Article

A Novel XOR-Based Threshold Visual Cryptography with Adjustable Pixel Expansion

Yusheng Guo ¹, Xingxing Jia ^{1,2,*}, Qimeng Chu ¹ and Daoshun Wang ³

¹ School of Mathematics and Statistics, Lanzhou University, Lanzhou 730000, China; guoysh17@lzu.edu.cn (Y.G.); chuqm14@lzu.edu.cn (Q.C.)

² Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541000, China

³ School of Computing, Tsinghua University, Beijing 100084, China; daoshun@mail.tsinghua.edu.cn

* Correspondence: jiaxx@lzu.edu.cn; Tel.: +86-151-1703-3572

Received: 25 December 2019; Accepted: 6 February 2020; Published: 15 February 2020

Abstract: A (k, n) visual cryptography (VC) scheme encodes a secret image into n shadows that are printed on transparencies distributed among a group of n participants secretly, and reveal the secret image by stacking no less than k of them. Its decryption requires no computation and attracts much attention in image security applications. The pixel expansion and contrast are two important characteristics to evaluate the visual quality of the revealed secret image for a (k, n) -VC scheme. The (k, n) XOR-based VC (XVC) schemes can greatly improve the visual quality including both pixel expansion and contrast. Previous methods require complex computation and result in high pixel expansion when they are used to construct such schemes. In this paper, we propose a pixel expansion adjustable (k, n) -XVC scheme, which allows pixel expansion to be changed among $2^{k-1} - 1$ different values. It can ensure each pixel being exactly recovered with the same average contrast no matter it takes any pixel expansion value. The least pixel expansion is much smaller than previous schemes. Our scheme can be easily implemented based on any conventional OR-based (k, n) -VC (OVC) scheme.

Keywords: visual cryptography; XOR; pixel expansion; contrast

1. Introduction

Visual cryptography (VC) was firstly designed by Naor and Shamir in 1994 to share an image secret in visual pattern instead of computational pattern as the traditional secret sharing [1]. It is a new type of secret sharing scheme that encodes an image secret into n seemingly random shadow images and printed them on n transparencies. When k or more of them are stacked together, the secret image will be recognized by the human visual system. This visual decoding method attracted much attention and was used in many applications such as visual image encoding [2–4], visual authentication [5,6], and steganography [7–10], as well as an important solution for secure multimedia content protection on cloud-based media hosting [11–13].

In a (k, n) -VC scheme, each pixel in the secret image is encoded into m subpixels on each shadow image. m is called the pixel expansion. Generally speaking, to minimize the pixel expansion, contrast takes the value $1/m$. Since the pioneering work of [1], much effort has been devoted to putting forward the optimization of VC construction. Most of the VC schemes inherited two drawbacks that are high pixel expansion and low contrast, which results in lower visual quality of the recovered image. Although some methods, including linear coding [1,14], supergraph [15,16], integer linear programming method [17–19], and linear algebraic technique [20,21], formulated the construction of VC schemes as the mathematical model to decrease the pixel expansion, the resulting pixel expansion

m is still large located in $[C_n^k \cdot 2^{k-2} + 1, C_{n-1}^{k-1} \cdot 2^{k-1} + 1]$. The resulting contrast is quite small with a value $1/m$.

A good strategy was proposed to improve the contrast, which introduced the “XOR” operation in recovering the secret [11,19,22–25]. It is investigated that the contrast for a (k, n) -XVC scheme is 2^{k-1} times the contrast for the (k, n) -OVC scheme if the basis matrices of the latter scheme are adopted [26]. The “XOR” operation can be easily run by the special lightweight devices such as smart phone or iPad. It just requires a little computation overload, but it can greatly enhance the contrast compared with the “OR” operation. With the “XOR” operation, some special schemes can greatly improve the contrast. The $(2, n)$ -XVC scheme can even reach contrast being $1/2$ with no pixel expansion [23]. The special (n, n) -XVC scheme has perfect contrast and no pixel expansion [21,23]. Some systematic methods by using linear coding [22], and integer linear programming [25], and linear algebraic [21] were proposed to improve the pixel expansion of a (k, n) -XVC scheme. However, these XVC schemes need complex computation to construct the basis matrices and also suffer from severe pixel expansion problem.

As proved by [26], the basis matrices in a (k, n) -OVC scheme also satisfy the contrast and security conditions of a (k, n) -XVC scheme. Meanwhile, the contrast is 2^{k-1} times enhanced by “XOR” operation. This is also an effective construction method for a (k, n) -XVC scheme. However, it has the same large pixel expansion as a (k, n) -OVC scheme. We propose to use part columns of the basis matrices of (k, n) -OVC scheme to construct a (k, n) -XVC scheme with flexible pixel expansion, and it can reduce the pixel expansion from the least 1 pixel to the largest $2^{k-1} - 1$ pixels at the same time it can keep the same average contrast with the corresponding (k, n) -XVC scheme. It is a deterministic scheme suitable for any secret image. The resulting pixel expansion is still optimal to the related (k, n) -XVC schemes [21,22,25].

The remainder of the article is organized as follows. Section 2 briefly introduces the definitions of a (k, n) -OVC scheme and a (k, n) -XVC scheme, and the relationship between them. The new solution to construct a (k, n) -XVC scheme with adjustable pixel expansion from a (k, n) -XVC scheme is proposed in Section 3. In Section 4, two detailed examples and its experimental images are presented to demonstrate the scheme. Section 5 is the conclusion.

2. Preliminaries

In this section, the preliminary knowledge such as the definitions of a (k, n) -OVC scheme and a (k, n) -XVC scheme are presented. The demonstrative examples are shown separately to explain their related concepts. The relation between them is important to construct our scheme and is shown in this section. Then the motivation about our scheme is shown.

2.1. A (k, n) -OVC Scheme

When a binary secret image is shared in a (k, n) VC scheme, each pixel in the secret image is encoded into m subpixels in each one of the n shadow images that are printed on transparencies. The encoding rule is represented by two $n \times m$ Boolean matrices B_1 and B_0 , whose elements are 1 and 0 denoting black and white subpixels, respectively. A white pixel lets through the light, and a black pixel blocks the light. Two families of basis matrices C_1 (resp. C_0) include all matrices obtained by permuting the columns in B_1 (resp. B_0). When a black (resp. white) pixel is taken from the secret image, one row of the basis matrix B_1 (resp. B_0) in the family C_1 (resp. C_0) is distributed to a related shadow image. Stacking shadows $i_1, \dots, i_r$ together, we obtain the OR-ed (“OR” operation) m -vector being $V = \oplus(i_1, \dots, i_r)$ and “ $\oplus$ ” denotes the “OR” operation for each secret pixel. The gray-level of each secret pixel in the recovered secret image is proportional to Hamming weight (the number of 1s in the vector V) $H(V)$. Let $\oplus(B_i|U)$ denote the Boolean OR-ing of the row j , $j \in U$ of B_i , $i = 0, 1$. Let $|U|$ denote the cardinality of participant set U . The formal definition of (k, n) -OVC scheme is given below [26].

Definition 1 ([26]). With a set of two $n \times m$ Boolean basis matrices, B_0 and B_1 , the result of a column permutation of B_i defines the color of the m subpixels in each one of the n shadows when encoding a pixel $i \in \{0, 1\}$. Such basis matrices constitute a (k, n) -OVC scheme if the following conditions are met.

- (1) Contrast condition: $H(\oplus(B_1|U)) \geq h$ and $H(\oplus(B_0|U)) \leq l$ for $|U| \geq k$, where $0 \leq l < h \leq m$.
- (2) Security condition: $H(\oplus(B_1|U)) = H(\oplus(B_0|U))$ for $|U| \leq k - 1$.

Condition (1) is called contrast condition: it requires that the secret image can be visually recognized by human eyes as the different Hamming weights of black and white colors. The contrast is generally defined as $\alpha = (H(\oplus(B_1|U)) - H(\oplus(B_0|U))) / m$, and it uses the relative difference of the gray levels of the two pixel to represent the visual quality of the recovered secret image. Condition (2) shows the perfect security of a (k, n) -OVC scheme such that any less than k shadows obtains nothing about the secret images. m is the pixel expansion.

The following is a more intuitive description of a (k, n) -OVC scheme through a simple example of a $(2, 2)$ -OVC scheme.

Example 1. The form of B_0 and B_1 is as follows when $n = 2$ and $k = 2$,

$$B_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \text{ and } B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The encoding and decoding process of the shadows is shown below in Table 1.

Table 1. The encoding and decoding process of the shadows in a $(2, 2)$ -OR-based (k, n) -VC (OVC) scheme.

Pixel	Shadow 1	Shadow 2	XOR

The white (resp. black) subpixels in pre-pixel are expressed by ϕW (resp. ϕB); here, ϕ (resp. φ) is the number of white (resp. black) subpixels in a pixel. It is observed that the $(2, 2)$ -VC scheme has perfect security through Example 1. When stacking less than two shadows, all black and white pixels are encoded as 1B1W or 1W1B. We have 2B0W and 1B1W for black and white secret pixels when stacking two shadows. The contrast is $\alpha = 1/2$.

2.2. A (k, n) -XVC Scheme

It is proven that a (k, n) -XVC scheme has higher contrast and lower pixel expansion than the (k, n) -OVC scheme [25,26]. It simply requires that the decryption of the secret from the shadows are assisted by the small, cheap, and lightweight computational devices, which can be flexibly connected through the internet network. When such mobile devices are available, a (k, n) -XVC schemes can be widely adopted to substitute a (k, n) -OVC scheme. Many schemes focused on a (k, n) -XVC scheme to decrease the construction complexity [21,23–26]. Let “ $\otimes$ ” denote the Boolean “XOR” operation and $\otimes(B_i|U)$ denote the Boolean XOR-ing of the row j , $j \in U$ of B_i , $i = 0, 1$. The formal definition of a (k, n) -XVC scheme is presented as follows [26].

Definition 2 ([26]). With a set of two $n \times m$ Boolean basis matrices, B_0 and B_1 , the result of a column permutation of B_i defines the color of the m subpixels in each one of the n shadows when encoding a pixel $i \in \{0, 1\}$. Such basis matrices constitute a (k, n) -XVC scheme if the following conditions are met.

- (1) *Contrast Condition*: $H(\otimes(B_1|U)) \geq h'$ and $H(\otimes(B_0|U)) \leq l'$ for $|U| = k$, where $0 \leq l' < h' \leq m$.
 (2) *Security Condition*: $H(\otimes(B_1|U)) = H(\otimes(B_0|U))$ for $|U| \leq k - 1$.

It is analogous to Section 2.1. The following is a more intuitive description of a (k, n) -XVC scheme through a simple example of a $(2, 2)$ -XVC scheme.

Example 2. The form of B_0 and B_1 is as follows when $n = 2$ and $k = 2$.

$$B_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \text{ and } B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

The encoding and decoding process of the shadows is shown below in Table 2.

Table 2. The encoding and decoding process of the shadows in a $(2, 2)$ -XVC scheme.

Pixel	Shadow 1	Shadow 2	XOR

Similar to the analysis in Section 2.1, the $(2, 2)$ -XVC scheme has perfect security. When stacking one shadow, all black and white pixels are 1B1W. We have 2B0W and 0B2W for black and white secret pixels when stacking two shadows. The contrast is $\alpha = 1/2$, which is 2^{k-1} times of the contrast in Section 2.1.

2.3. Motivation

A (k, n) -XVC scheme provides a simple way to greatly increase the contrast of a (k, n) -OVC scheme from Examples 1 and 2. It provides the possibility to reveal secret image on lightweight equipments, such as mobile phone and iPad, which can be used in the transmission of the secret images, security authentication, and access control. A (k, n) -XVC scheme greatly enhances the utility and flexibility of secret image sharing. However, it requires the same pixel expansion as a (k, n) -OVC scheme. Yang [26] proved that the contrast of a (k, n) -XVC scheme is 2^{k-1} times better than that of a (k, n) -OVC scheme if two kind of schemes are built based on the same basis matrix of a (k, n) -OVC scheme. Yang's specific conclusion is described in Theorem 1.

Theorem 1 (Theorem 1 in [26]). *Basis matrices satisfying the conditions of Definition 1 also satisfy the conditions of Definition 2. The relative difference of the gray levels of the recovered white and black pixels is $h' - l' = 2^{k-1}(h - l)$, where l and h (resp. l' and h') are the gray levels of recovered white and black pixels for a (k, n) -OVC (resp. a (k, n) -XVC) scheme, respectively.*

Yang's conclusion gives us such inspiration; we can construct a new (k, n) scheme by replacing "OR" operation with "XOR" operation directly without changing the basis matrices. Although the pixel expansion of the two schemes is the same, the contrast of a (k, n) -XVC scheme is enhanced 2^{k-1} times than that of a (k, n) -OVC scheme. To solve the problem of pixel expansion in a (k, n) -XVC scheme, we can allow the difference of the gray levels of recovered white and black pixels to be changed among the interval $[1, 2^{k-1}]$. To ensure such revealing condition, the corresponding new basis matrices can take any $m - 2^{k-1} + 1$ columns to any m columns in the original basis matrices of a (k, n) -OVC scheme. This process allows pixel expansion to be changed among a lightly large interval, and it can ensure each pixel being exactly recovered with the same average contrast no matter it takes any pixel expansion.

The least pixel expansion $m - 2^{k-1}m\alpha + 1$ is much smaller than that of the previous schemes. Our scheme can be easily implemented on any conventional (k, n) -OVC scheme.

3. The Proposed (k, n) -XVC Scheme with Adjustable Pixel Expansion

In this part, we propose a (k, n) -XVC scheme with adjustable pixel expansion being m' , which is built on any (k, n) -OVC scheme with pixel expansion m denoted as $(k, n)_m$ -OVC scheme. We denote the proposed scheme as a $(k, n)_{m'}$ -XVC scheme. It greatly improves the contrast and allows pixel expansion to be changed among a lightly large interval $[m - 2^{k-1}m\alpha + 1, m]$. It can ensure each pixel being exactly recovered with the same average contrast no matter it takes any pixel expansion. The least pixel expansion is much smaller than previous schemes.

3.1. The Proposed Scheme

Given a (k, n) -OVC scheme with basis matrices B_0 and B_1 , its pixel expansion is m . The scheme meets the contrast and security conditions:

$$H(\oplus(B_1|U)) \geq h \text{ and } H(\oplus(B_0|U)) \leq l, |U| \geq k, \quad (1)$$

$$H(\oplus(B_1|U)) = H(\oplus(B_0|U)), |U| \leq k - 1, \quad (2)$$

where $0 \leq l < h \leq m$. The contrast is $\alpha = (h - l)/m$. According to the contrast condition, it is known that $\alpha m = \frac{h-l}{m}m = h - l \geq 1$.

Next, we will give the construction of $(k, n)_{m'}$ -XVC scheme, the shadows of the proposed scheme is presented in Construction 1.

Construction 1: the proposed $(k, n)_{m'}$ -XVC scheme.

Input: the secret image S , the basis matrices B_0, B_1 and m of a (k, n) -OVC scheme.

Output: shadows $S_i, i = 1, 2, \dots, n$.

Construction procedure: 1. The dealer takes a expected pixel expansion $m' \in [m - 2^{k-1}m\alpha + 1, m]$;
2. When encoding a white (resp. black) pixel, the dealer randomly chooses a $n \times m'$ column matrix in B_0 (resp. B_1), and do random column permutation on it. The resulting matrix is denoted as B'_0 (resp. B'_1). The i -row of B'_0 (resp. B'_1) is assigned to a relative shadow S_i , where

$$B'_0 = B_0[i_1, \dots, i_{m'}], \quad B'_1 = B_1[j_1, \dots, j_{m'}].$$

Here, the shadow S_i is sent to participant U_i ; And the $B_0[i_1, \dots, i_{m'}]$ denotes the any m' columns of B_0 . $B_1[j_1, \dots, j_{m'}]$ denotes the another any m' columns of B_1 . The chosen columns and their orders are completely independent.

3.2. Contrast of the Proposed Scheme

To demonstrate that the proposed $(k, n)_{m'}$ -XVC scheme is an effective (k, n) -XVC scheme, we first prove that the contrast condition is satisfied. When any k rows of the basis matrices are superimposed, contrast α' of the proposed scheme must be large than 0. As the any m' columns are randomly chosen, we use average contrast to describe the visual quality of the recovered secret image. Then, we prove that the average contrast of the scheme is equal in Theorem 2 no matter whatever pixel expansion is taken.

Theorem 2. Construction 1 above is a (k, n) -XVC scheme. The pixel expansion is $m' \in [m - 2^{k-1}m\alpha + 1, m]$ and the average contrast is

$$\bar{\alpha} = 2^{k-1}\alpha \quad (3)$$

for $|U| = k$, if a original (k, n) -OVC scheme has pixel expansion m and contrast α , where $m\alpha \geq 1$.

Before proving the theorem, we will give some description and notations. For any basis matrices B_0 and B_1 of a (k, n) -OVC scheme, it satisfies the relationship:

$$H(\oplus(B_1|U)) - H(\oplus(B_0|k)) = h - l = m\alpha \geq 1, \quad (4)$$

$$H(\otimes(B_1|k)) - H(\otimes(B_0|U)) = h' - l' = 2^{k-1}m\alpha. \quad (5)$$

When any k rows are superimposed, the secret image will be revealed with contrast α and $2^{k-1}\alpha$ when “OR” and “XOR” operation are used, separately. The XORing results of any rows in U of B_0 and B_1 can be represented in the following form regardless of the arrangement order:

$$\otimes(B_0|U) = (\underbrace{0, 0, \dots, 0}_{h' - l'}, \underbrace{1, 1, \dots, 1}_{l'}, \underbrace{0, 0, \dots, 0}_{m - h'}), \quad (6)$$

$$\otimes(B_1|U) = (\underbrace{1, 1, \dots, 1}_{h' - l'}, \underbrace{1, 1, \dots, 1}_{l'}, \underbrace{0, 0, \dots, 0}_{m - h'}). \quad (7)$$

for $|U| = k$. When $|U| < k$, the above relationship has the following form:

$$\otimes(B_0|U) = (\underbrace{0, 0, \dots, 0}_{m - p}, \underbrace{1, 1, \dots, 1}_p), \quad (8)$$

$$\otimes(B_1|U) = (\underbrace{0, 0, \dots, 0}_{m - q}, \underbrace{1, 1, \dots, 1}_q). \quad (9)$$

Proof. First, we show the scheme satisfies the contrast condition and compute the average contrast. The basis matrices, B'_0 and B'_1 , of the proposed $(k, n)_{m'}$ -XVC scheme are composed of m' column vectors randomly selected from the basis matrices B_0 and B_1 are denoted as

$$B'_0 = B_0[i_1, \dots, i_{m'}], \text{ and } B'_1 = B_1[j_1, \dots, j_{m'}].$$

The XORing results of any rows in U of B'_0 and B'_1 can be represented in the following form regardless of the arrangement order:

$$\otimes(B'_0|U) = (\underbrace{0, 0, \dots, 0}_{m' - x}, \underbrace{1, 1, \dots, 1}_x), \quad (10)$$

$$\otimes(B'_1|U) = (\underbrace{0, 0, \dots, 0}_{m' - y}, \underbrace{1, 1, \dots, 1}_y). \quad (11)$$

Considering the Hamming weight of $\otimes(B'_1|U)$ (resp. $\otimes(B'_0|U)$), we need only determine $H(\otimes(B'_0|U))$ (resp. $H(\otimes(B'_1|U))$) with $|U| = k$. Considering the extreme situation, $\otimes(B'_1|U)$ has the least “1”s of $\otimes(B_1|U)$ and $\otimes(B'_0|U)$ has the most ‘1’s of $\otimes(B_0|U)$. In such situation, if the contrast condition is satisfied, then all other possible basis matrices B'_1 and B'_0 must satisfy the contrast condition. Applying (6) and (7), the extreme situation of basis matrices has the following XORing results if any rows in U of B'_0 and B'_1 are XORed, regardless of the arrangement order of the elements.

$$\otimes(B'_0|U) = (\underbrace{0, 0, \dots, 0}_{m' - l'}, \underbrace{1, 1, \dots, 1}_{l'}), \quad (12)$$

$$\otimes(B'_1|U) = (\underbrace{1, 1, \dots, 1}_{m' - m + h'}, \underbrace{0, 0, \dots, 0}_{m - h'}). \quad (13)$$

Because $m' - m + h' > l'$, we have $H(\otimes(B'_1|U)) > H(\otimes(B'_0|U))$. The contrast condition is obtained.

Next, we compute the average contrast. According to (10) and (11), we denote $x = H(\otimes(B'_0|U))$ and $y = H(\otimes(B'_1|U))$ for any participant set U with $|U| = k$. From (7) and (13), we obtain

$$m' - m + h' \leq y \leq \min\{h', m'\}. \quad (14)$$

From (6) and (12), we obtain

$$\max\{0, m' - m + l'\} \leq x \leq l'. \quad (15)$$

x and y conform to hypergeometric distribution, we have

$$\Pr[H(\otimes(B'_0|U)) = x] = \frac{\binom{l'}{x} \binom{m-l'}{m'-x}}{\binom{m}{m'}} \quad (16)$$

$$\Pr[H(\otimes(B'_1|U)) = y] = \frac{\binom{h'}{y} \binom{m-h'}{m'-y}}{\binom{m}{m'}} \quad (17)$$

$$E[x] = \frac{m'l'}{m} \quad (18)$$

$$E[y] = \frac{m'h'}{m} \quad (19)$$

We denote $E[x]$ and $E[y]$ as $\bar{x}$ and $\bar{y}$, respectively. They are the average Hamming weight of B'_0 and B'_1 . Therefore, the average contrast is

$$\bar{\alpha} = \frac{\bar{y} - \bar{x}}{m'} = 2^{k-1}\alpha. \quad (20)$$

Then, we show the scheme satisfies security condition. When $|U| \leq k$, $\otimes(B_0|r)$ and $\otimes(B_1|r)$ have the form (8) and (9), separately, it requires $p = q$. The Hamming weights of B'_0 and B'_1 by XOR-ing any rows in U are $H(\otimes(B'_0|U))$ and $H(\otimes(B'_1|U))$, satisfying the relationships (10) and (11). The difference lies that $|U| < k$. Naturally, Equations (16)–(19) hold for $H(\otimes(B'_0|U))$ and $H(\otimes(B'_1|U))$ only through replacing l' and h' by p and q , respectively. Therefore, we have $\bar{x} = \bar{y}$ due to $p = q$. We have $H(\otimes(B'_0|U)) = H(\otimes(B'_1|U))$ for $|U| \leq k - 1$. The security condition is obtained. $\square$

4. Experimental Results and Analysis

We designed two different experiments for the proposed scheme to demonstrate the construction process and effectiveness of our approach. The overall performance is compared with the state-of-the-art schemes shown in Section 4.2.

4.1. Experimental Results

In this subsection, we give two different schemes to show the visual quality of the recovered images with different pixel expansion.

Experiment 1: This experiment is about a $(3,5)_4$ -XVC scheme. It is constructed by a $(3,5)$ -OVC scheme with basis matrices

$$B_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

and

$$B_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Its pixel expansion is $m = 8$ and the contrast is $\alpha = 1/8$ in a $(3,5)$ -OVC scheme. To decrease the pixel expansion, we take $m' = 4$ to construct a $(3,5)_4$ -XVC scheme. The contrast is $\alpha' = 1/2$. Its shadow images and reconstructed secret images are shown in Figure 1. It is easy to verify the security condition is satisfied. Superimposing two shadows leaks no information about the secret image, which is shown in Figure 1g–i. The secret image can be revealed by superimposing any three shadows, which is shown in Figure 1j–l. The contrast condition is satisfied.

Figure 1. The shadow images and reconstructed images for a $(3, 5)$ -XVC scheme: (a) secret image, (b) shadow S_1 , (c) shadow S_2 , (d) shadow S_3 , (e) shadow S_4 , (f) shadow S_5 , (g) $S_1 \otimes S_2$, (h) $S_3 \otimes S_2$, (i) $S_2 \otimes S_5$, (j) $S_1 \otimes S_2 \otimes S_3$, (k) $S_2 \otimes S_3 \otimes S_4$, (l) $S_3 \otimes S_4 \otimes S_5$.

It can be seen that the proposed $(3,5)_4$ -XVC scheme keeps the same contrast with that of the $(3,5)$ -XVC scheme, and furthermore reduces the pixel expansion. Relative to a $(3,5)$ -OVC scheme, the visual quality of the recovered image is greatly improved.

Experiment 2: The other experiment is regarding a $(4,5)_6$ -XVC scheme. This example aims to show that the proposed scheme with different pixel expansion still shows good visual quality of the recovered image. It is constructed by a $(4,5)$ -OVC scheme with basis matrices

$$B_0 = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

and

$$B_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Its pixel expansion is $m = 15$, and the contrast is $\alpha = 1/15$ in a $(4,5)$ -OVC scheme. To decrease the pixel expansion, we take $m' = 6$ to construct a $(4,5)_6$ -XVC scheme. The contrast is $\alpha' = 8/15$. Its shadows and reconstructed secret images are shown in Figure 2. It is easy to verify that the security

condition is satisfied. Superimposing two shadows or three shadows leaks no information about the secret image, which is shown in Figure 2g–l. The secret image can be revealed by superimposing any four shadows, which is shown in Figure 2m–o. The contrast condition is satisfied.

It can be seen that the proposed $(4,5)_6$ -XVC scheme keeps the same contrast with that of a $(4,5)$ -XVC scheme, and furthermore reduces the pixel expansion. Relative to the $(4,5)$ -OVC scheme, the visual quality of the recovered image is greatly improved.

Figure 2. The shadow images and reconstructed images for $(4,5)$ -XVC scheme: (a) secret image, (b) shadow S_1 , (c) shadow S_2 , (d) shadow S_3 , (e) shadow S_4 , (f) shadow S_5 , (g) $S_1 \otimes S_2$, (h) $S_3 \otimes S_4$, (i) $S_2 \otimes S_5$, (j) $S_1 \otimes S_3 \otimes S_4$, (k) $S_2 \otimes S_3 \otimes S_4$, (l) $S_3 \otimes S_4 \otimes S_5$, (m) $S_1 \otimes S_2 \otimes S_3 \otimes S_4$, (n) $S_1 \otimes S_2 \otimes S_4 \otimes S_5$, (o) $S_2 \otimes S_3 \otimes S_4 \otimes S_5$.

4.2. Performance Comparison with the Related Schemes

The performance of the proposed scheme is compared with other important (k,n) -XVC schemes in terms of pixel expansion and contrast. The state-of-the-art schemes [21,22,25] formulated the different constructions of the existing (k,n) -XVC schemes. We compare the experimental $(3,5)$ -XVC scheme and $(4,5)$ -XVC scheme with three other schemes. The results are shown in Table 3. We can see that our scheme keeps the high unchanged contrast, and, at the same time, it allows the pixel expansion to change among a slight large interval. Only the scheme in [21] has perfect contrast, but it reveals the secret image on a fraction of the recovered image. The proposed scheme does not need any mathematical model to compute the basis matrices, it can be built on any existing (k,n) -OVC scheme. However, the schemes in [22,25] require complex computation by using linear coding or integer linear programming. Although the proposed scheme uses average contrast to represent the visual quality of the revealed secret image, it can recover each pixel of the secret image deterministically. It provides a good strategy to improve the image quality of the VC scheme.

Table 3. The pixel expansion and contrast comparison.

Scheme	(3,5)-XVC Scheme		(4,5)-XVC Scheme	
	m	α	m	α
Scheme in [22]	≥ 8	$1/m$	≥ 15	$1/m$
Scheme [21]	8	1	15	1
Scheme in [25]	8	$1/8$	15	$1/15$
Ours	5~8	$1/2$	8~15	$8/15$

5. Conclusions

In this paper, we propose a novel strategy to construct a (k,n) -XVC scheme. It is built on any existing (k,n) -OVC scheme. It can enhance the contrast by 2^{k-1} times from its original scheme. More importantly, it allows the pixel expansion to change among an interval $[m - 2^{k-1}m\alpha + 1, m]$. The proposed scheme is a deterministic scheme with the high unchanged contrast $2^{k-1}\alpha$ regardless

of if it takes any pixel expansion. The security and contrast conditions are proved by theoretical analysis. $2^{k-1} - 1$ different choices of pixel expansion provides many different potential applications for VC schemes.

Author Contributions: Y.G. and X.J. conceived the experiments and completed the paper written. Y.G. and Q.C. presented the scheme construction. D.W. analyzed the scheme rationality. Q.C. and X.J. searched related articles. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported in part by the National Natural Science Foundation Nos. 61902164, 61972225, 61601358, and 41807150; in part by Guangxi Key Laboratory of Trusted Software No. KX201907 and the Science and Technology Foundation of Guangxi No. AA17204096; and in part by the Key Laboratory of Digital Content Anti-Counterfeiting and Security, Forensics of State Administration of Press, Publication, Radio, Film and Television (SAPPRFT).

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Naor, M.; Shamir, A. Visual cryptography. In *Cryptography: Proceedings of the Workshop on Cryptography Advances in Cryptology—EUROCRYPT '94*, 1994; Beth, T., Ed.; Springer: Berlin/Heidelberg, Germany, 1994; pp. 1–12.
2. Liu, F.; Wu, C.; Lin, X. Step Construction of Visual Cryptography Schemes. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 27–38.
3. Yan, X.; Lu, Y. Generalized general access structure in secret image sharing. *J. Vis. Commun. Image Represent.* **2019**, *58*, 89–101. [\[CrossRef\]](#)
4. Wu, X.; Yang, C.N. A combination of color-black-and-white visual cryptography and polynomial based secret image sharing. *J. Vis. Commun. Image Represent.* **2019**, *61*, 74–84. [\[CrossRef\]](#)
5. Naor, M.; Pinkas, B. Visual authentication and identification. In *Cryptography: Proceedings of the Workshop on Cryptography Advances in Cryptology—Crypto'97*, 1997; Beth, T., Ed.; Springer: Berlin/Heidelberg, Germany, 1997; pp. 322–336.
6. Yang, C.N.; Ouyang, J.F.; Harn, L. Steganography and authentication in image sharing without parity bits. *Opt. Commun.* **2012**, *285*, 1725–1735. [\[CrossRef\]](#)
7. Qiao, T.; Shi, R.; Luo, X.; Xu, M.; Zheng, N.; Wu, Y. Statistical Model-Based Detector via Texture Weight Map: Application in Re-Sampling Authentication. *IEEE Trans. Multimed.* **2019**, *21*, 1077–1092. [\[CrossRef\]](#)
8. Zhang, Y.; Luo, X.; Guo, Y.; Qin, C.; Liu, F. Multiple Robustness Enhancements for Image Adaptive Steganography in Lossy Channels. *IEEE Trans. Circuits Syst. Video Technol.* **2019**. [\[CrossRef\]](#)
9. Wang, J.; Li, T.; Luo, X.; Shi, Y.; Jha, S.K. Identifying Computer Generated Images Based on Quaternion Central Moments in Color Quaternion Wavelet Domain. *IEEE Trans. Circuits Syst. Video Technol.* **2019**, *29*, 2775–2785. [\[CrossRef\]](#)
10. Wang, J.; Wang, H.; Li, J.; Luo, X.; Shi, Y.; Jha, S.K. Detecting double JPEG compressed color images with the same quantization matrix in spherical coordinates. *IEEE Trans. Circuits Syst. Video Technol.* **2019**. [\[CrossRef\]](#)
11. Singh, P.; Raman, B.; Misra, M. A (n, n) threshold non-expansible XOR based visual cryptography with unique meaningful shares. *Signal Process.* **2018**, *142*, 301–319. [\[CrossRef\]](#)
12. Song, J.; Liu, Y.; Shao, J.; Tang, C. A Dynamic Membership Data Aggregation (DMDA) Protocol for Smart Grid. *IEEE Syst. J.* **2019**. [\[CrossRef\]](#)
13. Liu, Y.; Zhao, Q. E-voting scheme using secret sharing and K-anonymity. *World Wide Web* **2019**, *22*, 1657–1667. [\[CrossRef\]](#)
14. Bose, M.; Mukerjee, R. Optimal (k, n) visual cryptographic schemes for general k. *Des. Codes Cryptogr.* **2010**, *55*, 19–35. [\[CrossRef\]](#)
15. Guo, T.; Zhou, L. Constructing Visual Cryptography Scheme by Hypergraph Decomposition. *Procedia Comput. Sci.* **2018**, *131*, 336–343. [\[CrossRef\]](#)
16. Yang, C.N.; Wu, F.H.; Peng, S.L. Enhancing multi-factor cheating prevention in visual cryptography based minimum (k, n)-connected graph. *J. Vis. Commun. Image Represent.* **2018**, *55*, 660–676. [\[CrossRef\]](#)

17. Droste, S. New Results on Visual Cryptography. In *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*; Springer-Verlag: Berlin/Heidelberg, Germany, 1996.
18. Shyu, S.J.; Chen, M.C. Optimum Pixel Expansions for Threshold Visual Secret Sharing Schemes. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 960–969. [[CrossRef](#)]
19. Jia, X.; Wang, D.; Chu, Q.; Chen, Z. An efficient XOR-based verifiable visual cryptographic scheme. *Multimed. Tools Appl.* **2019**, *78*, 8207–8223. [[CrossRef](#)]
20. Adhikari, A. Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images. *Des. Codes Cryptogr.* **2014**, *73*, 865–895. [[CrossRef](#)]
21. Shen, G.; Liu, F.; Fu, Z.; Yu, B. Perfect contrast XOR-based visual cryptography schemes via linear algebra. *Des. Codes Cryptogr.* **2016**, *85*, 1–23. [[CrossRef](#)]
22. Tuyls, P.; Hollmann, H.D.L.; Lint, J.H.V.; Tolhuizen, L. XOR-based Visual Cryptography Schemes. *Des. Codes Cryptogr.* **2005**, *37*, 169–186. [[CrossRef](#)]
23. Wang, D.; Zhang, L.; Ma, N.; Li, X. Two secret sharing schemes based on Boolean operations. *Pattern Recogni.* **2007**, *40*, 2776–2785. [[CrossRef](#)]
24. Wu, X.; Sun, W. Extended Capabilities for XOR-Based Visual Cryptography. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1592–1605. [[CrossRef](#)]
25. Shyu, S.J. XOR-based Visual Cryptographic Schemes with Monotonously Increasing and Flawless Reconstruction Properties. *IEEE Trans. Circuits Syst. Video Technol.* **2017**, *28*, 2397–2401. [[CrossRef](#)]
26. Yang, C.N.; Wang, D.S. Property Analysis of XOR-Based Visual Cryptography. *IEEE Trans. Circuits Syst. Video Technol.* **2014**, *24*, 189–197. [[CrossRef](#)]

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).