engineering proceedings

MDPI

Proceeding Paper

RG-Based (*k*, *n*)-Threshold Visual Cryptography with Abilities of OR and XOR Decryption †

Yu-Ru Lin and Justie Su-Tzu Juan *

Department of Computer Science and Information Engineering, National Chi Nan University, Nantou 545, Taiwan; s111321509@mail1.ncnu.edu.tw

* Correspondence: jsjuan@ncnu.edu.tw

† Presented at the IEEE 5th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability, Tainan, Taiwan, 2–4 June 2023.

Abstract: A (*k*, *n*) visual cryptography (VCS) is used to build a system for secret sharing. The system divides a secret image (*S*) into *n* shares and recovers *S* by stacking shares bigger than or equal to *k*, while shares below *k* provide no information about *S*. The fundamental idea of VCS is that, rather than relying on mathematical or cryptographic skills, human vision can be used to decrypt the secret image. Typically, a Boolean OR operation can be used to indicate the stacking action in a VCS. The reconstructed secret image gradually darkens as more shares are stacked. However, this intractable issue can be overcome by designing an XOR-based VCS that uses the Boolean XOR operator rather than the OR operation. This indicates that by using the XOR-based VCS, higher image quality can be attained. Because the XOR operation requires the use of additional equipment, scholars consider that when no equipment is available, the traditional OR operation can still be used to reveal the secret images. That is, the secret image can be decrypted without a computing device by stacking enough shares, and if a lightweight computing device is available, a better-quality image can be produced via an XOR operation. In 2015, an RG-based (*k*, *n*) VCS to restore the secret image by using an OR or XOR operation was proposed. In this study, we improve the scheme and design a new (*k*, *n*) VCS, called (*k*, *n*) 2D_VCS to encrypt a secret image into *n* shares. The secret image can be recovered when *k* or more shares are gathered and stacked (OR operation) together or when an XOR procedure is utilized. Both the theoretical proof and experimental results show that the quality of the restored image obtained by our method is better than that of the previous methods.

Keywords: secret sharing scheme; visual cryptography; (*k*, *n*)-threshold; XOR operation; random grids

Citation: Lin, Y.-R.; Juan, J.S.-T. RG-Based (*k*, *n*)-Threshold Visual Cryptography with Abilities of OR and XOR Decryption. *Eng. Proc.* **2023**, *55*, 65. https://doi.org/10.3390/engproc2023055065

Academic Editors: Teen-Hang Meen, Kuei-Shu Hsu and Cheng-Fu Yang

Published: 7 December 2023

1. Introduction

The Visual Cryptography Scheme (VCS) was suggested in 1995 for distributing secrets [1]. A binary secret image can be recovered by encrypting it into *n* random images (shares) and then stacking those *n* shares. They also developed a threshold *k*-out-of-*n* VCS method, (*k*, *n*)-threshold VCS. Encrypting a secret image in binary into *n* shares and then stacking any *k* or more than *k* shares ($k \leq n$) can reconstruct the secret image. Fewer than *k* shares cannot provide any clues about the binary secret image.

Visual secret sharing (VSS) by random grids (RG) was introduced by Kafri and Keren in 1987 [2]. It eliminates the secret pixel expansion issue, and this approach does not demand codebook designs, which is the disadvantage of Naor and Shamir's scheme [1]. Random grids mean that we obtain every pixel by randomly selecting between 1 (opaque or black) and 0 (transparent or white). In 2009, Shyu gave a scheme of (*n*, *n*) RG-based VCS [3]. Chen and Tsao constructed a (*k*, *n*) RG-based VCS [4]. Then, Guo, Liu, and Wu improved Chen and Tsao's scheme in 2013 [5]. The stacking operation in a VCS is denoted by a Boolean OR operation. However, the more shares of stacking, the darker the reconstructed

image. An XOR-based VCS can solve this problem, as a better recovered image quality can be obtained when using an XOR operation instead of an OR operation. A new idea was suggested in Ref. [6]. In their method, OR or XOR is optionally used to restore the secret image when restoring the binary secret image. As a result, the secret image can be restored when computing resources are limited by stacking k or more shares (using an OR operation). When computing resources are available, a secret image of higher quality can be obtained (using an XOR operation). We improved their scheme by designing a new (k, n) VCS that can also extract binary secret images by OR or XOR operations and achieved a better quality of restored images than their scheme.

This paper is structured as follows. The related work is presented in the next section, the suggested scheme, (k, n) 2D_VCS is presented in Section 3, and an analysis of the (k, n) 2D_VCS is shown in Section 4. Sections 5 and 6 show the experimental results and conclusion, respectively.

2. Related Work

2.1. (2, 2) RG-Based VCS

In 1987, Kafri and Keren firstly proposed (2, 2) RG-based VCS [2], Algorithm 1, to encrypt a binary image S, and their algorithm output two shares B_1 and B_2, which looked like random grids. After superimposing them, the secret image S was reconstructed by using the Human Visual System (HVS) without specific computational and cryptographic knowledge.

Algorithm 1 KK [2]

Input:	Secret binary image S.
Output:	Two shares B_1, B_2.
Step 1.	Generate the first share B_1 randomly selecting 0 or 1 for each pixel of B_1.
Step 2.	Based on the pixels $S[i, j]$ of S and the pixel $B_1[i, j]$ of B_1, the pixel value $B_2[i, j]$ of share B_2 is calculated by $B_2[i, j] = \begin{cases} B_1[i, j], \ if \ S[i, j] = 0 \\ \overline{B_1[i, j]}, \ if \ S[i, j] = 1 \end{cases}$.

2.2. (k, n) RG-Based VCS

As mentioned above, a scheme of (k, n) RG-based VCS, Algorithm 2, was proposed in 2011 [4]. For comparison with the proposed scheme, we rewrite their algorithm as follows. Note that it is essentially the same as their original algorithm.

Algorithm 2 CT [4]

Input:	A secret binary image S.
Output:	n shares $(B_1, B_2, \ldots, B_n)$.
Step 1.	For each position $[i, j]$, repeat Steps 2–4:
Step 2.	Randomly select from $\{0, 1\}$ to generate n random pixels $b_1, b_2, \ldots, b_n$.
Step 3.	If $S[i, j] \neq b_1 \oplus b_2 \oplus \ldots \oplus b_k$, then $b_k = \overline{b_k}$.
Step 4.	Rearrange the above n bits $b_1, b_2, \ldots, b_n$ into $B_1[i, j]$, $B_2[i, j]$, …, $B_n[i, j]$ randomly.
Step 5.	Output $(B_1, B_2, \ldots, B_n)$.

3. Proposed Scheme

A new (k, n) RG-based VCS used with two decryption methods (OR and XOR) for binary images is presented, called (k, n) 2D_VCS. Algorithm 2 only considers the case of stacking k shares and does not consider the case of stacking more than k shares. Furthermore, additional consideration is required to fully restore the original secret image when collecting all the shares. Therefore, we add two steps, resulting in the following algorithm.

Algorithm 3 differs only in Steps 4 and 5 from Algorithm 2. These two steps lead to important consequences. Step 4 of Algorithm 3 makes the reconstructed image clearer when staking t $(k < t \leq n)$ shares. Step 5 of Algorithm 3 makes it possible to fully recover the secret image after collecting all n shares. Since we do not change the first k shares constructed

by Algorithm 2, when Algorithm 3 stacks k shares, the quality of the reconstructed image is similar to that by Algorithm 2. When stacking t shares, the probability of recovering the secret image is $1/C(n, t)$ $(n - k + 1)$, which makes the proposed scheme more clearly recover the secret using the XOR operator for tacking $k < t < n$ shares. Therefore, compared to earlier studies, the method has a higher quality of the recovered image and improved ability to recover the secret image with both XOR and OR operations. Figure 1 depicts the suggested scheme's schematic.

Algorithm 3 (k, n) 2D_VCS.

Input:	An $M \times N$ secret binary image S.
Output:	n shares $(B_1, B_2, \ldots, B_n)$.
Step 1.	For each position $[i, j]$, repeat Steps 2–6.
Step 2.	Randomly select from $\{0, 1\}$ to generate n random pixels $b_1, b_2, \ldots, b_n$.
Step 3.	If $S[i, j] \neq b_1 \oplus b_2 \oplus \ldots \oplus b_k$, then $b_k = \overline{b_k}$.
Step 4.	Select a number t randomly from $\{k + 1, k + 2, \ldots, n\}$. If $S[i, j] \neq b_1 \oplus b_2 \oplus \ldots \oplus b_t$, then $b_t = \overline{b_t}$.
Step 5.	If $S[i, j] \neq b_1 \oplus b_2 \oplus \ldots \oplus b_n$, then $b_n = \overline{b_n}$.
Step 6.	Randomly rearrange these n bits $b_1, b_2, \ldots, b_n$ into $B_1[i, j], B_2[i, j], \ldots, B_n[i, j]$.
Step 7.	Output $(B_1, B_2, \ldots, B_n)$

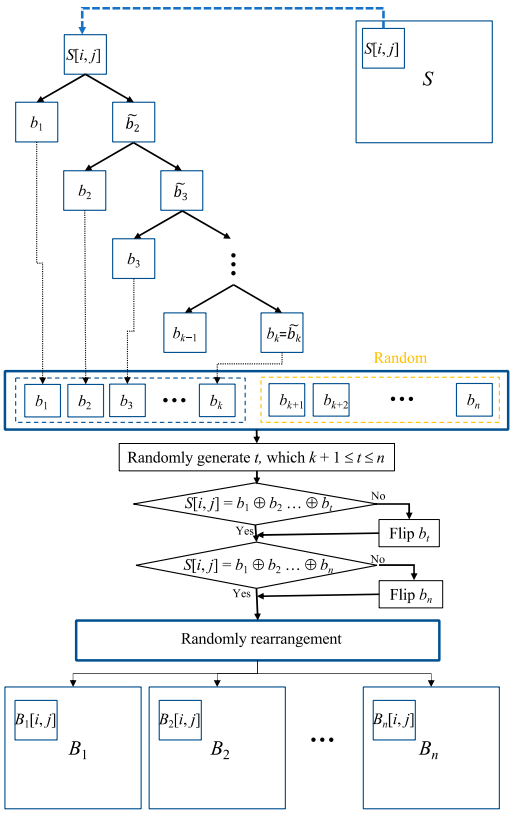


Figure 1. Schematic of the proposed scheme.

Therefore, we can directly stack enough shares ($\geq k$) to recover the binary secret image via HVS. Computers enable us to obtain more accurate secret images. However, when less than k shares are acquired, any clue about the binary secret image cannot be found.

4. Analysis

The proposed scheme's security is theoretically shown, and its performance is evaluated in terms of the visual aspect. First, we review useful tools and analyze the proposed scheme with these tools. We refer to definitions from previous works.

Definition 1. (Average light transmission [3]). *The probability that a given pixel, x, in the binary image X is transparent. Let Prob (x = 0) denote the light transmission of pixel x, which is shown by the symbol l[x]. The average light transmission of image X, with the size M × N, is expressed as*

$$LX \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} l[X[i,\ j]] \tag{1}$$

So, l[x] = 0 for an opaque pixel x, l[x] = 1 for a transparent pixel x. Also, we say L[B] = 1/2 for a random grid B normally.

Definition 2. (Contrast [3]) *The visual quality will determine how effectively the reconstructed image is recognized by human eyes. Contrast α is expressed as*

$$\alpha = \frac{L[B[S(0)]] - L[B[S(1)]]}{1 + L[B[S(1)]]} \tag{2}$$

where S(0) (S(1), respectively) stands for all of S's transparent (opaque, respectively) pixels, and B[S(0)] (B[S(1)], respectively) for all of the encrypted pixels from S(0) (S(1), respectively).

Definition 3. (Visually recognizable) *When L[B[S(1)]] < L[B[S(0)]], the contrast of the restored image α > 0, and the binary secret image S is recognized. Moreover, if α = 1, the recovered image B is the same as the original image S.*

Definition 4. (Security). *When L[B[S(0)]] = L[B[S(1)]], the light transmission of the transparent part of the original image is the same as that of the opaque part of the original image. That means no clue about the original secret image S can be recognized from the reconstructed image B. Therefore, if α = 0 when less than k shares are collected, the approach is secured since no information of S is retrieved.*

Table 1 lists all possibilities for sharing pixels when $k = 3$ and $n = 4$ of the (k, n) 2D_VCS, which is used to show this scheme is secured and visually recognizable.

Table 1. All possibilities b_1, b_2, b_3, b_4 for the proposed (3, 4) RG-based VCS.

S[*i*, *j*]	b_1	b_2	b_3	b_4
0	0	0	0	0
	0	1	1	0
	1	0	1	0
	1	1	0	0
1	0	0	1	0
	0	1	0	0
	1	0	0	0
	1	1	1	0

Lemma 1. *Algorithm 3 (k, n) 2D_VCS gives a (k, n) RG-based VCS with two decryption methods (OR and XOR) when k = 3 and n = 4. That is, Algorithm 3 satisfies the (1) security and (2) visually recognizable conditions.*

Proof. The following is divided into two parts to prove: (1) We must prove that stacking less than $k = 3$ shares (including one share) fails to yield any information regarding the binary secret image. From Tables 1–4 are induced, where $b_{x \oplus y}$ means $b_x \oplus b_y$, and $b_{x \otimes y}$ means $b_x \otimes b_y$ for any integers $1 \leq x < y \leq 4$. Similar notations are used later for stacking more than two shares.

Table 2. Contrast of each bit for Table 1.

$S[i, j]$	b_1	b_2	b_3	b_4
0	0	0	0	0
	0	1	1	0
	1	0	1	0
	1	1	0	0
1	0	0	1	0
	0	1	0	0
	1	0	0	0
	1	1	1	0
$L[B[S(0)]]$	0.5	0.5	0.5	1
$L[B[S(1)]]$	0.5	0.5	0.5	1
α	0	0	0	0

Table 3. Contrast of stacking any two bits using XOR operator for Table 1.

S	$b_{1\oplus2}$	$b_{1\oplus3}$	$b_{1\oplus4}$	$b_{2\oplus3}$	$b_{2\oplus4}$	$b_{3\oplus4}$
0	0	0	0	0	0	0
	1	1	0	0	1	1
	1	0	1	1	0	1
	0	1	1	1	1	0
1	0	1	0	1	0	1
	1	0	0	1	1	0
	1	1	1	0	0	0
	0	0	1	0	1	1
$L[B[S(0)]]$	0.5	0.5	0.5	0.5	0.5	0.5
$L[B[S(1)]]$	0.5	0.5	0.5	0.5	0.5	0.5
α	0	0	0	0	0	0

Table 4. Contrast of stacking any two bits using OR operator for Table 1.

S	$B_{1\otimes2}$	$B_{1\otimes3}$	$B_{1\otimes4}$	$B_{2\otimes3}$	$B_{2\otimes4}$	$B_{3\otimes4}$
0	0	0	0	0	0	0
	1	1	0	1	1	1
	1	1	1	1	0	1
	1	1	1	1	1	0
1	0	1	0	1	0	1
	1	0	0	1	1	0
	1	1	1	0	0	0
	1	1	1	1	1	1
$L[B[S(0)]]$	0.25	0.25	0.5	0.25	0.5	0.5
$L[B[S(1)]]$	0.25	0.25	0.5	0.25	0.5	0.5
α	0	0	0	0	0	0

Tables 2–4 show that α is 0 for any possible case; therefore, the proposed (k, n) 2D_VCS is safe when (k, n) = (3, 4). For proving Equation (2), we need to show that stacking k = 3 or 4 shares recovers the binary secret image S. Tables 5 and 6 show the correctness.

Table 5. Contrast of stacking any three or four bits using XOR operator for Table 1.

S	$b_{1\oplus2\oplus3}$	$b_{1\oplus2\oplus4}$	$b_{1\oplus3\oplus4}$	$b_{2\oplus3\oplus4}$	$b_{1\oplus2\oplus3\oplus4}$
0	0	0	0	0	0
	0	1	1	0	0
	0	1	0	1	0
	0	0	1	1	0
1	1	0	1	1	1
	1	1	0	1	1
	1	1	1	0	1
	1	0	0	0	1
$L[B[S(0)]]$	1	0.5	0.5	0.5	1
$L[B[S(1)]]$	0	0.5	0.5	0.5	0
Average α			0.1818		1

Table 6. Contrast of stacking any three or four bits using OR operator for Table 1.

S	$b_{1\otimes2\otimes3}$	$b_{1\otimes2\otimes4}$	$b_{1\otimes3\otimes4}$	$b_{2\otimes3\otimes4}$	$b_{1\otimes2\otimes3\otimes4}$
0	0	0	0	0	0
	1	1	1	1	1
	1	1	1	1	1
	1	1	1	1	1
1	1	0	1	1	1
	1	1	0	1	1
	1	1	1	0	1
	1	1	1	1	1
$L[B[S(0)]]$	0.25	0.25	0.25	0.25	0.25
$L[B[S(1)]]$	0	0.25	0.25	0.25	0
Average α			0.0526		0.25

According to Tables 5 and 6, the average α all > 0, which means that the proposed (3, 4) RG-based VCS is visually recognizable. Hence, the proof is complete.□

Then, the following theorem can be obtained. Due to the page limit, we skip the proof.

Theorem 1. *Algorithm 3 (k, n) 2D_VCS is a (k, n) RG-based VCS of two decryption methods (OR and XOR).*

Tables 7 and 8 show the theoretical contrast of the (k, n) 2D_VCS for stacking $2 \leq p \leq n$ shares for any $2 \leq k \leq n \leq 6$. We obtain these two tables by analyzing each case using a method similar to that in Lemma 1, which shows nothing is found when staking less than k shares, and the secret image S is revealed when staking more than or equal to k shares.

Table 7. Contrast of the proposed (*k*, *n*) RG-based VCS using OR operator.

(*k*, *n*)	*p* = 2	*p* = 3	*p* = 4	*p* = 5	*p* = 6
(2, 4)	0.0606	0.1579	0.375	-	-
(3, 4)	0	0.0526	0.25	-	-
(4, 4)	0	0	0.125	-	-
(2, 5)	0.0382	0.0786	0.1154	0.2083	-
(3, 5)	0	0.0204	0.0674	0.1875	-
(4, 5)	0	0	0.0227	0.125	-
(5, 5)	0	0	0	0.0625	-
(2, 6)	0.0260	0.0492	0.0621	0.0704	0.1094
(3, 6)	0	0.0106	0.0277	0.0495	0.1042
(4, 6)	0	0	0.0074	0.0294	0.0938
(5, 6)	0	0	0	0.0099	0.0625
(6, 6)	0	0	0	0	0.0313

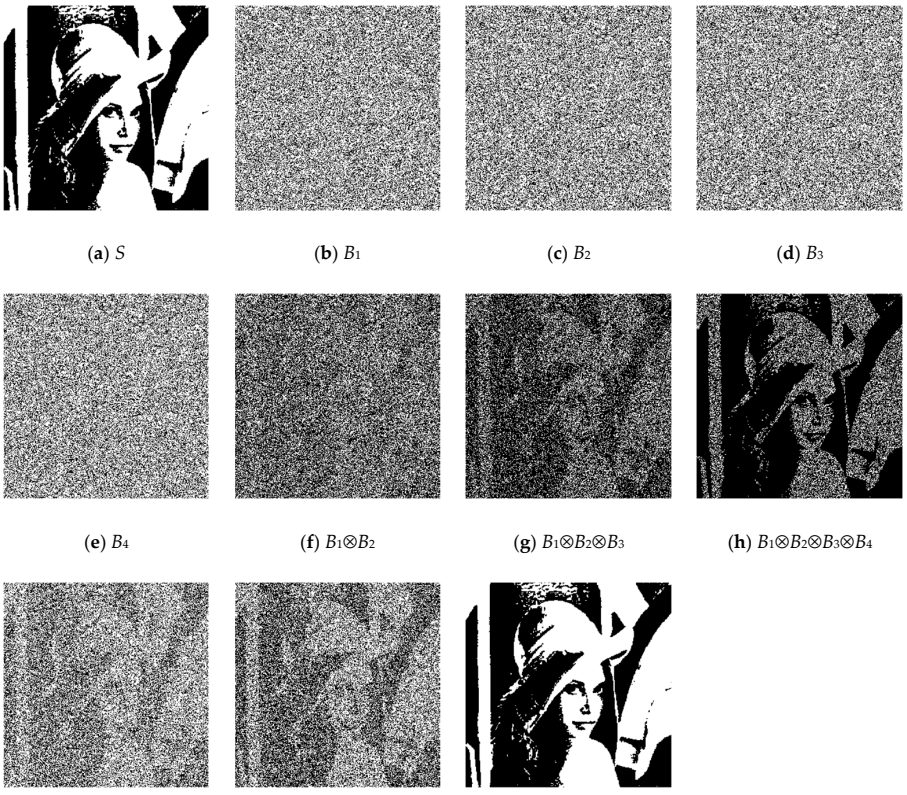
Table 8. Contrast of the proposed (*k*, *n*) RG-based VCS using XOR operator.

(*k*, *n*)	*p* = 2	*p* = 3	*p* = 4	*p* = 5	*p* = 6
(2, 4)	0.1111	0.1818	1	-	-
(3, 4)	0	0.1818	1	-	-
(4, 4)	0	0	1	-	-
(2, 5)	0.0674	0.0440	0.0930	1	-
(3, 5)	0	0.0690	0.1429	1	-
(4, 5)	0	0	0.1429	1	-
(5, 5)	0	0	0	1	-
(2, 6)	0.0449	0.0167	0.0220	0.0571	1
(3, 6)	0	0.0333	0.0301	0.0769	1
(4, 6)	0	0	0.0455	0.1176	1
(5, 6)	0	0	0	0.1176	1
(6, 6)	0	0	0	0	1

5. Experimental Results

The results of the (*k*, *n*) 2D_VCS when (*k*, *n*) = (2, 4), (3, 4), and (3, 5) are obtained in this section. The 300 × 300 pixels images in those experiments are utilized for original secret images and shares. Figure 2 shows the result for the proposed (2, 4) 2D_VCS. Figure 2a shows the secret image *S*, and Figure 2b–e show the four random-noise-like shares B_1, B_2, B_3, and B_4. The recovered binary images based on the OR operator are shown in Figure 2f–h. The recovered binary images based on the XOR operator are shown in Figure 2i–k.

Similarly, the experimental findings for the suggested (3, 4) and (3, 5) 2D_VCS are shown in Figures 3 and 4. Both (a) are the original binary secret images. Figures 3b–e and 4b–f are random shares. Figures 3f–h and 4g–j show the recovered binary images based on the OR operator. Then, Figures 3i–k and 4k–n are the recovered binary images based on the XOR operator.

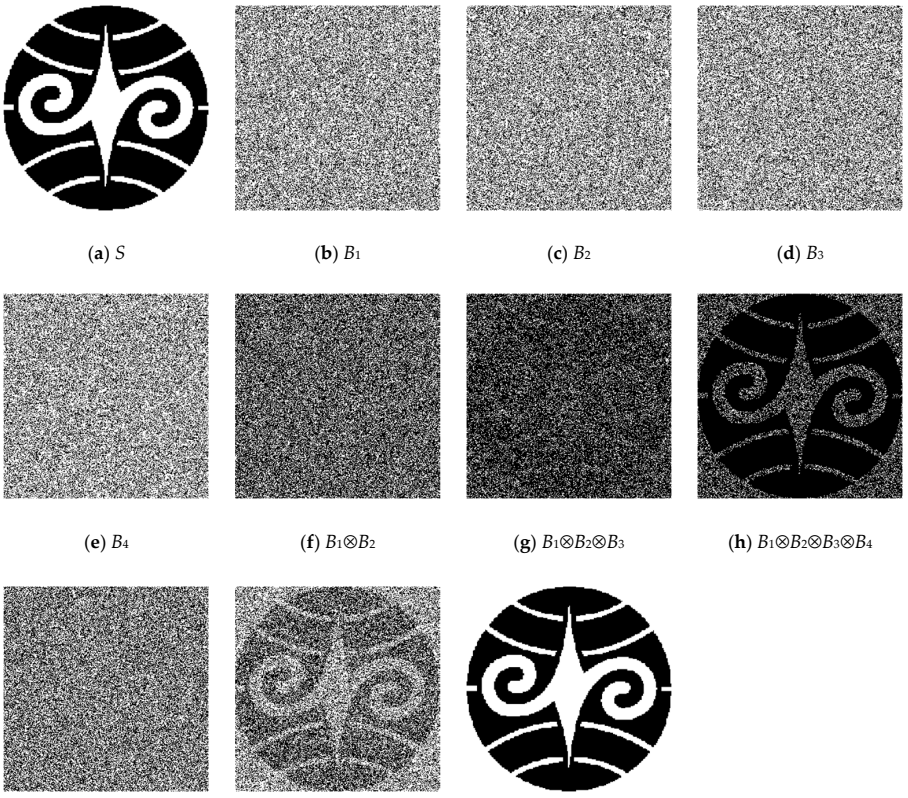


(**a**) S (**b**) B_1 (**c**) B_2 (**d**) B_3

(**e**) B_4 (**f**) $B_1 \otimes B_2$ (**g**) $B_1 \otimes B_2 \otimes B_3$ (**h**) $B_1 \otimes B_2 \otimes B_3 \otimes B_4$

(**i**) $B_1 \oplus B_2$ (**j**) $B_1 \oplus B_2 \oplus B_3$ (**k**) $B_1 \oplus B_2 \oplus B_3 \oplus B_4$

Figure 2. The experimental result of the proposed (2, 4) 2D_VCS.

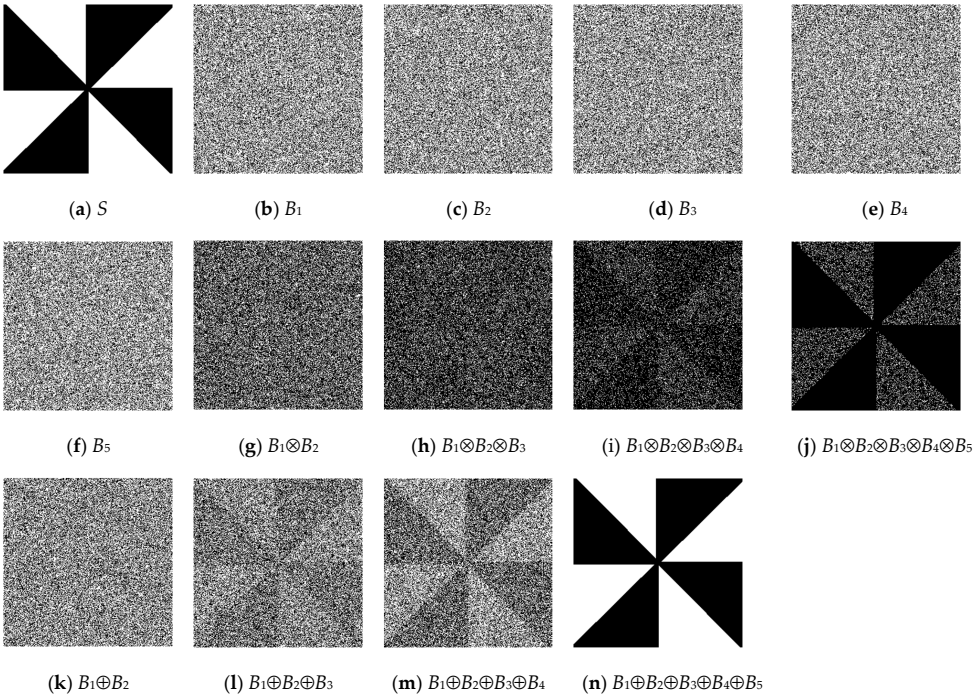


(**a**) S (**b**) B_1 (**c**) B_2 (**d**) B_3

(**e**) B_4 (**f**) $B_1 \otimes B_2$ (**g**) $B_1 \otimes B_2 \otimes B_3$ (**h**) $B_1 \otimes B_2 \otimes B_3 \otimes B_4$

(**i**) $B_1 \oplus B_2$ (**j**) $B_1 \oplus B_2 \oplus B_3$ (**k**) $B_1 \oplus B_2 \oplus B_3 \oplus B_4$

Figure 3. The experimental result of the proposed (3, 4) 2D_VCS.



(**a**) S (**b**) B_1 (**c**) B_2 (**d**) B_3 (**e**) B_4

(**f**) B_5 (**g**) $B_1 \otimes B_2$ (**h**) $B_1 \otimes B_2 \otimes B_3$ (i) $B_1 \otimes B_2 \otimes B_3 \otimes B_4$ (**j**) $B_1 \otimes B_2 \otimes B_3 \otimes B_4 \otimes B_5$

(**k**) $B_1 \oplus B_2$ (**l**) $B_1 \oplus B_2 \oplus B_3$ (**m**) $B_1 \oplus B_2 \oplus B_3 \oplus B_4$ (**n**) $B_1 \oplus B_2 \oplus B_3 \oplus B_4 \oplus B_5$

Figure 4. The experimental result of the proposed (3, 5) 2D_VCS.

We present more results in Tables 9 and 10. Compared to Tables 7 and 8, the theoretical analysis with the proposed method is more accurate.

Table 9. Average contrast for five experiments of the proposed method using OR operator.

(k, n)	$p = 2$	$p = 3$	$p = 4$	$p = 5$	$p = 6$
(2, 4)	0.05976	0.15859	0.37504	-	-
(3, 4)	0	0.05356	0.25135	-	-
(4, 4)	0	0	0.12456	-	-
(2, 5)	0.03624	0.07584	0.11362	0.20624	-
(3, 5)	0	0.02107	0.06915	0.18865	-
(4, 5)	0	0	0.02155	0.12336	-
(5, 5)	0	0	0	0.06257	-
(2, 6)	0.02564	0.05044	0.06234	0.07023	0.1086
(3, 6)	0	0.01071	0.02679	0.04997	0.10429
(4, 6)	0	0	0.00747	0.02963	0.09385
(5, 6)	0	0	0	0.009	0.06202
(6, 6)	0	0	0	0	0.03117

Table 10. Average contrast for five experiments of the proposed method using XOR operator.

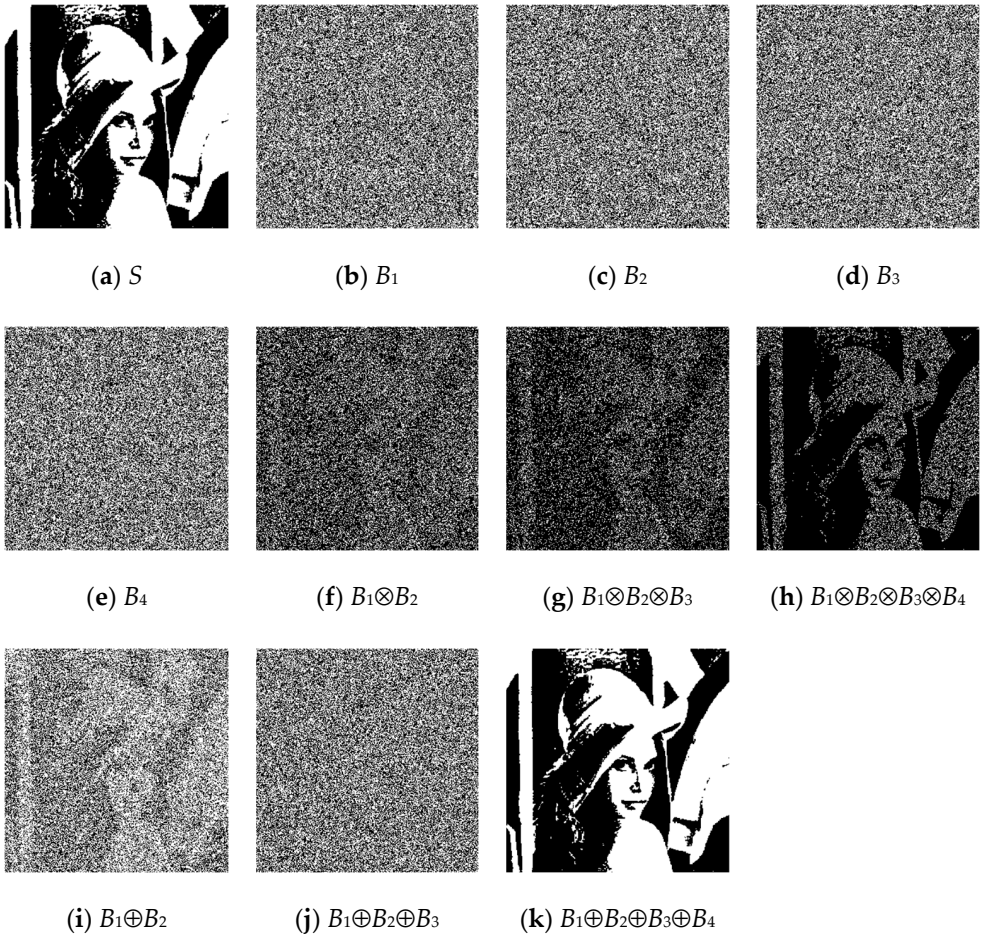
(k, n)	$p = 2$	$p = 3$	$p = 4$	$p = 5$	$p = 6$
(2, 4)	0.10901	0.18131	1	-	-
(3, 4)	0	0.18211	1	-	-
(4, 4)	0	0	1	-	-
(2, 5)	0.06857	0.04455	0.09344	1	-
(3, 5)	0	0.06945	0.14342	1	-

Table 10. *Cont.*

(*k*, *n*)	*p* = 2	*p* = 3	*p* = 4	*p* = 5	*p* = 6
(4, 5)	0	0	0.14142	1	-
(5, 5)	0	0	0	1	-
(2, 6)	0.04424	0.0168	0.02187	0.05863	1
(3, 6)	0	0.03139	0.0289	0.07784	1
(4, 6)	0	0	0.04554	0.11652	1
(5, 6)	0	0	0	0.12059	1
(6, 6)	0	0	0	0	1

6. Comparison and Conclusions

An RG-based (*k*, *n*) VCS restoring the secret image using OR or XOR operation was presented by Yan et al. [6]. We compared their scheme with the (*k*, *n*) 2D_VCS. The experimental outcome of Yan et al.'s scheme for the (*k*, *n*) = (2, 4) is shown in Figure 5. The results in Figures 2 and 5 show the better visual quality of the proposed scheme, especially when staking three shares and using the XOR operator on them ((j) in both figures). Thus, an RG-based (*k*, *n*)-threshold visual cryptography with XOR and OR decryption capabilities, called (*k*, *n*) 2D_VCS, is proposed to restore the secret image in a human visual system (OR) and computer visual system (XOR). The results are better than all previous studies. Future work will be carried out to design other RG-based (*k*, *n*) threshold VCSs with better contrast of the restored image and demonstrate that the scheme is theoretically safe and correct.



(**a**) S (**b**) B_1 (**c**) B_2 (**d**) B_3

(**e**) B_4 (**f**) $B_1 \otimes B_2$ (**g**) $B_1 \otimes B_2 \otimes B_3$ (**h**) $B_1 \otimes B_2 \otimes B_3 \otimes B_4$

(**i**) $B_1 \oplus B_2$ (**j**) $B_1 \oplus B_2 \oplus B_3$ (**k**) $B_1 \oplus B_2 \oplus B_3 \oplus B_4$

Figure 5. The experimental result used the (2, 4) RG-based VCS proposed in [6].

Author Contributions: Conceptualization, J.S.-T.J. and Y.-R.L.; methodology, J.S.-T.J.; software, Y.-R.L.; validation, J.S.-T.J. and Y.-R.L.; formal analysis, J.S.-T.J. and Y.-R.L.; investigation, J.S.-T.J. and Y.-R.L.; data curation, Y.-R.L.; writing—original draft preparation, Y.-R.L.; writing—review and editing, J.S.-T.J.; visualization, Y.-R.L.; supervision, J.S.-T.J.; project administration, J.S.-T.J.; funding acquisition, J.S.-T.J. and Y.-R.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Ministry of Science and Technology of the Republic of China grant number MOST 110-2221-E-260-003, and 110-2813-C-260-005-E. And The APC was funded by MOST 110-2221-E-260-003.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable to this article.

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

References

1. Naor, M.; Shamir, A. Visual cryptography. In *Workshop on the Theory and Application of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 1994.
2. Kafri, O.; Keren, E. Encryption of pictures and shapes by random grids. *Opt. Lett.* **1987**, *12*, 377–379. [CrossRef] [PubMed]
3. Shyu, S.J. Image encryption by multiple random grids. *Pattern Recognit.* **2009**, *42*, 1582–1596. [CrossRef]
4. Chen, T.; Tsao, K. Threshold visual secret sharing by random grids. *J. Syst. Softw.* **2011**, *84*, 1197–1208. [CrossRef]
5. Guo, T.; Liu, F.; Wu, C. Threshold visual secret sharing by random grids with improved contrast. *J. Syst. Softw.* **2013**, *86*, 2094–2109. [CrossRef]
6. Yan, X.; Wang, S.; Niu, X.; Yang, C.N. Random grid-based visual secret sharing with multiple decryptions. *J. Vis. Commun. Image Represent.* **2015**, *26*, 94–104. [CrossRef]