCS with 308 × 924 pixels. (**c**) The revealed image of 6GVCS with 333 × 999 pixels. (**d**) The revealed image of 5GVCS with 365 × 1095 pixels. (**e**) The revealed image of 4GVCS with 408 × 1224 pixels.

Table 2. The size of binary image H for (k, n)-TiOSIS scheme based on qGVCS.

q		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Size of H	(2, 2)	997 × 997	705 × 705	576 × 576	500 × 500	446 × 446	408 × 408	377 × 377	356 × 356
	(2, 3)	814 × 814	576 × 576	470 × 470	408 × 408	365 × 365	333 × 333	308 × 308	290 × 290
	(2, 4)	705 × 705	500 × 500	408 × 408	353 × 353	316 × 316	288 × 288	267 × 267	251 × 251
	(3, 4)	470 × 470	333 × 333	272 × 272	236 × 236	211 × 211	192 × 192	178 × 178	168 × 168

Moreover, Figures 6 and 7 show the contrast and size expansion trend with q changing separately. We can see that as q increases, contrast is going down, meaning that the visual quality of previewed image H' is poorer. Comparing SR trends of $p_b = 0.3$ with $p_b = 0.7$, it can be found that if there are more black pixels in binary image, less size of binary image is used to hide gray information.

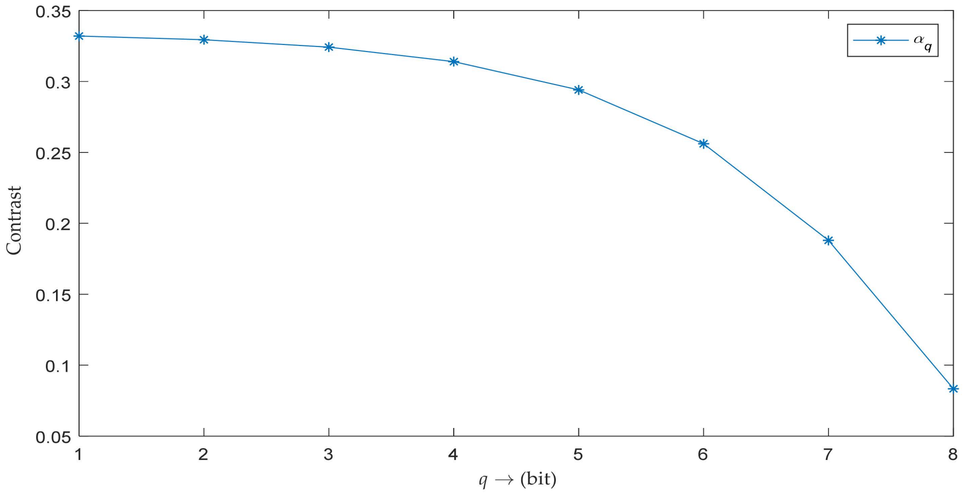

Figure 6. The contrast trend with q changing.

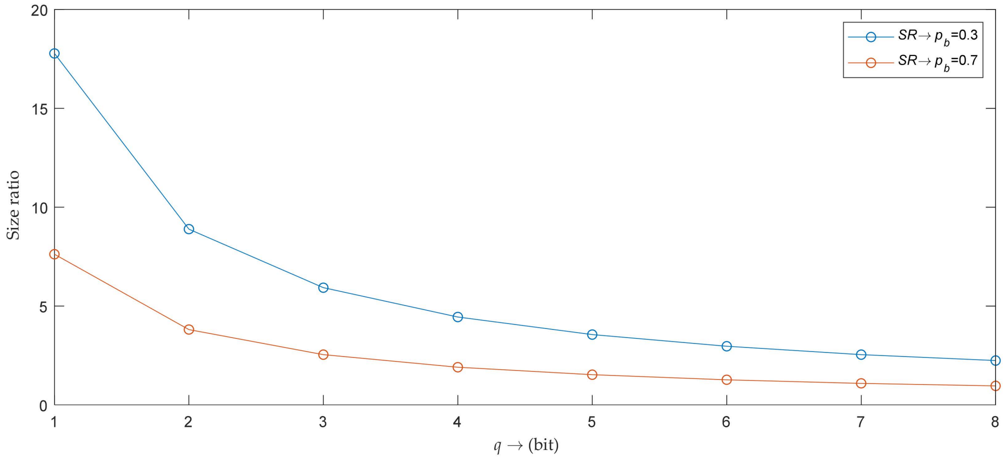

Figure 7. Size expansion (SR) trend with q changing.

4.2. Comparison

For better measuring visual quality of previewed image, structural similarity (SSIM) is utilized as below:

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \tag{33}$$

where

$$\begin{aligned}[l(x,y)]^{\alpha} &= \frac{2\mu_x\mu_y+C_1}{\mu_x^2+\mu_y^2+C_1} \\ [c(x,y)]^{\alpha} &= \frac{2\sigma_x\sigma_y+C_2}{\sigma_x^2+\sigma_y^2+C_2} \\ [s(x,y)]^{\alpha} &= \frac{\sigma_{xy}+C_3}{\sigma_x\sigma_y+C_3}\end{aligned} \tag{34}$$

If two images are the same, then SSIM = 1, or SSIM = 0, if they have no connection completely. Table 3 states SSIM of previewed image and binary secret image comparing the proposed model for $q \in [0, 7]$ with BO-TiOSIS scheme. The variation tendency is consistent with contrast. Table 4 shows the comparison of the proposed model with the previous SIS schemes. It has the advantages of two decoding options, low computation in the second revealing phase and good visual quality of the previewed image.

Table 3. Comparison of the proposed model with BO-TiOSIS scheme in SSIM of previewed image and binary secret image.

Sharing Scheme				**The Proposed Model**				**BO-TiOSIS [28]**
q	1	2	3	4	5	6	7	8
SSIM	0.284	0.283	0.282	0.279	0.271	0.249	0.200	0.126

Table 4. Comparison of the proposed model with the previous SIS schemes.

Sharing Scheme	**Construction**	**Preview**	**Perfect Recovery**	**Computational Complexity**
Naor, Shamir [3]	VCS	YES	NO	-
Thien, Lin [2]	PSIS	NO	YES	$O(n^2)$
Lin, Lin [24]	PSIS + VCS	YES	YES	$O(n^2)$
Yang, Ciou [25]	PSIS + GVCS	YES	YES	$O(n^2)$
Li, Ma [26]	PSIS + GVCS	YES	YES	$O(n^2)$
Li, Yang [28]	BSIS + PBVCS	YES	YES	$O(n)$
Sun, Lu [21]	MSIS [1] + NS	NO	YES	$O(n^2)$
Liu, Lu [30]	PSIS + RGVCS	YES	YES	$O(n^2)$
Proposed scheme	BSIS + qGVCS	YES	YES	$O(n)$

[1] Meaningful secret image sharing.

5. Conclusions

In this paper, we propose a TiOSIS scheme, which shares two secret images with two decoding options. It has two advantages, low computation in the second revealing phase and good visual quality of the previewed image. We also build a mathematical model of the relationship between size expansion and visual quality of previewed image. In practical application, the proposed scheme can be used to fast preview secret image without computation before revealing the perfect grayscale secret image by computation. Further research directions can be focused on reducing shadow size and increasing the information embedding efficiency in shadows.

Author Contributions: Conceptualization, X.W. and P.L.; Formal analysis, X.W. and Z.R.; Methodology, X.W. and P.L.; Writing—original draft, X.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Natural Science Foundation of Hebei Province (Grant number: F2019502173), National Natural Science Foundation of China (Grant number: 61602173) and the Fundamental Research Funds for Central Universities (Grant number: 2019MS116).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

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. Thien, C.C.; Lin, J.C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [CrossRef]
3. Naor, M.; Shamir, A. Visual Cryptography. *Lect. Notes Comput. Sci.* **1994**, *950*, 1–12.
4. Hu, C.M.; Tzeng, W.G. Cheating Prevention in Visual Cryptography. *IEEE Trans. Image Process.* **2007**, *16*, 36–45. [CrossRef]
5. Zhou, Z.; Arce, G.R.; Di, C.G. Halftone visual cryptography. *IEEE Trans. Image Process. A Publ. IEEE Signal. Process. Soc.* **2006**, *15*, 2441–2453. [CrossRef]
6. Li, P.; Yin, L.; Ma, J.F. Visual Cryptography Scheme with Essential Participants. *Mathematics* **2020**, *8*, 838. [CrossRef]
7. Tuyls, P.; Hollmann, H.D.L.; Lint, J.H.V. XOR-based Visual Cryptography Schemes. *Des. Codes Cryptogr.* **2005**, *37*, 169–186. [CrossRef]
8. Chao, K.Y.; Lin, J.C. Secret image sharing: A Boolean-operations-based approach combining benefits of polynomial-based and fast approaches. *Int. J. Pattern Recognit. Artif. Intell.* **2009**, *23*, 263–285. [CrossRef]
9. Guo, S.; Donghui, L.; Dai, Y.; Ren, Y. (k, n) visual cryptography scheme based on XOR decryption. *J. Shanghai Univ.* **2020**, *26*, 21–32.
10. Yang, C.N.; Chen, C.H.; Cai, S.R. Enhanced Boolean-based multi secret image sharing scheme. *J. Syst. Softw.* **2016**, *116*, 22–34. [CrossRef]
11. Wu, X.T.; Yao, P.; An, N. Extended XOR-based Visual Cryptography Schemes by Integer Linear Program. *Signal. Processing* **2021**, *186*, 108122. [CrossRef]
12. Manisha, E. Colour Visual Cryptography (3,3) Scheme. *Turk. J. Comput. Math. Educ. (TURCOMAT)* **2021**, *12*, 3189–3198.
13. Shankar, K.; Taniar, D.; Yang, E.; Yi, O. Secure and Optimal Secret Sharing Scheme for Color Images. *Mathematics* **2021**, *9*, 2360. [CrossRef]
14. Bhagate, S.; Kulkarni, P.J. Improved Extended Progressive Visual Cryptography Scheme Using Pixel Harmonization. *Int. J. Inf. Secur. Priv. (IJISP)* **2021**, *15*, 196–216. [CrossRef]
15. Lin, C.S.; Chen, C.C.; Chen, Y.C. XOR-Based Progressively Secret Image Sharing. *Mathematics* **2021**, *9*, 612. [CrossRef]
16. Cai, H.; Tang, D. Multi Secret Image Sharing Scheme of General Access Structure with Meaningful Shares. *Mathematics* **2020**, *8*, 1582. [CrossRef]
17. Chen, Y.Y.; Huang, B.Y.; Juan, J.S.T. A (k, n)-Threshold Progressive Visual Secret Sharing without Expansion. *Cryptography* **2018**, *2*, 28. [CrossRef]
18. Shyu, S.J.; Ming, C.C. Minimizing Pixel Expansion in Visual Cryptographic Scheme for General Access Structures. *IEEE Trans. Circuits Syst. Video Technol.* **2015**, *25*, 1557–1561. [CrossRef]
19. Yu, L.; Liu, L.; Xia, Z.; Yan, X.; Lu, Y. Lossless and Efficient Secret Image Sharing Based on Matrix Theory Modulo 256. *Mathematics* **2020**, *8*, 1018. [CrossRef]
20. Horng, J.H.; Chen, S.S.; Chang, C.C. A (k, n)-Threshold Secret Image Sharing Scheme Based on a Non-Full Rank Linear Model. *Mathematics* **2022**, *10*, 524. [CrossRef]
21. Sun, Y.; Lu, Y.; Chen, J.; Zhang, W.; Yan, X. Meaningful Secret Image Sharing Scheme with High Visual Quality Based on Natural Steganography. *Mathematics* **2020**, *8*, 1452. [CrossRef]
22. Wu, Z.; Liu, Y.; Jia, X. A Novel Hierarchical Secret Image Sharing Scheme with Multi-Group Joint Management. *Mathematics* **2020**, *8*, 448. [CrossRef]
23. Jiang, Y.; Yan, X.; Qi, J.; Lu, Y.; Zhou, X. Secret Image Sharing with Dealer-Participatory and Non-Dealer-Participatory Mutual Shadow Authentication Capabilities. *Mathematics* **2020**, *8*, 234. [CrossRef]
24. Lin, S.J.; Lin, J.C. VCPSS: A two-in-one two-decoding-options image sharing method combining visual cryptography (VC) and polynomial-style sharing (PSS) approaches. *Pattern Recognit.* **2007**, *40*, 3652–3666. [CrossRef]
25. Yang, C.N.; Ciou, C.B. Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability. *Image Vis. Comput.* **2010**, *28*, 1600–1610. [CrossRef]
26. Li, P.; Ma, P.J.; Su, X.H.; Yang, C.N. Improvements of a two-in-one image secret sharing scheme based on gray mixing model. *J. Vis. Commun. Image Represent.* **2012**, *23*, 441–453. [CrossRef]
27. Li, P.; Yang, C.N.; Kong, Q. Sharing more information in gray visual cryptography scheme. *J. Vis. Commun. Image Represent.* **2013**, *24*, 1380–1393. [CrossRef]
28. Li, P.; Yang, C.N.; Kong, Q. A novel two-in-one image secret sharing scheme based on perfect black visual cryptography. *J. Real-Time Image Process.* **2018**, *14*, 41–50. [CrossRef]
29. Sridhar, S.; Sudha, G.F. Two in One Image Secret Sharing Scheme (TiOISSS) for extended progressive visual cryptography using simple modular arithmetic operations. *J. Vis. Commun. Image Represent.* **2020**, *74*, 102996. [CrossRef]
30. Liu, L.T.; Lu, Y.L.; Yan, X.H. A novel (k_1, k_2, n)-threshold two-in-one secret image sharing scheme for multiple secrets. *J. Vis. Commun. Image Represent.* **2021**, *74*, 102971. [CrossRef]